APUNTES
2/2018

FRIEDRICH EBERT STIFTUNG BOLIVIA

Protección de datos personales y derechos digitales

Cristian León Coronado - Eliana Quiroz - Adriana Foronda[1]

Julio, 2018

- La alta penetración de internet y digitalización de las actividades diarias de las personas ha complejizado y ampliado el debate en torno al derecho a la privacidad e intimidad. El uso regular de plataformas digitales facilita la producción, captura y procesamiento de datos personales, que pueden utilizarse para vigilar a las personas para la manipulación de información y desinformación tal, como ha sucedido en el caso de Cambridge Analytica. Así pues, varios países y bloques regionales están fortaleciendo sus normativas para la protección de datos personales.

- En este contexto, el Estado boliviano ha iniciado la elaboración de distintas normas relativas al uso y procesamiento de datos personales. Por un lado, se ha propuesto la reforma a la Ley Electoral para generar la interoperabilidad entre distintas bases de datos personales con el fin de facilitar la autenticación. Paralelamente, se ha impulsado una ley de ciudadanía digital para desburocratizar los trámites con el Estado a través de firmas digitales y otros procesos de gobierno electrónico. No obstante, aún queda pendiente una normativa específica para la protección de datos personales.

- En ese marco, el presente documento hace referencia a las tensiones que conlleva dicha legislación, acudiendo a un análisis de sus implicaciones y potenciales. Se menciona las problemáticas en torno a la ralentización de la modernización del Estado, así como las afectaciones a los negocios de internet. También aborda algunos puntos mínimos que la normativa de protección de datos debería incluir: respeto a derechos y garantías de las personas, consentimiento, adecuado tratamiento técnico y uso responsable.

FRIEDRICH EBERT STIFTUNG

INTERNET BOLIVIA .ORG

1 Se agradece las contribuciones de Gaspar Emilio Pisanu y Javier Pallero de la organización Access Now.

Tabla de contenidos

Introducción

La protección de datos personales está actualmente inmersa en un gran debate internacional y algunos últimos acontecimientos le han hecho ganar mayor visibilidad recientemente. Por un lado, la fuga de información protagonizada por Christopher Wylie acerca de la operación de la empresa británica Cambridge Analytica en las elecciones de 2016 en EE.UU[2]. y en el referéndum Brexit que marcó la próxima salida del Reino Unido de la Unión Europea -por mencionar solo dos procesos electorales en los que esa empresa estuvo contratada-. Por otro lado, la entrada en vigencia del Reglamento General de Protección de Datos (RGPD) de la Unión Europea a finales de mayo de este año, que se ha dicho pretende devolver a la ciudadanía mayor control sobre sus datos. El RGPD es una de las legislaciones de protección de datos más complejas que se ha creado para el sector tecnológico, con una implementación que ha tardado más de 2 años y que afectará al modelo de negocios de varias empresas.

En varios países de América Latina también existe una profunda preocupación acerca de este tema. La Declaración del XV Encuentro Iberoamericano de Protección de Datos 2017, Santiago de Chile lo expresa así:

Los avances tecnológicos que facilitan la obtención de información y la elaboración de perfiles, el tratamiento masivo de datos, la ubicuidad de las actividades y servicios prestados a través de internet, la inadecuada concientización sobre el verdadero valor de la información personal frente a los aparentes beneficios de la multiplicidad de productos o servicios ofrecidos por proveedores que solicitan dicha información, entre otros, genera importantes desafíos[3].

De manera más específica, el debate del voto electrónico y la privacidad en Argentina[4], además de los eventos de vigilancia estatal dirigida, como el caso del espionaje por parte del gobierno mexicano a periodistas y activistas[5], han puesto en la agenda pública el debate sobre la protección de datos personales; y aunque diez países de la región tienen normas generales sobre la materia, aún faltan varios, entre ellos: Bolivia, Brasil, Ecuador, El Salvador, Honduras, Guatemala, Panamá, Paraguay y Venezuela[6].

En el caso particular de Bolivia, este país tiene su propio proceso. Hace algunas semanas comenzó un debate sobre algunos aspectos de la protección de datos personales a raíz de una modificación del Artículo 79 de la Ley del Órgano Electoral que permitirá interoperar al Servicio de Registro Cívico (SERECI) y al Servicio General de Identificación (SEGIP). Posteriormente, se amplió el debate en torno a una Ley de ciudadanía digital en la Asamblea Legislativa, que según la norma aún en debate se entiende como:

2 The Guardian (6 de mayo de 2018) Cambridge Analytica: how did it turn clicks into votes? [Online]. Recuperado de https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie.

