SITUACIÓN DE LA

Privacidad **en Bolivia**

SERIE
#FUTURODIGITAL**BO**

SITUACIÓN DE LA

Privacidad **en Bolivia**

SERIE
#FUTURODIGITAL**BO**

Este informe fue realizado por la Fundación InternetBolivia.org, con el apoyo del Fondo de Respuesta Rápida para la Protección de los Derechos Digitales en América Latina, gestionado por Derechos Digitales, y con apoyo de la Fundación Friedrich Ebert en Bolivia.

Autor

- Cristian León Coronado.

Coordinación de la serie

- Cristian León

Edición

- Eliana Quiroz

Diseño

- Marcelo Lazarte

Febrero de 2020 La Paz – Bolivia

Índice

EL ESTADO DE LA

Privacidad en Bolivia

Cristian León Coronado[1]

INTRODUCCIÓN

En una era en la cual las empresas mercantilizan los datos personales y los gobiernos hipervigilan a la población, la privacidad cobra mayor importancia como derecho humano y garantía para ejercer una democracia plena. Los casos en los que se comprobó abusos a partir del mal uso de las tecnologías digitales para monitorear a la ciudadanía y recopilar datos personales para perfilar personas, levantaron una gran alerta a nivel global. Estas acciones afectan la libertad de expresión, al derecho a la privacidad, sesgan la opinión pública y buscan manipular el comportamiento. Es por ello, que en diversos países y regiones, se empezó a legislar y a tomar acciones al respecto aprobando normativa para la protección de los datos personales e intentando regular a las grandes plataformas como Facebook, Twitter, Google, entre otras.

Tomando en cuenta ese marco, el Estado boliviano así como varios otros, no se encuentra preparados para ofrecer a los ciudadanos y ciudadanas las garantías para la protección al derecho a la privacidad.

La débil situación de la protección de la privacidad en Bolivia se debe a múltiples aspectos:

- Un marco legislativo desactualizado, políticas públicas sin visión de protección de derechos – algunas incluso los vulneran en vez de protegerlos, como es el caso de infraestructura de seguridad de los sistemas de información públicos con vulnerabilidades (como se verá más adelante), entre otros.

1 Politólogo boliviano. MSC en Desarrollo Internacional (Universidad de Bristol, UK). Miembro fundador de InternetBolivia.org.

- Incremento de la penetración de las tecnologías digitales y el aumento del uso de internet, sobre todo en lo que corresponde al uso de internet móvil. La futura implementación de redes 5g, trae enormes desafíos para los cuales Bolivia no está preparada en términos de derechos digitales.
- Se están aprobando e implementando varias políticas públicas, ligadas a la seguridad ciudadana y a la modernización del Estado, que potencialmente pueden plantear esquemas de abuso de los derechos humanos. Está por ejemplo, el Programa de seguridad BOL 110 financiado por China y basado en tecnología de la empresa estatal CEIEC. Esta es de especial preocupación debido a los antecedentes de la empresa en otros países[2].
- El anterior gobierno implementó un sistema de identificación digital (Ciudadanía digital) con potenciales riesgos en cuanto a concentración de datos en una sola entidad pública y perfilamiento de ciudadanos y ciudadanas. Esa infraestructura, bases de datos y servicios, no han sido transparentados y requieren un análisis con respecto a sus implicaciones.
- Estas políticas se implementan sin un marco de referencia o reglamentación y con varios vacíos preocupantes. En Bolivia no existe una Ley de Protección de Datos Personales, no existe ningún marco sobre el uso de tecnologías de vigilancia, monitoreo en video (más allá de plazas, bancos y algunos recintos), ni manejo de datos biométricos.
- Empresas, organizaciones e incluso partidos políticos están empezando a usar servicios de marketing y perfilamiento a través de la captura de datos personales. En las pasadas elecciones generales de 2019, que fueron anuladas, se supo por medios extranjeros que algunos partidos políticos contrataron empresas de este tipo[3].

2 https://www.nytimes.com/es/2019/04/24/ecuador-vigilancia-seguridad-china/

3 De acuerdo a un artículo publicada en Quartz de agosto de 2019, el partido Demócratas había usado los servicios de la empresa IDEIA, la cual utiliza los mismos métodos de perfilamiento que la empresa Cambridge Analytica. https://qz.com/1666776/data-firm-ideia-uses-cambridge-analytica-methods-to-target-voters/

Las falencias mencionadas son sólo la parte perimetral de lo que implica la protección y regulación de la privacidad, en tanto ni siquiera se toman en cuenta temas más complejos y enfoques normativos más avanzados en Bolivia. Así por ejemplo, todavía no se discute o menciona sobre regulación de flujo transfronterizo de datos personales, manejo de datos biométricos, la responsabilidad de los intermediarios, autorización para el uso de datos para marketing y operaciones de big data, regulación del uso de pseudónimos en cuentas y cifrado, construcción de estándares legales para la vigilancia, entre otros. Estos temas requieren todavía una base mínima de reconocimiento de la protección de la privacidad como derecho y un enfoque normativo, desde una ley de protección de datos personales. Esto, aún no se ha logrado en Bolivia.

Basado en estos argumentos, es necesario abordar la necesidad de un mayor marco de protección de la privacidad y los datos personales en Bolivia.

Es por ello que el presente documento busca dar algunos pasos para la comprensión de la problemática vista desde el caso boliviano, e influir así en la profundización de su debate y la adopción de futuras políticas públicas.

El mismo se divide en cuatro secciones: la primera parte está destinada a discutir la privacidad desde un enfoque amplio, entrando a lo político, y analizandola desde sus tensiones con la seguridad pública y el mercado capitalista. La segunda se centra en el marco normativo de protección en Bolivia, describiendo las leyes existentes. La tercera sección aborda los riesgos que implican algunas políticas públicas que se empezaron a implementar en Bolivia (Ley de ciudadanía digital, y el programa de seguridad BOL-110), las cuales deberían ser analizadas con respecto a su continuidad para determinar si cumplen o no con estándares de derechos humanos. Finalmente, se suma a la débil protección jurídica garantías mínimas que los servicios estatales deberían poder brindar a la ciudadanía (páginas web y bases de datos sobre la ciudadanía).

1. La privacidad como derecho humano

Decir que toda acción realizada por un ciudadano/a, tanto en el ámbito público como en el privado, es observada por un gran ojo que todo lo ve y todo lo registra, dejó de ser una ficción. Ese gran ojo tiene nombre: son Google y Facebook, son incluso las empresas que nos brindan servicio de internet, incluso puede ser el Estado. Cada acción que ejecutamos en Internet es una acción que se convierte en un dato que se almacena en algún lugar. En tanto ahora los dispositivos celulares nos acompañan a cada momento y estos son rastreados por antenas para brindarnos cobertura todo el tiempo, poseen cámaras y micrófonos, y todo tipo de sensores, estos también generan datos de nuestra vida diaria.

A su vez, no sólo se trata de los datos que producimos a través de nuestras acciones en internet, pero en general todo tipo de dato sobre nuestra identidad que gobiernos y las empresas sistematizan y guardan en repositorios digitales.

¿Qué pasa si alguien accede a esos datos sin nuestra autorización para cambiarlos o exponerlos públicamente? ¿Entendemos que esa información puede ser usada para extorsionarnos o manipularnos? ¿Quién puede y quién no, saber nuestra información personal? ¿Cuánta capacidad tiene la ciudadanía para reclamar, pedir rectificaciones y proteger su privacidad? Los riesgos son múltiples y la brecha de poder entre quienes tienen esos accesos y la ciudadanía se ensancha cada vez más. Ante esa situación, las únicas garantías que tiene el ciudadano son el derecho a la privacidad, el *habeas data*, y la protección de datos personales, los cuales son diferentes, pero están ligados entre sí.

La privacidad, en términos jurídicos, es aquello que tiene carácter particular, personal, íntimo y/o confidencial (Quiroz, 2016). El derecho a la privacidad es, entonces, una garantía de protección que tiene el ciudadano/a, así como la facultad de decidir, sobre aquella información que es de carácter privado (esto incluye aspectos de la vida personal, identidad, imagen, forma de pensar, situación financiera, salud, etc.); por lo que nadie puede inmiscuirse en ella sin autorización del dueño de esos datos (Quiroz, 2016).

De acuerdo a la abogada Roxana Pérez del Castillo: "el derecho a la privacidad es uno de los derechos más intrínsecos al ser humano, porque permite delimitar el espacio en el cual te circunscribes. Tienes la intimidad que quieres que se resguarde para no tener interferencias de terceras personas, que te pongan en una situación de vulnerabilidad y ultravulnerabilidad, y que no te generen una inequidad en el ejercicio de tus otros derechos" (Entrevista personal, octubre, 2019).

En ese marco, la protección de la privacidad está presente en múltiples instrumentos internacionales y en constituciones de distintos países. No obstante, la concepción de privacidad está ligada desde la esfera de lo íntimo, como ese espacio personal que busca ser diferenciado de lo público, con antecedentes de su legislación desde alrededor de 1890 en Estados Unidos.

La relación de la privacidad con respecto al manejo de la información como tal es un concepto relativamente reciente. En esa intersección surge el: *habeas data*. El *habeas data* es la autodeterminación informativa que tiene cada ciudadano/a para acceder y controlar la información que es registrada y almacenada por distintas entidades públicas y privadas (Quiroz, 2016). Como tal, el *habeas data* faculta a los individuos a poder dar autorización expresa previa sobre toda información privada que le es solicitada, así como de consultar el uso que se le dará a la misma, pedir correcciones, actualizaciones, entre otros (Chiriboga, 2001).

"La autodeterminación es esencial en el marco legislativo de los derechos digitales, porque a través de este derecho, se otorga a las personas la facultad de decidir, qué, cuándo y cómo sus datos van a estar en el escenario digital, esa persona tiene que saberlo, esto te da la seguridad y el resguardo jurídico de que tú estás dando tu consentimiento, estás siendo informada, esto le da un contexto de legalidad y seguridad jurídica de que tienes conocimiento y control de lo que está pasando en el mundo digital respecto a tus datos personales" (Roxana Pérez del Castillo, entrevista personal)

En Latinoamérica, el *hábeas* data se introdujo a través de los derechos y garantías de "tercera generación" a partir de 1988 (en la Constitución de Brasil), y posteriormente con otras reformas constitucionales en Colombia (1991), Perú (1993), Argentina (1994), Ecuador (1998), Venezuela (1999) (Masciotra, 2018).

Los avances de las tecnologías digitales incrementaron la recopilación de datos personales y su procesamiento para nuevos bienes y servicios, generando así nuevas necesidades con respecto al tratamiento de datos personales sensibles. A partir de eso, se empezó a desarrollar legislación más específica al respecto, creándose leyes de protección de datos personales en varios países. De acuerdo a la Red Iberoamericana de Protección de Datos (RIPD, 2017), la protección de datos personales es un derecho en sí mismo. Los datos personales deben ser tipificados

en base a su sensibilidad, se deben establecer y garantizar condiciones mínimas de seguridad para su manejo, así como alcances y restricciones para su procesamiento.

Es decir, a diferencia del derecho a la privacidad y el *habeas data*, la protección de datos personales avanza un paso más en la protección de la privacidad, en tanto atiende una nueva necesidad: la de resguardar lo que los datos dicen sobre nosotros. La exposición o mal uso de estos puede afectar la intimidad, dignidad y reputación de las personas, rasgos de la identidad, afectar la libertad de expresión, pensamiento y/o asociación, o hasta poner en riesgo la integridad física. De acuerdo a últimos acontecimientos, como el de Cambridge Analytica, también sabemos que los datos pueden ser usados para manipulación e influencia en el comportamiento.

Entonces, se entiende que la protección de la privacidad no sólo involucra reconocerla en la Constitución desde la perspectiva de la intimidad, sino a su vez, fortalecerla desde mecanismos como la autodeterminación informativa (*habeas data*) y, en el marco de la era digital, con la protección de datos personales. La ausencia de estos mecanismos contraviene derechos humanos esenciales.

LA TENSIÓN ENTRE SEGURIDAD Y PRIVACIDAD

Cuando Edward Snowden, el investigador en seguridad que trabajaba para la Agencia Nacional de Seguridad (NSA) de los Estados Unidos, filtró la existencia de una serie de iniciativas y proyectos de gobierno con la ayuda de empresas para vigilar a la ciudadanía a través de medios digitales, el mundo entero se sacudió. Este fue uno de los primeros hitos, de varios otros posteriores, que marcaron la agenda para la protección de la privacidad a nivel global.

Los Estados modernos, por definición, tienen el monopolio de la fuerza, por lo que deben salvaguardar la integridad de sus ciudadanos/as y protegerlos/as de todo acto criminal. Esta perspectiva ha llevado a los gobiernos a adoptar cada vez más métodos y tecnologías no sólo para luchar contra la criminalidad, sino también para prevenirla. En una época en la cual los límites de la privacidad están dados, no tanto por la línea entre lo público y lo íntimo, sino por la propia capacidad de las tecnologías digitales para inmiscuirse en cada aspecto de nuestras vidas, se requiere repensar esa línea (Becker et al., 2018).

En ese marco, los gobiernos, independientemente de su línea ideológica, adoptan cada vez más tecnologías que puedan de alguna manera, prevenir incidentes de seguridad a través del monitoreo constante de lo que hacen o no los ciudadanos. Algunas de estas son:

- Programas de malware para guardar información de los usuarios, rastrear sus actividades (qué visitan cuando navegan en internet, a quién escriben, qué otros programas ejecutan). Estos programas no sólo son usados para vigilar criminales sino también se han usado con fines políticos y para espiar a periodistas y activistas. Tal caso se dio en México, donde el Gobierno instaló el software de vigilancia Pegasus[4] a varias personas. Además de este software, se supo el año 2016, que varios Gobiernos de América Latina habían comprado o habían entrado en tratativas para hacerlo, software de la empresa italiana Hacking Team (Pérez de Achá, 2016).
- Cámaras con reconocimiento facial y lectores biométricos. Estas son una amenaza para la privacidad pues, al tener capacidad de reconocer a la personas en lugares públicos y hacerles seguimiento continuo de actividades que realizan. Estos además tienen el problema de sus altos niveles de errores que han llevado a que se arresten a personas equivocadas. Con el surgimiento de tecnologías que usan rasgos del cuerpo humano para identificar a las personas, tales como sus huellas digitales, su aspecto facial, la forma de su silueta, entre varias otras, surge toda una nueva necesidad de legislación y mayor profundización sobre sus implicaciones.
- Aeronaves no tripuladas/drones. Estos pueden tener cámaras, lectores de calor u otros que registren información de las personas sin su consentimiento. Sus mayores funcionalidades son su fácil desplazamiento en varios tipos de entornos, rapidez y dificultad para ser detectados.
- IMSI-catchers. Son antenas falsas que capturan llamadas y tráfico de datos provenientes de móviles en un rango dado. Estos pueden ser usados en tres tipos de ataques: intercepción de la conexión entre antenas y dispositivos, locación de personas e interrupción del servicio (Electronic Frontier Foundation, 2019)

4 https://r3d.mx/2017/06/19/gobierno-espia/

Todas estas tecnologías y varias otras en desarrollo son invasivas y contrarias a los derechos humanos. Al realizar un monitoreo constante tienen efectos psicológicos en las personas pues se convierten en una suerte de panóptico de la vida diaria.

De acuerdo al Alto Comisionado de las Naciones Unidas para los Derechos Humanos, las tecnologías de vigilancia y la recopilación de datos personales tienen impactos importantes en la libertad de expresión, de reunión y asociación pacífica (Becker et al., 2018). Si la participación libre y sin prejuicios es una condición para la libertad de expresión, entonces la vigilancia se verá necesariamente reducida.

Por ende, el Sistema Interamericano de Derechos Humanos ha establecido la necesidad de verificar la adecuación de toda injerencia estatal o no estatal en la vida privada mediante estas tecnologías. La aplicación de las mismas debe ser legal, tanto en su sentido formal como material, además de necesarias y proporcionales (Becker et. al., 2018). Ello implica, además, que su aplicación debe ser expresa, taxativa, precisa y clara, a la vez que debe existir un orden judicial que establezca el alcance, duración y justifique el uso de estas, así como que exprese los organismos competentes para su uso.