3 Red Iberoamericana de Protección de Datos (2017) Declaración del XV Encuentro Iberoamericano de Protección de Datos 2017. [Online]. Recuperado de http://www.redipd.es/documentacion/common/Declaracion_RIPD_XV_encuentro.pdf

4 Beatriz Busaniche y Federico Heinz (ed.) (2008) Voto electrónico: Los riesgos de una ilusión. 1era Edición. Córdoba: Fundación Vía Libre/Fundación Heinrich Böll.

5 Animal Político (19 de junio de 2017) Activistas y periodistas en México son espiados con un software adquirido por el gobierno: NYT. [Online]. Recuperado de https://www.animalpolitico.com/2017/06/periodistas-gobierno/

6 Red Iberoamericana de Protección de Datos (2017) Informe de la Presidencia 2017. [Online]. Recuperado de http://www.redipd.es/actividades/encuentros/XV/common/INFORME_DE_LA_PRESIDENCIA_PLAN_DE_ACTIVIDADES_2017-2018.pdf

La ciudadanía digital consiste en el ejercicio de derechos y deberes a través del uso de tecnologías de información y comunicación en la interacción de las personas con las entidades públicas y privadas que presten servicios públicos delegados por el Estado (…) El uso de los mecanismos de la ciudadanía digital implica que las instituciones mencionadas en el Parágrafo anterior puedan prescindir de la presencia de la persona y de la presentación de documentación física para la sustanciación del trámite o solicitud. (Artículo 4, proyecto de Ley Ciudadanía Digital).

Finalmente, si bien existe otro Proyecto de Ley que promovería el empadronamiento permanente y la votación electrónica en el exterior, y que abriría la posibilidad del debate sobre la implementación del voto electrónico a futuro, por el momento, el Tribunal Supremo Electoral descartó la propuesta para los comicios de 2019[7]. El voto electrónico tiene una implicación directa con respecto al uso de datos personales, en tanto requiere de mayores controles y protocolo de seguridad con respecto a la autenticación de votantes y al cuidado de votos emitidos, lo cual a su vez puede poner en peligro la privacidad, anonimidad e integridad del voto[8].

La principal crítica a estas modificaciones y desarrollos legislativos en Bolivia ha sido la falta de debate con amplios sectores y actores, además de la aparente escasa reflexión desde el punto de vista de los derechos humanos. En la región, estos temas han derivado en debates con participación inclusiva de diversos sectores sociales, así como de tiempos prolongados para su consenso. No son problemáticas que sólo conciernen a un sector privado tecnológico, a un grupo de intelectuales tech savvy o a entidades burocráticas de Estado; éstas son problemáticas normalmente trabajadas con transversalidad e interdisciplinariedad, pues tienen varias aristas y sus impactos conciernen, en gran medida, a los derechos humanos.

En ese sentido, el presente documento busca ser un aporte a la reflexión acerca de la protección de datos en Bolivia, desde un enfoque de los derechos digitales, que proporcione argumentos con respecto a su legislación.

¿Qué son los datos personales y por qué importan?

Los datos personales tienen múltiples acepciones con respecto a su comprensión. Son, por un lado, una representación de lo que somos y cómo nos identificamos. Su valor deriva de que contienen información de la identidad de las personas que incluso puede ser íntima. No obstante, el mundo digital impone más complejidades al respecto que veremos en la siguiente sección.

En su lado más conceptual-legal, de acuerdo, por ejemplo, a los Estándares de Protección de Datos Personales para los Estados Iberoamericanos[9] -que son usados como referencia por varias organizaciones latinoamericanas-, el término "dato personal"

7 Página Siete (16 de mayo de 2018) TSE: no habrá voto electrónico en el exterior. [Online]. Recuperado de http://www.paginasiete.bo/nacional/2018/5/16/tse-en-2019-no-habra-voto-electronico-en-el-exterior-180166.html.

8 Ártica y Fundación Vía Libre. Prólogo. Curso virtual: El voto electrónico en el marco de los derechos civiles y políticos. [Online]. Recuperado de https://cursos.vialibre.org.ar/pluginfile.php/40/mod_resource/content/2/Voto%20electr%C3%B3nico%20-%20Pr%C3%B3logo%20%28clase%201%29.pdf.