Por lo anterior, es claro que en la aplicación de estas tecnologías, sobre todo en materia de seguridad ciudadana y del Estado es aún más necesaria la exigencia de un marco legislativo fuerte para la protección de la privacidad pues su ausencia, incide social y éticamente sobre libertades individuales antes descritas al combinar sistemas de identificación de videovigilancia, esto provoca que se pierda el anonimato público y con él, la posibilidad de movilidad libre en espacios públicos sin que seamos registrados y monitoreados (Diaz, 2018). Entonces, estos sistemas inhiben a las personas y afectan directamente a su derecho a libre circulación y expresión. Más aún, el efecto psicológico, puede ser múltiple, en tanto las personas que se encuentran en espacios vigilados, pueden llegar a desenvolverse de diferente manera y generar una personalidad distinta o auto restringirse.

EL CAPITALISMO DE LA PRIVACIDAD

Además de las razones de seguridad pública y/o ciudadana para justificar la hipervigilancia desde el Estado, existe otro problema quizás más grande que eleva la necesidad de normativa de protección a la privacidad: la comercialización de los datos personales.

Desde hace varios años se viene mencionando el alto valor comercial que tienen los datos. Ciertamente, estos son uno de los principales negocios detrás de la economía digital y son la principal fuente de ingreso de la mayoría de las grandes empresas de internet (Facebook y Google, por ejemplo), las cuales aparentemente ofrecen servicios gratuitos, pero en que en el fondo el precio que pagan usuarios y usuarias son los datos personales que brindan al hacer uso de los servicios.

La psicóloga social y profesora de Harvard Soshana Zuboff, describió este modelo como "capitalismo de vigilancia", el cual es la transformación de la experiencia humana como materia prima a datos sobre comportamiento, que son usados para mejorar servicios, alimentar las empresas de marketing, potenciar algoritmos de *machine learning*, entre otros (Zuboff, 2019).

Las empresas antes mencionadas llevan recopilando estos datos desde hace varios años y sólo recientemente, están siendo puestas en cuestionamiento y reguladas. No obstante, Facebook ya acumuló años de datos de sus más de 2 mil millones de usuarios/as, y Google ya digitalizó casi toda calle y casa en el mundo.

Más allá de que los datos sean extraídos y usados para mejorar los mismos servicios y bienes que consumimos, el problema es que se extraen más datos de los que realmente se necesitan, sin el consentimiento informado de las personas y para usos más allá de la experiencia de esas plataformas5.

La reproducción de ese modelo, de acuerdo a Zuboff (2019), requiere de 4 condicionantes: (1) Más capacidad de extracción, pero sobre todo de análisis; (2) El desarrollo de nuevas formas contractuales que permitan mayor automatización; (3) Personalización y deseo de customización de servicios; (4) Infraestructura tecnológica acorde al crecimiento del consumo. Este tipo de modelo de negocios no es único a estas empresas ni sólo afecta a una población, es global. Entonces, el modelo seguirá explorando maneras vulnerar aún más la privacidad. En ese sentido, se hace más que necesaria una garantía legal que fortalezca la capacidad de la ciudadanía de poner límites a los intereses de las empresas.

5 https://www.lanacion.com.ar/tecnologia/nada-es-privado-big-data-politica-oportunidad-nid2285255?utm_campaign=meetedgar&utm_medium=social&utm_source=meetedgar.com

Marco normativo de protección de la privacidad

LEGISLACIÓN INTERNACIONAL PARA LA PROTECCIÓN DE LA PRIVACIDAD

A nivel internacional, existe una extensa base legal para la protección a la privacidad. No obstante, gran parte está orientada a entender la privacidad en torno a la esfera de la intimidad, no así en relación a los desafíos que implican las nuevas tecnologías. Lo más avanzado, se halla en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, implementado en mayo de 2018, rige solamente a los países que son parte de ese bloque de integración regional europeo.

Un primer reconocimiento internacional a la protección de la privacidad se encuentra en la Declaración Universal de los Derechos Humanos (1948): "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" (Art. 12).

En el Sistema Interamericano, tenemos la Declaración Americana de los Derechos y Deberes del Hombre, la cual estipula que: "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, su reputación y su vida privada y familiar..." (Art. 5). De igual manera, la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica, ratifica que "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques" (Art. 11).

Más allá de su ámbito jurídico-normativo, lo cual brinda una potestad legal para poder proteger a la privacidad desde un contexto internacional y nacional, la privacidad es un valor y principio fundamental, y ante todo, un derecho humano. Empero, como se observó anteriormente, en la era digital la protección de la privacidad se halla afectada por dos tensiones: la seguridad pública y la mercantilización de datos. Por ende, se requieren perspectivas más actualizadas.

En América Latina, tenemos como referencia a la Red Iberoamericana de Protección de Datos que desde 2003, viene dando lineamientos para poder generar legislación adecuada en esta materia a sus países miembros. En el año 2016, esta entidad publicó sus estándares para el cumplimiento de la protección de datos personales6, entre los cuales se debe destacar al menos los siguientes tres puntos:

1. En el tratamiento de datos personales, el responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

2. El titular (la persona física a quien le conciernen los datos personales) tiene los siguientes derechos: acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen.

3. El encargado del tratamiento de datos personales, no deberá ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el responsable.

6 Disponible en: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

EL MARCO NORMATIVO BOLIVIANO

Existe una normativa de protección de la privacidad vigente en Bolivia, aunque no suficiente ni específica. Empecemos diciendo que el Estado Plurinacional de Bolivia, como miembro de la Organización de Estados Americanos, se adhiere a la Convención Americana de Derechos Humanos7 y reconoce jurisdicción tanto a la Comisión Interamericana de Derechos Humanos como a la Corte Interamericana de Derechos Humanos.

Conforme al Núm. IV del art. 13° de la Constitución Política del Estado: "Los tratados y convenios internacionales ratificados por la Asamblea Legislativa Plurinacional, que reconocen los derechos humanos y que prohíben su limitación en los Estados de Excepción prevalecen en el orden interno. Los derechos y deberes consagrados en esta Constitución se interpretarán de conformidad con los Tratados internacionales de derechos humanos ratificados por Bolivia".

Más en la legislación local, la protección de la privacidad se ha derivado, casi automáticamente, del derecho general a la privacidad de la Constitución Política del Estado, de sentencias constitucionales referidas a la autodeterminación informativa y de la normativa sectorial, como la Ley de Telecomunicaciones y la Ley de Servicios Financieros.

No obstante, esta es insuficiente pues "no es un marco transversal, (los datos personales) al tratarse de un derecho independiente, debería ser regulado por una ley orgánica que establezca principios, definiciones, responsables del tratamiento, establezca autoridades de control, funciones y procedimientos" (Karina Medinacelli). A su vez, la abogada experta en temas de privacidad Roxana Pérez del Castillo, menciona: "Se necesita regular específicamente todas las condiciones y características de los que significa la protección de datos, se necesita tener una instancia específica de monitoreo de todo lo que implica el alcance de protección de datos, también es necesaria la asignación de recursos".

Por un lado, la privacidad está regulada por la Constitución Política del Estado y la Ley No 254. En el Art. 21 de la CPE, se menciona: "Las bolivianas y los bolivianos tienen los siguientes derechos: b. A la privacidad, intimidad, honra, honor, propia imagen y dignidad". Otra norma dentro del Código Procesal Civil, regula las medidas cautelares específicas (Art. 336) para el caso en que las demandas sean de reconocimiento o restablecimiento del derecho a la intimidad de la vida personal o familiar, o en la preservación y aprovechamiento de la imagen o la voz de una persona.

7 Disponible en: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos_firmas.htm

El recurso de *Habeas data* está presente en los artículos 130 y 131 de la CPE: "I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad. II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa".

La Ley 254 (Código Procesal Constitucional) plasma y profundiza la autodeterminación informativa. Esta indica "el derecho de toda persona a conocer sus datos registrados por cualquier medio físico, electrónico, magnético o informático…". así como objetar objetar u obtener la eliminación o rectificación de éstos cuando contengan errores o afecten a su derecho a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación (Art. 58 a 63). De acuerdo a Roxana Pérez del Castillo, "la Constitución Política del Estado no reconoce la autodeterminación informativa, lo que reconoce es una acción constitucional de protección, es una acción de defensa constitucional para tratar de redimir y reivindicar alguna lesión de los derechos constitucionales".

También se puede mencionar la petición de *habeas data* en la vía administrativa o también llamada '*Habeas data* administrativo', que se encuentra regulado en el artículo 19 del Decreto Supremo 28168 de 2005. De acuerdo a este, en su Art. 19: "Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos o registros la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía, podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público". Dicha acción no sustituye a la acción constitucional establecida para tal efecto.

Por lo visto hasta aquí, de acuerdo a la jerarquía normativa, en Bolivia hay un tipo de orientación proclive a la reacción más que a la protección como garantía. "El *habeas data* es cuando tienes una amenaza o ha sido lesionado tu derecho, en esas circunstancias puedes empezar una acción de defensa. Se trata de una acción posterior" (Roxana Pérez del Castillo, entrevista personal).

Por otra parte, está también la normativa sectorial. Se pueden mencionar la protección de datos personales desde el sector de telecomunicaciones y en la Ley de Servicios Financieros (393).

La Ley 164 (Ley General de Telecomunicaciones y Tecnologías de la Información y Comunicación) señala en su Art. 54 los derechos que tienen los usuarios y usuarias, especificando en el numeral 6 el derecho a exigir respeto a la privacidad e inviolabilidad de sus comunicaciones, salvo casos expresamente señalados por la Constitución Política, y en su art. 56 establece la protección de los datos personales y la intimidad de usuarias y usuarios. Posteriormente, en su reglamentación, a través del Decreto Supremo 1391, establece en su artículo 176: "(I). El personal de operadores y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación está obligado a guardar secreto de la existencia o contenido de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios. (II.) Los operadores y proveedores de servicios están obligados a adoptar las medidas más idóneas para garantizar, preservar y mantener la confidencialidad y protección de los datos personales de los usuarios del servicio (...)".

En el Decreto Supremo 1793, esta protección se extiende a la firma y certificados digitales, mencionados en la Ley 164 de Telecomunicaciones y TIC. En este, se reconoce y describe los mecanismos de funcionamiento de la Acción de Protección de Privacidad. Estos instrumentos legales proponen un marco de protección, pero referidos a las telecomunicaciones y a un servicio específico, no así para todos los registros que impliquen datos personales, ni para el resto de actividades comerciales, políticas y de otra índole.

Con respecto a la Ley de Servicios Financieros (393), en el Art. 477, se establece la "Acción de protección de la privacidad". No obstante tiene un enfoque más desde el *habeas data* que desde la protección de datos personales, en tanto alega que "toda persona individual o colectiva que considera estar indebidamente o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por las entidades financieras, por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad o privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de la Privacidad prevista en el Artículo 131 de la Constitución Política del Estado".

Visto hasta aquí, si bien hay avances en cuanto a la protección de la privacidad, está se enfoca a la privacidad en tanto intimidad, y a los recursos propios de *habeas data*, con una perspectiva más reactiva (cuando el dato debe ser rectificado) que de garantía preventiva a la mala utilización. A todo esto, conviene mencionar que a partir de la creación de AGETIC, se generan nuevas necesidades al respecto.

De acuerdo al Decreto Supremo 2514 – que crea la AGETIC – en su Art. 19, dicha entidad coordina las entidades del sector público para lograr los servicios de interoperabilidad entre los datos e información que deben estar disponibles para el Gobierno electrónico. Se autoriza a que las entidades públicas proporcionen estos datos a la AGETIC.

En 2018, se generaron dos nuevas normas con capacidad de afectar la privacidad. En mayo de 2018, el gobierno modificó el Artículo 79° de la Ley del Órgano Electoral para permitir interoperar entre el Servicio de Registro Cívico (SERECI) y el Servicio General de Identificación (SEGIP), pero impidiendo además que éste último transfiera la información a terceros. Adicionalmente, dispone que las personas puedan realizar consultas y validar la información de identificación obrante en los registros.8

Ese mismo año se promulgó la Ley de Ciudadanía Digital (Ley 1080). Esta normativa crea la ciudadanía digital, cuyo principal impulsor era AGETIC, la cual 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". Asimismo, esta implica que las entidades públicas y privadas que presten servicios públicos delegados por el Estado, en todos los Órganos y niveles de gobierno, "puedan prescindir de la presencia de la persona interesada y de la presentación de documentación física para la sustanciación del trámite o solicitud." (Art. 4). Esta misma norma, en su Art. 12, prevé el principio de finalidad para cualquier tratamiento de datos personales realizado por entidades públicas. Examinaremos en el capítulo siguiente algunas deficiencias y potenciales vulneraciones de este estatuto.

En ese sentido, como argumenta la experta Karina Medinacelli, la misma dispersión y la falta de una normativa, afecta al "desconocimiento del sector público y privado de normativa que ya está vigente y de jurisprudencia, tanto de la protección de datos personales, la privacidad y la intimidad". La implementación de nuevos procesos que requieren incluir información sensible, deberían estar enmarcadas en una Ley que contemple sus alcances y prevenga de su mal utilización.

8 Disponible en: http://anterior.gacetaoficialdebolivia.gob.bo/normas/verGratis_gob/157730

PROCESO CREACIÓN DE LEY DE PROTECCIÓN DE DATOS PERSONALES

Cabe decir que Bolivia es uno de los pocos países de la región que aún no tiene una Ley de Protección de Datos Personales, pese que la mayoría de los países vecinos ya tienen leyes que datan de hace 20 años (como es el caso chileno).

Desde el año 2018 comenzó el debate público para empezar a desarrollar una normativa de esa índole. Este ha sido en alguna medida, impulsado por tres principales motivaciones. Primero, en lo jurídico, de acuerdo a la experta Karina Medinacelli: "se debe considerar que la protección de datos personales es un derecho independiente de la privacidad y la intimidad, que a pesar de existir jurisprudencia que data del año 2004, está no contempla varias definiciones y tipos de datos, y que se encuentra rezagada con respecto a normativa internacional". Paralelamente, el proceso de modernización del aparato público – a través de por ejemplo el programa de Gobierno electrónico – ha generado justamente necesidad de hacer una tipificación más estricta de los datos en función a la autodeterminación de la información y su tratamiento. Segundo, la creciente necesidad de proteger la privacidad de las personas, ante un contexto cada vez más preocupante con respecto al uso de las tecnologías – coincidiendo con el caso de Cambridge Analytica, por ejemplo. Tercero, a nivel político, el anuncio de crear una modificación a la normativa electoral para generar interoperabilidad, los partidos empezaron a generar desconfianza sobre el alcance del uso de los datos personales en el Estado.

Se han impulsado al menos 3 procesos para la creación de un anteproyecto de ley. El primero fue a partir de la diputada nacional, Giovana Jordán Antonio, del Partido Demócrata Cristiano. Esta diputada generó un anteproyecto de ley en diciembre de 2018 y ha convocado algunos foros ciudadanos para conversar con ciudadanos y ciudadanas.

A su vez, la Fundación Internet Bolivia generó otro proceso de construcción participativa a través de 8 eventos realizados en las 4 principales ciudades de Bolivia (La Paz, El Alto, Cochabamba y Santa Cruz), y con apoyo de otras 12 organizaciones que participaron en partes del proceso. En estos eventos se logró generar un borrador del anteproyecto de Ley de protección de datos personales, el cual fue luego presentado por ventanilla única en la Asamblea Legislativa Plurinacional en abril de 2019.

A su vez, el Gobierno nacional ha impulsado un propio proceso a través de AGETIC. Esta entidad estatal empezó un proceso de consulta sectorial en cuatro ciudades de Bolivia (La Paz, El Alto, Cochabamba y Santa Cruz), de acuerdo a una de las consultoras de esta iniciativa, Karina Medinacelli, ésta incluyó grupos empresariales, LGTBI, movimientos sociales, activistas individuales y otros sectores comerciales. convocó al menos dos reuniones, a miembros de la sociedad civil, en calidad de expertos/as para la elaboración del proyecto de ley de esta normativa. También, contrató a dos consultores para llevar a cabo procesos consultivos y elaborar los mínimos comunes. Este proceso es similar al que ha sido descrito en Chile, en el cual se llamaron instancias de opinión de la sociedad civil sobre los criterios que la ley debería cumplir, aunque estas no tienen un carácter resolutivo (Voilier, 2017).