9 Red Iberoamericana de Protección de Datos (2017) Estándares de protección de datos para los Estados iberoamericanos. [Online]. Recuperado de http://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf.

se refiere a la: "información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente (...)".

Dentro de los datos personales se hace una diferencia con los datos personales sensibles; denominados así cuando:

"Se refieran a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos[10]*".*

Tomando en cuenta que los datos personales y datos personales sensibles son formas de identificación de las personas, se han desarrollado diferentes niveles de protección considerando los distintos actores.

Desde su perspectiva de garantes de la seguridad y del monopolio de la fuerza, los Estados tienen el deber de garantizar la protección de datos personales, pues el acceso inescrupuloso a estos podría tener consecuencias directas sobre la seguridad de las personas. Existen varios ejemplos de piratería de datos. Uno de ellos se realizó el año 2015 cuando un grupo de delincuentes robó 21,5 millones de registros de la Oficina de Administración de Personal de EE.UU. que contenían información personal, sumamente sensible, de los empleados federales y de los miembros de su familia[11]. Por otro lado, el escaso cuidado en el manejo de datos con respecto a personas protegidas en programas de testigos, grupos religiosos, agentes encubiertos u otros, puede derivar en ataques a los mismos; como fue el caso del ex-magistrado Gualberto Cusi de quien se reveló que tenía una enfermedad autoinmune, provocando cuestionamientos en su contra y rechazo a su persona.

Asimismo, desde una esfera más amplia, que concierne tanto al Estado como a empresas y organizaciones que manejan información, se busca proteger los datos personales para salvaguardar la identidad e intimidad de las personas. Información sobre creencias, orientaciones sexuales, salud de las personas o incluso la dirección del domicilio no son necesariamente datos que todos y todas estén dispuestos a compartir. En ese sentido, las personas deben tener la posibilidad de decidir si desean o no compartir ciertos datos, quién puede tener acceso a ellos, por cuánto tiempo, por qué razones, tener la posibilidad de modificarlos y de oponerse a compartirlos si así no lo desean.

Por lo tanto, la regulación debe ser capaz de poner límites en cuanto a la recolección, el uso y procesamiento de datos personales; establecer sanciones al uso indiscriminado de datos; restringir tratamientos automatizados de datos por parte de empresas que puedan abusar de ellos a través de: vigilancia masiva o dirigida, micro segmentación de perfiles para el posicionamiento publicitario, creación de noticias falsas, u otros mecanismos, que van en contra del derecho de privacidad y de libertad de expresión.

10 Ibid.

11 Pisanu, G. y Massé, E. (7 de mayo de 2018) Protección de datos:¿por qué es importante y cómo debes hacerlo?, Access Now. [Online]. Recuperado de https://www.accessnow.org/proteccion-de-datos-es-importante/.

Tres razones de la complejidad de la gestión de datos personales en la era digital

En la era digital la gestión de los datos personales se hace más compleja debido a tres razones: primero, la masividad de datos recolectados; segundo, la intimidad que refieren varios de éstos; y tercero, el valor económico que han adquirido.

Con respecto a lo primero, es preciso comprender que la capacidad de recolección de datos supera cualquier precedente. Según estimaciones, la recolección de datos, apenas en 2011, alcanzaba a un total de 1,8 zettabytes, con una proyección de crecimiento anual, para ese entonces, de 40%[12] . Sin duda, ha sido la enorme explosión de la web 2.0 la que ha incrementado exponencialmente este gran flujo de información. Los más de 2 mil millones de usuarios de Facebook crean, cada uno, en promedio, 90 piezas de contenidos diferentes cada mes y en conjunto comparten cerca de 30 mil millones de fotos, noticias, notas, links, entre otros, en ese mismo periodo de tiempo. En Youtube, hay alrededor de 490 millones de visitantes diferentes que ven, al menos, 2 millones de horas de video al mes y suben 24 horas de material cada minuto[13].

Segundo, en lo referido a la intimidad que implica la información recolectada, gran parte de ella contiene datos que pueden considerarse sensibles; desde las locaciones diarias de las personas -las cuales pueden ser accedidas fácilmente a través de la autenticación vía Google y el programa MyLocations-, las búsquedas realizadas en Google, o nuestras conexiones familiares que son capturadas por Whatsapp o Facebook. Los incidentes que comprometieron servidores como Yahoo, Apple, Snapchat, entre varios otros han demostrado que la información puede ser penetrable[14] [15].