POLÍTICAS PÚBLICAS CON CAPACIDAD DE AFECTAR A LA PRIVACIDAD

A pesar de no existir una normativa específica de protección de datos personales en Bolivia, se crearon varias políticas públicas y proyectos con posibilidad de afectar potencialmente la privacidad de toda la ciudadanía. Si bien, al momento de escribir este documento, se desconoce si las mismas seguirán en el mismo rumbo (debido al cambio de gestión de gobierno), estas dejaron bases normativas e infraestructura instalada que es necesaria analizar.

Entre las tres políticas públicas, se encuentran la ciudadanía digital, aprobada, y el programa BOL 110, en implementación de su primera fase. Existe una tercera se hallaba en proceso de discusión: el proyecto de Ley de protección de datos personales (que ya fue abordado).

LEY DE CIUDADANÍA DIGITAL

La ciudadanía digital se encuentra plasmada, como se mencionó, en la Ley 1080 que fue promulgada en julio de 2018. De acuerdo a esta, para ejercer la ciudadanía digital, es necesario realizar un proceso de registro y autenticación para recibir una credencial que sólo puede ser usada por el interesado/a (Art. 5).

Este registro consiste en: darse de alta en el sistema con una huella digital y fotografía, firma digital y confirmación vía correo electrónico y SMS. Desde ese aspecto, la Ley de ciudadanía digital sigue una tendencia vista en varios otros países que es la de proveer una sola identidad compatible e indivisible entre la identidad natural de un/a ciudadano/a de un Estado y aquella de tipo digital. Es decir, se hace una compatibilización y/o asociación de datos entre la persona natural y los registros online a través del uso de datos personales.

Con ello, la normativa busca facilitar la realización de trámites, acceder a servicios públicos, posibilitar la participación y control social en espacios creados por el Estado, y cualquier otro que llegue a generar en un futuro próximo de acuerdo a la normativa (Art. 6). Esto supondría mejorar los servicios de atención y acelerar la burocracia. Así también, normas como esta pueden contribuir a uno de los Objetivos del Desarrollo Sostenible (ODS) de las Nacionales Unidas, por la cual, los Estados deben poder proveer identidad legal a sus ciudadanos/as hasta el 2030 (Objetivo 16.9).

No obstante, existen varios problemas asociados con este tipo de implementaciones y que ha llevado a que sea rechazado en varios países. Algunas de estas consideraciones son las siguientes (Access Now, 2018):

- Fortalecen la capacidad de control de los Estados sobre los ciudadanos/as. Esto pues el Estado puede asociar más fácilmente todo tipo de acciones realizadas con la identidad de quien los hizo. Si bien esto ayuda en temas de seguridad pública, la hipervigilancia es nociva para varios derechos humanos.
- La concentración de todos los datos de identificación en un solo mecanismo, en este caso, una cédula de identidad electrónica, puede ser riesgoso en términos de ciberseguridad, pues una sola brecha de datos, expone íntegramente a todas las personas registradas.
- El uso de datos biometrizados, como fotografías, estructura del rostro y huellas digitales, eleva los peligros de ciberseguridad mencionados. A su vez, estos son datos sensibles que deben ser regulados con normativa que brinde garantías sobre su uso adecuado.
- Las autoridades y funcionarios encargados de su manejo deben estar debidamente regulados debido a posibles abusos.

La Ley de Ciudadanía Digital boliviana posee varios de estos riesgos. Por ejemplo, usa datos biometrizados (fotografías y huellas digitales); así también, de acuerdo al Art. 5, las instituciones públicas y privadas que presenten servicios públicos, deberán compartir datos a partir de mecanismos de interoperabilidad que no son transparentes. Lo anterior implica centralizar datos personales y ponerlos a disposición de pocas entidades que manejan el sistema de registro y verificación. Hay una relación muy estricta entre datos biométricos y derecho a la privacidad y protección de datos personales. Un problema no resuelto tiene que ver con el carácter automatizado de recolección sin consentimiento previo (Díaz, 2018). Al mismo tiempo, como contempla la experta boliviana Karina Medinacelli, la implementación de este proyecto generará nuevos tipos de datos personales que requerirán propios principios y reglamentaciones para ser protegidos adecuadamente.

Sin garantías de protección de privacidad, esto resulta riesgoso, pues se puede convertir en una carta abierta para que información sobre los usuarios circule y se transmita entre instituciones sin restricciones.

Además de esos dos aspectos, de acuerdo a un análisis realizado por el investigador Pablo Voillier existen las siguientes cuestionantes:

- No existe claridad sobre la referencia "prestación de servicios" pues existen varias circunstancias de relación entre la administración y los administrados que no son necesariamente encuadrables en relaciones de servicios. Están, por ejemplo, otras categorías de manejo electoral, emergencias públicas, entre otras (Pablo Voillier, 2018 – inédito).
- La ley no recoge como objetivo, el respeto de otros derechos civiles y políticos, o económicos, sociales y culturales, que pueden resultar implicados en su aplicación. Particularmente llamativa es la falta de referencia a los derechos a la privacidad, libertad de pensamiento y expresión, entre otros. Esto brinda un cierto grado de inmunidad para la implementación de servicios sin atender estos derechos. Aunque estos se encuentren garantizados en la Constitución Política del Estado, sin una referencia específica, es necesario referenciarlos, sobre todo si es una ley sobre ciudadanía (Pablo Voillier, 2018 – inédito).
- La ley impone a la población la obligación de registrarse para obtener sus credenciales de ciudadanía digital que le habilitarán en la interacción con el Estado. No se contempla aquí tampoco, como no se hacía en los objetivos de la ley, un compromiso con el respeto "a la privacidad, intimidad, honra, honor, propia imagen y dignidad" (Art. 21 de la Constitución Política del Estado). Los lineamientos técnicos resultan pobres sustitutos de consideraciones de privacidad, que a lo menos urge sean explicitadas como compromisos del Estado en el reglamento que se dicte para acompañar la implementación de la Ley (Pablo Voillier, 2018 – inédito).
- La transmisión de datos entre entidades sin restricciones y/o consideraciones, puede resultar desproporcionada. Primero, porque no toda la información compartida puede ser de pertinencia para el ejercicio de funciones de una entidad con respecto a otra; segundo, porque puede contener datos sensibles que puede dar lugar a abusos por parte de algunas entidades y autoridades; y tercero, por que incrementa los puntos en que la información puede ser objeto de acceso indebido por terceros.
- La ley abarca la interoperabilidad con entidades privadas que presten servicios públicos, abriendo con ello nuevamente en forma desorbitada el riesgo de que la información sea compartida con terceros respecto de los cuales la capacidad de control y supervisión acerca del adecuado uso será aún más limitada de parte del Estado.

Para que este tipo de programas sean realmente empoderantes para la ciudadanía, estos deben estar basados en la privacidad por diseño y la existencia previa de una institucionalidad que garantice su adecuado uso. Su centralización en una sola organización y sistema, afecta la posibilidad de que exista contrapesos a usos interesados y abusivos. La organización Access Now (2018) hace las siguientes recomendaciones para este tipo de programas, varias de las cuales la Ley de Ciudadanía Digital no necesariamente cumple. Estas son:

- Disposición a que los sistemas sean debidamente auditados por entidades externas, imparciales y con toda la transparencia posible para la sociedad civil.
- Garantías legales con respecto a usos abusivos, a través de una Ley de protección de datos personales.
- Consentimiento voluntario, expreso e informado.
- Creación de mecanismos independientes de observancia de la implementación de este servicio.
- Limitar al mínimo posible, los datos colectados y usados. Los datos a ser compartidos deberían ser los estrictamente necesarios.
- Brindar derecho a la población a rectificar sus datos o denunciar datos falsos.
- Existencia de mecanismos robustos de protección de la información y/o ciberseguridad.
- Evitar la centralización de datos.
- Implementar cifrado en todas las transacciones.
- Crear incentivos para denunciar posibles vulnerabilidades y abusos para evitar que estas sean mal aprovechadas.
- Tener protocolos claros para casos de exposición y vulneración de información.