Tercero, acerca del valor económico de los datos, la economía de los datos representa un paradigma nuevo para hacer negocios y comprender el mundo. A través de su tratamiento y procesamiento, se pueden crear formas inteligentes para generar toma-de-decisiones y planificar todo tipo de cosas. El Bigdata es la evolución natural de la sociedad de la información a la sociedad del conocimiento[16]; y esto es posible porque en los datos están contenidos, potencialmente, patrones de comportamiento, gustos, sentimientos e ideas, de modo que se pueden crear perfiles psicológicos de individuos y sociedades enteras, identificar estructuras de incentivos, y dinámicas de relacionamiento, entre otros[17].

La generación y producción de datos a través de la navegación en la red ha sido identificada por algunos autores como una forma de "plusvalía cognitiva", un concepto que Marx había introducido en sus cuadernos

12 McKinsey Global Institute (2011) Big data: The next frontier for innovation, competition and productivity. [Online]. Recuperado de https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx.
13 Ibid.

14 Mediatelecom Tecnología (10 de octubre de 2014) Roban fotos privadas de más de 200 mil cuentas de Snapchat. [Online]. Recuperado de http://tecnologia.mediatelecom.com.mx/2014/10/10/roban-fotos-privadas-de-mas-de-200-mil-cuentas-de-snapchat/.
15 Eleven Paths (12 de julio de 2016) Ataques Ransomware a iOS siguen ocurriendo en Estados Unidos y Europa, Seguridad Apple. [Online blog] Recuperado de http://www.seguridadapple.com/2016/07/ataques-ransomware-ios-siguen.html.
16 Hilbert, M. (2013) Big Data for Development: From Information to Knowledge Societies. SSRN Electronic Journal, 1-39. [Online]. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2205145.
17 Ibid.

Grundrisse[18]. La plusvalía cognitiva es ahora parte del proceso productivo que está beneficiando a las empresas que se dedican al data mining, analítica web, marketing, y a las que en general ofrecen algún tipo de servicio gratuito en internet: motores de búsqueda, servicios de redes sociales, juegos en línea, salas de chat, entre otras.

La privacidad como modelo de negocios en internet

La privacidad, en el marco de los modelos de negocios de internet, se ha convertido en un bien altamente mercantizable, y es ahí donde existen más vacíos legales.

No es novedad que servicios como Facebook, Twitter, Instagram, Google, entre otros, acumulan grandes conjuntos de datos personales que luego son comercializados y procesados por terceras empresas. Estas transacciones son desconocidas por la mayoría de los usuarios, y las empresas se escudan alegando que los usuarios consentimos el uso de nuestros datos personales a través de los contratos de término de uso que firmamos para acceder a los servicios; o bien, que los datos son anonimizados y, por ende, que no son datos personales. El problema con respecto a los datos personales es que están siendo recolectados y usados para diversos fines. Uno de ellos, según se vio en el caso de Cambridge Analytica, para microsegmentar públicos y hacer curaduría de la información que vemos.

Otro gran problema es que no sólo se vende privacidad, sino que al hacerlo, se afectan también otros derechos. Esta instrumentalización de los datos personales vulnera el derecho a la libertad de expresión y de pensamiento, pues básicamente se programan los contenidos que se consumen en internet para buscar manipular opiniones y acciones.

A nivel de los Estados, en cuanto a gestión de datos personales, si bien los mismos están lejos de tener la sofisticación de las grandes empresas de base tecnológica, hay casos de uso ilegal por parte de gobiernos contra grupos más vulnerables como periodistas, activistas y opositores políticos. No obstante, los gobiernos requieren de softwares de vigilancia desarrollados por empresas como Hacking Team. En esos casos, los Estados tiene que ser capaces de, por un lado, ponerse límites a sí mismos y, por otro, asegurar los niveles de seguridad suficientes para evitar poner en riesgo los datos de la ciudadanía en manos de terceros no autorizados.

Finalmente, las obligaciones en la ley de protección de datos deben aplicar claramente tanto al sector privado como al sector público. Las autoridades públicas recopilan cada vez más la información de los individuos, obteniendo acceso a bases de datos del sector privado, o bien construyendo grandes bases de datos de datos personales. Este procesamiento debe estar sujeto a obligaciones claras para la protección de la información personal de los individuos, de la misma manera en que se regula el procesamiento llevado a cabo por entidades privadas[19].