Parte de estas falencias y observaciones mencionadas, pueden llegar a ser subsanadas a través de una adecuada reglamentación. Pero se necesita a su vez, una legislación fuerte que proteja los derechos a la privacidad y los datos personales de la ciudadanía.

PLAN NACIONAL DE SEGURIDAD CIUDADANA-BOL 110

Desde el año 2012 se empezó a implementar el nuevo Plan Nacional de Seguridad Ciudadana en Bolivia. Este se encuentra normado a través de la Ley 264. Esta normativa, dedica el Capítulo IV, a medidas de prevención tecnológica, las cuales incluyen "sistemas de monitoreo y vigilancia electrónica para el control y prevención de delitos, faltas y contravenciones" (Art. 47), cámaras de seguridad en "empresas prestadoras de servicios públicos, entidades financieras bancarias, las entidades públicas y centros de esparcimiento público y privado con acceso masivo de personas" (Art. 50). La Policía Boliviana tendrá acceso a las grabaciones y sistemas con fines investigativos. A su vez, el Ministerio de Gobierno y la Policía Boliviana suscribirán convenios con empresas y cooperativas telefónicas para el uso de su infraestructura de red para el funcionamiento de los sistemas de seguridad (Art. 51).

En el marco de este Plan, se creó el programa BOL-110, el cual fue puesto en marcha en agosto de 2019. Este programa se creó sin una ley o reglamento previo[9].

El programa BOL-110 fue encargado a las empresas chinas CEIEC[10] y Huawei. Estas empresas son responsables de construir uno de los sistemas de reconocimiento facial más poderosos a nivel global, con la capacidad de identificar a cualquier persona de entre 1,3 mil millones de ciudadanos/as en 3 segundos, y apuntando a una precisión del 90%[11] Así también, tiene capacidades para combinar múltiples tipos de tecnología con Inteligencia Artificial (Oxford Analytica, 2019).

En Bolivia, el proyecto de seguridad ciudadana implementado por CEIEC y Huawei implicó una inversión de más de 105 millones de dólares. Este consiste en la instalación masiva de cámaras de video vigilancia de alta velocidad y resolución en ciudades, las cuales tendrían capacidad de reconocimiento facial, uso de 5 drones de tipo militar, 60 equipos de radio-comunicación, desplazamiento de 100 vehículos patrulleros equipados con cámaras, 2.500 alarmas comunitarias, y 1.900 equipos de taxi seguro.[12] Más allá de todos los aspectos positivos que podría implicar este programa en cuanto a lucha contra el crimen, el uso de las tecnologías de reconocimiento facial y el despliegue masivo de sistemas de monitoreo dan lugar a posibles abusos.

9 Al momento de escribir este artículo – octubre de 2019 – la ley para su implementación era introducida en la Asamblea del Estado Plurinacional, no obstante su discusión fue suspendida debido a los conflictos políticos posteriores a las elecciones nacionales del 20 de octubre.

10 CEIEC es una empresa subsidiria de la Corporación China de Electrónicos (CEIEC), una de las empresas más grandes de defensa de ese país.

11 https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any

12 https://www.urgentebo.com/noticia/evo-pone-en-marcha-el-sistema-integrado-de-seguridad-ciudadana-bol-110

De acuerdo al proyecto de Ley de Sistema Integrado de Seguridad Ciudadana – BOL 110 (PL N° 441/2019-2020), que estaba en discusión en la Asamblea Legislativa, además de las capacidades de capturar información a través de diversos canales de tecnología de vigilancia, tendría serias implicancias en cuanto a la interoperabilidad de datos en el Estado. Así, en el Art 23 del proyecto, se menciona que las instituciones públicas deberán implementar mecanismos de interoperabilidad de información para el desarrollo de acciones del SISC-BOL 110, mecanismos que debían ser implementados y supervisados por AGETIC. Este artículo, incluye prácticamente todas las instituciones públicas, por lo cual puede resultar desproporcionado. Por otro lado, los requerimientos de información de una persona determinada, en caso de que sea a partir de la Comisión Interministerial de Seguridad Ciudadana, son obligatorios, por lo que las entidades públicas no podrían negarse a entregar información (Art. 9). Finalmente, el Proyecto de Ley no da ningún margen de control y/o fiscalización, en tanto, de acuerdo al Art. 25, toda información generada por el SISC-BOL 110, es confidencial.

Por tanto, este sistema, como se observó ya con respecto a la Ciudadanía Digital, podría tener algunas implicaciones preocupantes como la concentración del manejo de datos personales (más allá de los absolutamente necesarios), falta de garantías contra usos abusivos y casi ninguna mención a la protección y seguridad de la información.

También, es preciso mencionar otros puntos que generan desconfianza con respecto a este sistema. En primer lugar, la empresa encargada de su implementación fue cuestionada en otros países. Esta empresa ha creado los sistemas de seguridad pública de Ecuador, Angola, Venezuela, entre otros países.

En Ecuador se instaló el sistema ECU-911, similar al instalado en Bolivia. A varios años de la instalación de este sistema, no se ha reportado una reducción del crimen porque este depende de varios factores, más allá de la vigilancia. Empero, activistas han expresado su miedo a que tal capacidad de vigilancia permita incrementar la persecución y represión por parte del gobierno, como de hecho se evidenció en algunos casos en el mencionado país13. Los sistemas de vigilancia de China, han sido también observados por usar técnicas de integración total de datos de video, locación, comunicaciones telefónicas, transacciones comerciales, entre otras; estas capacidades pueden ser usadas para otros temas además de persecución criminal, como el monitoreo de actividades y comportamientos ciudadanos (Centro Estratégico de Estudios Internacionales, 2018). Otro aspecto relativo a las tecnologías de vigilancia de China es que a diferencia de otros contratistas, las empresas chinas son más difíciles de fiscalizar debido al poder político que detenta ese país, así como las restricciones legales.

13 https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Más allá de los problemas de los antecedentes con la empresa contratista, las tecnologías de vigilancia masiva para fines de seguridad presentan serias preocupaciones en cuanto a la vulneración de derechos humanos (Derechos Digitales, 2018). Dependiendo el tipo de tecnología, una de las más observadas es el reconocimiento facial (una de las principales características de BOL-110). El reconocimiento facial utiliza algoritmos para asociar patrones o rasgos biométricos de una persona con respecto a una base de datos de registros, y así dar, por ejemplo, con personas más buscadas por delitos o personas desaparecidas. No obstante, se ha observado su alta tasa de error y porcentajes de falsos positivos que llevaron a arrestar personas inocentes en Buenos Aires y Londres – con 96% de las personas mal identificadas (ADC, 2019). Además de estos posibles errores, preocupa que este sistema pueda ser usado para identificar adversarios políticos, activistas u otros y hacerles seguimiento constante o incluso dar lugar a cometer delitos contra su integridad.

RIESGOS DE CIBERSEGURIDAD EN EL ESTADO

Gran parte de los datos personales de la población se encuentran alojados en servidores y páginas web del Estado. A nivel global, se tienen múltiples antecedentes en los cuales servidores de gobiernos fueron atacados y vulnerados, extrayéndose de estos bases de datos con información sensible sobre la ciudadanía. El caso más reciente es el de Ecuador, en el cual se encontró datos personales sensibles expuestos de casi todos los ciudadanos de ese país (17 millones de personas)[14]. Este se suma a una serie de otros casos en México[15], Filipinas[16], Estados Unidos, entre otros. La ciberseguridad de la infraestructura del Estado, es una materia pendiente y que puede afectar a toda la ciudadanía.

La infraestructura tecnológica del Estado boliviano ha presentado a lo largo de los años varias vulnerabilidades. Hasta noviembre de 2019, estás podían ser detectadas fácilmente sin la necesidad de realizar pruebas de penetración de sistemas – pentesting – y/o auditorías de seguridad.