18 Rendueles, C. (2014) Emancipación, cuidado y codependencia, ISEGORÍA Revista de Filosofía, Moral y Política, 50: 167-187. [Online]. Recuperado de http://isegoria.revistas.csic.es/index.php/isegoria/article/viewArticle/855 .

19 Access Now (2018) La creación de un marco para la protección de datos: una guía para los legisladores sobre qué hacer y qué no. Lecciones del Reglamento General de Protección de Datos de la UE. [Online]. Recuperado de https://www.accessnow.org/cms/assets/uploads/2018/04/manual-de-proteccion-de-datos.pdfv.

Propiedad de los datos personales

Los datos personales, no solamente representan los atributos del individuo sino que además son resultado de sus propias acciones: habitar el espacio, ser ciudadano de un Estado, tener una identidad social y, por último, navegar en el ciberespacio usando distintas plataformas. Estas acciones, derivadas del impulso del propio individuo, le corresponden por lógica. Los datos personales son sus datos, su propiedad, independientemente de quién los recolecta o procesa.

Las entidades públicas generan datos personales en su interacción con los ciudadanos al crear documentos de identificación, licencias de conducir, registros domiciliarios. También lo hacen las empresas privadas al hacer registros de compras, fidelizar clientes, entre otros. No obstante, a pesar de que estos registros pueden generarse en beneficio de los ciudadanos, estos últimos siguen siendo dueños de sus datos. Esto implica que, en caso de que alguna de estas entidades tuviera que usar los datos o traspasarlos a otras entidades, debería primero tener el consentimiento del propietario del dato personal. A su vez, debería poder garantizar una adecuada gestión de estos datos, con la mayor protección posible, y tomando en cuenta los derechos de las personas a acceder, rectificar, cancelar y oponerse al tratamiento de los mismos. Estos son los derechos denominado ARCO.

Enfoque de derechos y principios

Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) son los derechos básicos cuando se trata de la protección de datos personales. Se refieren al derecho de las personas a: 1) acceder a sus propios datos, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento; 2) obtener la rectificación o corrección de sus datos personales por parte del responsable de la base de datos; 3) solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último; y, finalmente, 3) oponerse al tratamiento de sus datos personales por alguna razón legítima.

Además, existen principios que guían el tratamiento de los datos personales. Si bien no hay consenso acerca de todos los principios, se han extraído los principales de dos fuentes: los mencionados en las sugerencias a partir de la experiencia de RGPD de la Unión Europea[20] y la sugerencia de la Red Iberoamericana de Protección de datos personales[21]:

Licitud. Los datos personales deben ser procesados de acuerdo al marco legal del país, lo que implica que la información debe ser procesada en una base jurídica clara, con un propósito claro y con transparencia.

Consentimiento. "Para que exista un tratamiento de datos personales debe existir un consentimiento por parte del titular de Información, debe ir de la mano con que hay que informar (políticas de privacidad) sobre qué tratamiento se va a hacer, qué datos se van a tratar, con qué finalidad, dónde se va

20 Ibid.

21 Red Iberoamericana de Protección de Datos (2017) Estándares de protección de datos para los Estados iberoamericanos. [Online]. Recuperado de http://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf.

a transferir los datos, etc[22]."

Lealtad. El responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos.

Transparencia. El responsable debe informar al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Limitación de la finalidad o legitimidad. Los datos deberán ser recopilados y procesados sólo para fines específicos y legítimos. El propósito debe ser específico, explícito, y de duración limitada. Los datos no deben ser procesados en una manera que sea incompatible con dicho propósito.

Integridad y confidencialidad. Los datos personales deben ser procesados de manera que se garantice estrictos protocolos de seguridad para los datos, junto con la protección contra tratamiento no autorizado o ilegítimo y contra la pérdida accidental, destrucción o daños de los datos, utilizando medidas técnicas y organizacionales pertinentes.

Minimización de datos o proporcionalidad. Los datos personales recopilados y utilizados deben limitarse a ser suficientes, pertinentes y no excesivos en relación con un propósito específico y definido.

Exactitud. Los datos personales deben ser precisos y, cuando corresponda, deben ser actualizados.

Conservación limitada. Los datos personales procesados por cualquier propósito no deben ser mantenidos por más tiempo del necesario.

Adecuación. Los datos personales no deben ser transferidos a un país o territorio tercero, a menos que el país o territorio en cuestión garantice un nivel adecuado de protección para los derechos y libertades de los usuarios en relación con el procesamiento de datos personales. Los marcos de protección de datos deben brindar un mecanismo que habilite la libre circulación de datos entre países y garantice un alto nivel de protección de datos.

Sin embargo, estos principios y derechos son enunciativos si solo se plasman en normativa. Se requiere, además, crear las condiciones para su ejercicio; y eso pasa por recursos para informar y formar a la ciudadanía de manera que el consentimiento sea realmente informado, con plena comprensión del alcance de la gestión de sus datos. De igual manera, se requiere una institución políticamente independiente, que asegure el cumplimiento de la normativa y de los derechos humanos en espacios digitales. En algunos países, esto ha tomado la forma de una Agencia de Protección de Datos.

Las tensiones derivadas de legislar sobre datos privados

El mercado está liderando esta dinámica en la que los insumos básicos de las grandes empresas de Internet han pasado a ser los datos personales, mientras que los Estados están comenzando a utilizar los datos personales para programas modernizadores de gobierno electrónico y gobierno abierto,

22 LACIGF (2017) Sesión 3: Protección de datos: Alternativas para América Latina y el Caribe para la Protección de Datos. Uso de datos por parte del sector del sector privado y el público. [Online]. Recuperado de https://lacigf.org/wp-content/uploads/2017/10/lacigf10-s3-leyprotecciondatos-es.pdf

interoperándolos, proponiendo algoritmos, inteligencia artificial y tecnologías de cadenas de bloques que usan los datos para hacer perfiles de ciudadanos y ciudadanas, y para mejorar los servicios públicos.

Así, nos vemos ante dos tensiones. La primera hace referencia a que se deben proteger los derechos de privacidad de datos personales y, a la vez, no ralentizar la velocidad de los negocios en Internet, aunque esto suene lejano para un país como Bolivia en el que el comercio electrónico es incipiente[23]. La segunda se refiere a que se deben proteger los derechos de privacidad de datos personales y, a la vez, no parar la modernización hacia un Estado más eficiente, cálido y participativo.

Debemos comprender, en primer lugar, que los datos personales son parte del derecho de cada individuo a la intimidad y privacidad, consagrado en la Declaración Universal de Derechos Humanos de 1948 en su artículo 12:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

En Bolivia, el artículo 21 de la Constitución Política del Estado regula la privacidad como un derecho de las personas, mientras que la garantía constitucional de Acción de Protección a la Privacidad está regulada en los artículos 130 y siguientes.

La Protección de datos personales se deriva de este derecho más general a la privacidad. En Bolivia, el artículo 56 del Decreto Supremo No. 1793 (Reglamento para el Desarrollo de Tecnologías de la Información y Comunicación) del 13 de noviembre de 2013, cuando habla del titular del certificado digital, menciona la protección de datos personales:

A fin de garantizar los datos personales y la seguridad informática de los mismos, se adoptan las siguientes previsiones:

a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;

b) El tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo;

c) Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales

23 Según Encuesta de AGETIC (2017), solo el 9% de los internautas han hecho algún pago por Internet. Resultados Finales Encuesta TIC. [Online]. Recuperado de https://agetic.gob.bo/pdf/dia_internet_encuesta.pdf.

objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;

d) Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;

e) El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Sin embargo, estas previsiones legales son solo válidas para los datos que se recaban para los certificados digitales, como la firma digital, y no para todos los registros que impliquen datos personales, ni para el resto de actividades comerciales, políticas y de otra índole. Lo que vemos entonces, es la necesidad de que la legislación no sólo involucre ciertas tecnologías, o sólo rija sobre actividades precisas, sino que sea general y se aplique en un marco amplio, pues la recolección de datos personales es, hoy en día, un problema transversal.

La legislación debe tener como eje principal la protección de la privacidad como bien y derecho de las personas, entendiendo que los datos personales les pertenecen. Estos deben regirse sobre los principios de los derechos ARCO y no pueden estar sujetos a interpretaciones para facilitar procesos burocráticos o comerciales.

Conclusiones

La problemática de datos personales no es necesariamente nueva. De hecho, la primera legislación fue aprobada en 1970 en Bremen, Alemania, y desde ahí ha tenido un largo recorrido. Los Estados recolectan datos personales de la ciudadanía para armar sus registros administrativos y las empresas negocian con datos personales desde inicios del siglo XX (cuando, por ejemplo, las empresas aseguradoras requerían información de sus clientes y potenciales clientes).