14 https://www.eluniverso.com/noticias/2019/09/16/nota/7521358/masiva-filtracion-online-informacion-casi-cada-ciudadano

15 https://arstechnica.com/information-technology/2016/04/millions-of-mexican-voter-records-leaked-amazon-cloud/

16 https://www.wired.co.uk/article/philippines-data-breach-comelec-searchable-website

Las mismas representaban un potencial riesgo pues no ofrecen garantías para sus usuarios, ni necesariamente cumplen con todas las medidas de seguridad para evitar que información de la población boliviana se exponga y/o se filtre. De hecho, se han venido registrando varios casos individualizados de mala utilización de sistemas estatales, "dumps" – colecciones de datos subidas a ciertos repositorios – a partir de hackeos de páginas web y existencia de páginas gubernamentales sin conexión cifrada y huecos de seguridad.

Estos problemas, en cualquier Estado, ponen en riesgo la información de la ciudadanía. Esto se agrava si el Estado busca generar sistemas complejos de identidad digital y repositorios de bases de datos concentrados como la ciudadanía digital.

CASOS DE EXPOSICIÓN Y FILTRACIONES

Aún no existe ningún registro pormenorizado y sistemático de los casos de exposición de datos personales desde páginas, repositorios o desde los mismos funcionarios del Estado boliviano. Sólo hay pocos casos que son conocidos por que se compartieron por plataformas de redes sociales o en medios de comunicación masivos y en los cuales se demostró la facilidad con los que se puede acceder a datos personales sensibles en sistemas del Estado o abusos que se pueden cometer sin la existencia de protocolos o garantías.

Durante el 2019, se registraron por ejemplo dos casos que involucraron el uso de los números de placa de autos para exponer a personas. El primero corresponde a un señor que fue filmado botando basura a un río; usuarios buscaron la placa expuesta en la foto, la ingresaron al sistema de registro de deudas y accedieron a varios de sus datos personales incluyendo su dirección domiciliaria, posteriormente, esta información fue compartida en Facebook a través de una captura de pantalla para denunciarlo. El segundo implicó una situación similar pero afectando a una ex diputada nacional. El mensaje publicado además ejercía violencia al aludir a su intimidad, exponía el número de placa, detalles de sus deudas y otros datos personales.

Ambos casos demostraron la facilidad de a través de sólo tener un dato personal se puede generar grandes brechas de acceso a datos más sensibles que pueden poner en riesgo a las personas afectadas. Ciudadanos pueden buscar tomar represalias contra estas personas, buscándolas en sus casas o usando los datos expuestos para otros fines.

Otro dato que ha sido denunciado fue la captura de datos de menores de edad que se ha dado a través del programa "Yo no soy X" del Órgano Electoral Plurinacional (OEP), éste no ha tenido el cuidado de informar debidamente a padres y tutores para recabar su consentimiento para tomar registros biométricos de jóvenes de entre 16 y 18 años, a pesar que en declaraciones públicas han asegurado que se pedía consentimiento de padres y tutores. Se han recibido denuncias internas en canales digitales de la Fundación Internet Bolivia de padres de colegios de La Paz en sentido que no recibieron información ni se les solicitó su consentimiento.

De parte de la OEP, también se ha hecho manifiesta la posible vulneración que puede implicar la publicación de los números de documentos de identificación – carnets – asociados a los nombres completos y los recintos de votación. Esta información es impresa en todos los periódicos de Bolivia y accesible a través del sistema "Yo Participo" (http://yoparticipo.oep.org.bo/aplicaciones/consulta). El Órgano Electoral Plurinacional de Bolivia, de quien depende esto, no tomó en cuenta ningún tipo de regulación jurídica tal como condiciones de uso o políticas de privacidad, desde un doble ángulo este servicio electrónico puede ser utilizado como un perjuicio en manos de un caso de acoso o persecución con lo cual se crean riesgos para las personas.

Por otra parte, el Centro de Gestión de Incidentes Informáticos (CGII), dependiente de AGETIC, el primer semestre del año 2018 se atendió al menos 112 incidentes. De estos, 4% fueron exposiciones de datos personales, aunque varios otros incidentes podrían haber afectado indirectamente a esto (62% eran configuraciones de seguridad incorrectas, por ejemplo. A su vez, 53% de los casos fueron intrusiones a cuentas y/o sistemas y 7% compromiso de información.

Más allá de los registros oficiales, es posible hacer búsquedas en repositorios abiertos usados por programadores y hackers maliciosos para subir información para el resto de usuarios y encontrar registros de vulneraciones/infiltraciones no autorizadas a páginas estatales. A través de una búsqueda en la plataforma Pastebin se encontró 6 de estos casos. En estos, se puede encontrar contraseñas, correos institucionales, registros de acceso a servidores, listas de routers de wifi, entre otros a entidades tan importantes como el Ministerio de la Presidencia, AGETIC, Entel y la Policía Nacional. Estas vulneraciones demuestran las debilidades de varios sistemas de información del Estado.

ENTIDAD	PÁGINA WEB	FECHA	INFORMACIÓN EXPUESTA	LINK
MINISTERIO PRESIDENCIA	www.presidencia.gob.bo	15/12/2011	contraseñas	https://pastebin.com/5mBWrTvs
MINISTERIO PRESIDENCIA	www.comunicacion.presidencia.gob.bo	30/04/2013	Listas de envío, correos, contraseñas	https://pastebin.com/hK8gmuud
AGETIC/ADSIB	www.agetic.gob.bo	31/03/2018	usuarios, contraseñas	https://pastebin.com/3XSrLVVL
ENTEL	www.entel.bo	27/09/2011	Contraseñas wifi	https://pastebin.com/QN2K874p
POLICÍA NACIONAL	www.policia.bo	sin fecha	usuarios, contraseñas	http://pastehtml.com/view/b8q95vm4d.html
MINISTERIO PRESIDENCIA	www.presidencia.gob.bo	14/09/2011	usuarios, contraseñas	https://pastebin.com/UH6wNafx

PÁGINAS WEB DEL ESTADO

Un gran porcentaje de páginas estatales no tiene buena medidas de seguridad ni protección para los usuarios que los visitan. Esto pudo comprobarse a través de 3 ejercicios ejecutados entre septiembre y octubre de 2019: 1. Verificar que las páginas web de páginas estratégicas del Estado tengan certificados de seguridad, 2. Contabilizar la cantidad de rastreadores de navegación que tienen instalados, y 3. Verificar que las páginas tengan ocultas sus puertas de acceso y sus subpáginas sensibles ocultas.

Se tomaron 24 entidades de importancia estratégica en el marco del Estado para evaluar tanto sus niveles de seguridad como la protección que ofrecen a los usuarios/as. Desde esa perspectiva, existe un tipo de cifrado de comunicaciones entre el sitio web y la persona que se conecta a éste, llamado HTTPS (Hypertext Transfer Protocol Secure). Este protocolo de cifrado crea una comunicación segura entre el usuario y el servidor en el cual el sitio está alojado. Al establecerse una conexión cifrada y segura. No obstante, menos del 25% de las páginas poseía este protocolo de seguridad (y varias de ellas poseen certificados no validados), por lo que a la gran mayoría de páginas, el/la ciudadana se exponía con sólo navegar a través de ellas. A esto se suma la gran cantidad de rastreadores que tienen las páginas estatales. Tener un rastreador implica que la página web puede registrar todos tus datos de navegación. Entidades como el Ministerio de Cultura y Turismo, Ministerio de Deportes, Ministerio de Justicia, Tribunal Supremo Electoral, poseían más de 10 rastreadores distintos, estos rastreadores son en sí mismos una falta a la privacidad de la ciudadanía desde el propio Estado.

Finalmente, se verificó que las páginas web hayan ocultado debidamente sus links de acceso a las consolas de gestión de contenidos u otros de tipo sensible. Esto se hizo buscando el fichero "robots.txt" de cada página. Sólo 33% de la muestra del ejercicio lo hizo, mientras que el resto, tiene este archivo accesible, por lo que básicamente se podría ingresar a los archivos de la página en cuestión dentro del servidor dónde se aloja la misma.