Sin embargo, la era digital promueve serios desafíos a la protección de datos personales porque se hace más compleja debido a tres razones: primero, la masividad de datos recolectados; segundo, la intimidad que refieren varios de éstos; tercero, el valor económico que han adquirido. Es un panorama que, potencialmente, puede afectar a varios derechos humanos, entre ellos, la privacidad y la libertad de expresión.

El mercado está guiando esta insaciabilidad por más y más datos personales, y los ha convertido en la materia prima de los negocios de la Sociedad de Conocimiento. Los Estados, por su parte, han comenzado a utilizar los adelantos tecnológicos para mejorar sus registros administrativos, concentrarlos e interoperarlos para dar un mejor servicio a la ciudadanía. Incluso hay iniciativas de uso de algoritmos, inteligencia artificial y cadenas de bloques para mejorar los servicios públicos.

Ante este ímpetu de extraer, tratar, comercializar y procesar los datos personales, se hace evidente que los actores fuertes son las empresas y que los gobiernos ahora se están fortaleciendo, mientras que quienes quedan en desventaja son el conjunto de

ciudadanos y ciudadanas.

Es necesario generar un equilibrio de poder, y eso pasa por el fortalecimiento de la protección de los datos personales en un marco de derechos humanos. De esa manera, se impulsa la formulación de normas de protección de datos personales, respetando ciertos principios que tienden a enmarcar las acciones de generación de datos dentro de fines legítimos, como informar al respecto a la ciudadanía y solicitarle su consentimiento a partir de la información brindada, en el entendido de que los datos personales les pertenecen a las personas. Además, es apremiante que no se soliciten más datos de los necesarios, que no se los conserve por más tiempo del necesario y que se asegure la protección contra tratamiento no autorizado o ilegítimo, y contra la pérdida accidental, destrucción o daños de los datos, utilizando medidas técnicas y organizacionales pertinentes.

Asimismo, se deben tomar en cuenta los derechos ARCO que son fundamentales cuando se trata de normas de este tipo. Sin embargo, es necesario asegurar las condiciones para el ejercicio de estos derechos; campañas de información y formación ciudadana permanentes y una Agencia de Protección de Datos políticamente independiente, son dos elementos que forman parte del paquete de protección de datos personales.

Bibliografía

Access Now (2018) "*La creación de un marco para la protección de datos: una guía para los legisladores sobre qué hacer y qué no. Lecciones del Reglamento General de Protección de Datos de la UE*". [Online]. Recuperado de https://www.accessnow.org/cms/assets/uploads/2018/04/manual-de-proteccion-de-datos.pdf.

AGETIC (2017) "*Encuesta Nacional de Opinión sobre Tecnologías de Información y Comunicación (TIC)*". [Online]. Recuperado de https://agetic.gob.bo/pdf/dia_internet_encuesta.pdf.

Animal Político (19 de junio de 2017) "Activistas y periodistas en México son espiados con un software adquirido por el gobierno": NYT. [Online]. Recuperado de https://www.animalpolitico.com/2017/06/periodistas-gobierno/.

Ártica y Fundación Vía Libre. Prólogo. Curso virtual "*El voto electrónico en el marco de los derechos civiles y políticos* "[Online]. Recuperado de https://cursos.vialibre.org.ar/pluginfile.php/40/mod_resource/content/2/Voto%20electr%C3%B3nico%20-%20Pr%C3%B3logo%20%28clase%201%29.pdf.

Asociación por los Derechos Civiles (2016) "*El Sistema de Protección de Datos Personales en América Latina.Oportunidades y desafíos para los derechos humanos. Argentina*". https://adcdigital.org.ar/wp-content/uploads/2017/06/Sistema-proteccion-datos-personales-LatAm.pdf.

Beatriz Busaniche y Federico Heinz (ed.) (2008) "*Voto electrónico: Los riesgos de una ilusión. 1era Edición. Córdoba: Fundación Vía Libre/Fundación Heinrich Böll*".

Eleven Paths (12 de julio de 2016) "*Ataques Ransomware a iOS siguen ocurriendo en Estados Unidos y Europa, Seguridad Apple*". [Online blog]. Recuperado de http://www.seguridadapple.com/2016/07/ataques-ransomware-ios-siguen.html.

Gantz, John; Reinsel, David y Rydning, John (2017) Data Age 2025: "*The evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big, IDC White Paper*". [Online]. Recuperado de https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.

Hilbert, Martin (2013) "*Big Data for Development: From information to knowledge societies. SSRN Electronic Journal, 1-39*". [Online]. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2205145.

LACIGF (2017) Sesión 3: "*Protección de datos: Alternativas para América Latina y el Caribe para la Protección de Datos. Uso de datos por parte del sector del sector privado y el público*". [Online]. Recuperado de https://lacigf.org/wp-content/uploads/2017/10/lacigf10-s3-leyprotecciondatos-es.pdf.

McKinsey Global Institute (2011) Big data: "*The next frontier for innovation, competition and productivity*". [Online]. Recuperado de https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx.

Mediatelecom Tecnología (10 de octubre de 2014) "*Roban fotos privadas de más de 200 mil cuentas de Snapchat*". [Online]. Recuperado de http://tecnologia.mediatelecom.com.mx/2014/10/10/roban-fotos-privadas-de-mas-de-200-mil-cuentas-de-snapchat/.

Página Siete (16 de mayo de 2018) TSE: "*no habrá voto electrónico en el exterior*". [Online]. Recuperado de http://www.paginasiete.bo/nacional/2018/5/16/tse-en-2019-no-habra-voto-electronico-en-el-exterior-180166.html.

Pisanu, Gaspar y Massé, Estelle (2018) "*Protección de datos personales: ¿Por qué es importante y cómo debes hacerlo?, Access Now*". [Online]. Recuperado de https://www.accessnow.org/proteccion-de-datos-es-importante/.

Red Iberoamericana de Protección de Datos (RIPD) (2017) "*Informe de la Presidencia 2017*". [Online]. Recuperado de http://www.redipd.es/actividades/encuentros/XV/common/INFORME_DE_LA_PRESIDENCIA_PLAN_DE_ACTIVIDADES_2017-2018.pdf.

Red Iberoamericana de Protección de Datos (2017) "*Estándares de protección de datos para los Estados iberoamericanos*". [Online]. Recuperado de http://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf.

Rendueles, César (2013) Sociofobia: "*El cambio político en la era de la utopía digital. Madrid:*" México D.F.: Debate.

Rendueles, César (2014) "*Emancipación, cuidado y codependencia, ISEGORÍA Revista de Filosofía, Moral y Política, 50: 167-187*". [Online]. Recuperado de http://isegoria.revistas.csic.es/index.php/isegoria/article/viewArticle/855.

The Guardian (6 de mayo de 2018) "*Cambridge Analytica: how did it turn clicks into votes?*" [Online]. Recuperado de https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie.

Unión Europea (2016) "*Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril (Reglamento General de Protección de Datos)*". [Online] Recuperado de https://www.boe.es/doue/2016/119/L00001-00088.pdf.

Autor:

Cristian León investigador y gestor de proyectos en derechos digitales, gobierno abierto y tecnopolítica. Es miembro del Directorio de InternetBolivia.org y coordinador de Innovación Política de Asuntos del Sur. Ha sido investigador en tecnología y sociedad en el CIS de la Vicepresidencia, PNUD, TSE y OEA; analista de conflictos sociales en la Fundación UNIR Bolivia. MSc en Desarrollo Internacional por la Universidad de Bristol (Inglaterra), licenciatura en Ciencias Políticas en la UCB.

Eliana Quiroz investigadora y activista de Internet y sociedad con estudios en Bolivia, Alemania e Italia. Coordinadora y coautora del libro "Bolivia digital, 15 miradas acerca de Internet y Sociedad en Bolivia", editado por el CIS de la Vicepresidencia del Estado. Msc en Gestión Pública y candidata a doctora en Ciencias del Desarrollo en CIDES/UMSA. Coordinadora Ejecutiva de Internet Bolivia. org.

Adriana Foronda economista con estudios en Desarrollo, Relaciones Internacionales y Diplomacia. Ha trabajado en proyectos sobre comercio, desarrollo regional y género. Está elaborando un estudio sobre comercio electrónico y gobernanza global.

Pie de imprenta

Friedrich-Ebert-Stiftung Bolivia

Av. Hernando Siles C/14 Obrajes N° 5998

La Paz - Bolivia

ISBN: 978-99974-0-245-5
DL: 4-4-2121-18

Contacto

Tel: +591 2-2750005
Fax: +591-2-2750090
www.fes-bolivia.org
info@fes-bolivia.org
Facebook: Fundación Friedrich Ebert Bolivia
Twitter: @BoliviaFes