ENTIDAD	PÁGINA WEB	CERTIFICADO SEGURIDAD	TRACKERS	VULNERABILIDADES
MINISTERIO DE TRABAJO, EMPLEO Y PREVISIÓN SOCIAL	www.empleo.gob.bo	No	1	Consola de administración accesible y otras puertas
MINISTERIO DE COMUNICACIÓN	https://comunicacion.gob.bo	Sí	6	Consola de administración accesible y otras puertas
MINISTERIO DE RELACIONES EXTERIORES	http://www.cancilleria.gob.bo	No	4	Links a páginas ocultas
MINISTERIO DE LA PRESIDENCIA	http://www.presidencia.gob.bo/	No	6	Links a páginas ocultas
MINISTERIO DE GOBIERNO	http://www.mingobierno.gob.bo/	No	8	Links a páginas ocultas
MINISTERIO DE DEFENSA	http://www.mindef.gob.bo/mindef/	No	8	Consola de administración accesible y otras puertas
MINISTERIO DE CULTURAS Y TURISMO	https://www.minculturas.gob.bo/	Sí	10	Links a páginas ocultas
MINISTERIO DE DEPORTES	http://www.mindeportes.gob.bo/	No	11	Links a páginas ocultas
MINISTERIO DE DESARROLLO PRODUCTIVO Y ECONOMÍA PLURAL	https://produccion.gob.bo/	No	2	Links a páginas ocultas
MINISTERIO DE DESARROLLO RURAL Y TIERRAS	https://www.ruralytierras.gob.bo/	No	8	Links a páginas ocultas
MINISTERIO DE ECONOMÍA Y FINANZAS	https://www.economiayfinanzas.gob.bo/	No	5	Links a páginas ocultas
MINISTERIO DE EDUCACIÓN	https://www.minedu.gob.bo/	No	11	Consola de administración accesible y otras puertas
MINISTERIO DE ENERGÍA	https://www.minenergias.gob.bo/	No	0	
MINISTERIO DE HIDROCARBUROS	https://www3.hidrocarburos.gob.bo/	No	3	
MINISTERIO DE JUSTICIA	https://www.justicia.gob.bo/	No	10	
MINISTERIO MEDIO AMBIENTE Y AGUA	https://www.mmaya.gob.bo/	No	4	Consola de administración
MINISTERIO DE MINERÍA Y METALURGÍA	http://www.mineria.gob.bo/	Sí	9	
MINISTERIO DE OBRAS PÚBLICAS, SERVICIOS Y VIVIENDA	https://www.oopp.gob.bo/	No	9	Links a páginas ocultas
MINISTERIO DE PLANIFICACIÓN DEL DESARROLLO	http://www.planificacion.gob.bo/index	Sí	3	
SERVICIO DE REGISTRO CÍVICO	https://sereci.oep.org.bo/	No	5	
ÓRGANO ELECTORAL PLURINACIONAL	https://www.oep.org.bo/	No	11	
SERVICIO IMPUESTOS NACIONALES	https://www.impuestos.gob.bo/	Sí	2	
CÁMARA DE DIPUTADOS	http://www.diputados.bo/	No	4	Consola de administración accesible y otras puertas
CÁMARA DE SENADORES	https://web.senado.gob.bo/	Sí	3	Consola de administración accesible y otras puertas

Balance y recomendaciones finales

Este documento fue escrito en un momento de transición política, entre la gestión del Gobierno de Evo Morales, la anulación de las elecciones de 2019 y el inicio de las nuevas campañas para las elecciones de 2020. En esa línea, se inscribe en un proceso de indefinición sobre la continuación o no de las políticas descritas. Más allá de eso, lo que este informe busca demostrar es que el Estado boliviano no tiene un enfoque normativo, político e infraestructural para la protección de la privacidad de la ciudadanía.

Se dice esto, en base a tres argumentos:

Primero, la legislación no es suficiente. Existe reconocimiento a la privacidad (desde el enfoque de la intimidad personal), avances en materia de *habeas data*, pero no así en términos de la protección de datos personales, la cual es un derecho en sí mismo, pero necesario para tener un marco amplio de protección de la privacidad.

Segundo, se generaron políticas públicas y sistemas dentro del Estado que requieren procesar datos personales y pueden brindar acceso irrestricto a algunas autoridades y funcionarios a la privacidad de varias personas. No obstante, funcionan sin reglamentaciones y garantías para limitar usos abusivos.

Tercero, la infraestructura del Estado, en cuanto a la seguridad de los sistemas de información, muestra fragilidad aún en los aspectos más básicos. Este fue, de hecho, uno de los argumentos de vicio que llevaron a la anulación de las elecciones de 2019. La ciberseguridad, en ese aspecto, debe ser vista como una garantía que el Estado debe brindar a la ciudadanía con respecto a cómo se maneja y trabaja la información de todos los bolivianos.

Entonces, hacia un futuro a mediano plazo, se hace las siguientes recomendaciones que deben ser atendidas por el siguiente Gobierno:

- Crear y aprobar una Ley de protección de datos personales, compatible con la normativa vigente, que recoja los aprendizajes y necesidades recopiladas a través de las organizaciones de la sociedad civil que ya vienen trabajando en esta área. Esta debería tener en cuenta leyes como el Reglamento General de Protección de Datos europeo y legislación similar en otros países. A su vez, debería cumplir con los estándares de la Red Iberoamericana de Protección de Datos, con respecto a los derechos ARCO (acceso, rectificación, cancelación, oposición) además del derecho de portabilidad de sus datos, e incluir la creación de una entidad autónoma que vigile y regule esos procesos. Esta ley debería generarse antes de acelerar o profundizar proyectos como el BOL-110 o la ciudadanía digital.
- Reglamentar las nuevas tecnologías incorporadas al Estado en el marco de los proyectos ya mencionados (Ciudadanía digital y BOL-110). Esto, tanto en sus formas de uso, alcances, responsabilidades de las entidades y funcionarios a cargo y medidas de seguridad. Al respecto, es importante entender que estas tecnologías plantean serios desafíos que van más allá de lo estipulado en un principio en los proyectos de ley de datos personales, como por ejemplo, el manejo de datos biométricos.
- Crear y aplicar estándares de ciberseguridad dentro del Estado. El Estado resguarda los datos personales de toda la ciudadanía boliviana, por lo que es necesario que se cumplan con todas las medidas posibles en cuanto a seguridad de la información para protegerlos. Entidades como AGETIC tienen un rol estratégico para velar que las medidas de seguridad sean implementadas en todos los niveles del Estado de manera programática y preventiva, más que reactiva (cuando ya sucedió el incidente). Por otra parte, debe hacerse una revisión sobre cómo las páginas y sistemas del Estado brindan información pública sobre otros ciudadanos.

Bibliografía

Access Now. (2018). National Digital Identity Programmes:What's next? Access Now Policy Paper. Accesible en (Última fecha de acceso: 08/12/2019): https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

Becket, S. Canales, M.P., Lara J.C. (2018). La construcción de estándares legales para la vigilancia en América Latina. Parte I: algunos ejemplos de regulación actual en América Latina Accesible en (Ultima fecha de acceso: 08/12/2019): https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-I.pdf

Chan, M., Kessel, J., Mozur, P. (2019). Hecho en China y exportado a Ecuador: el aparato de vigilancia estatal. New York Times. Accesible en (Última fecha de acceso: 08/12/2019): https://www.nytimes.com/es/2019/04/24/ecuador-vigilancia-seguridad-china/

Chen, S. (2017). China to build giant facial recognition database to identify any citizen within seconds. . Accesible en (Última fecha de acceso: 08/12/2019): https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any

Chiriboga, G. (2001).La acción de amparo y de *hábeas* data: garantías de los derechos constitucionales y su nueva realidad jurídica. Quito, AAJ/ILDIS.

Díaz, M. (2018). El cuerpo como dato. Derechos Digitales. Accesible en (Ultima fecha de acceso: 08/12/2019): https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

Electronic Frontier Foundation (2019). Cell-Site Simulators/IMSI Catchers. Accesible en (Última fecha de acceso: 08/12/2019): https://www.eff.org/es/pages/cell-site-simulatorsimsi-catchers

Faliero, C., Iglesias, R. (2018). Operación y uso de herramientas de privacidad y anonimato en Argentina. Derechos Digitales. Accesible en (Ultima fecha de acceso: 08/12/2019): https://www.derechosdigitales.org/wp-content/uploads/1.Legal-Informe-Argentina.pdf).

Goldhill, O. (2019) A 'big data' firm sells Cambridge Analytica's methods to global politicians, documents show. Quartz. Accesible en (Última fecha de acceso: 08/12/2019): https://qz.com/1666776/data-firm-ideia-uses-cambridge-analytica-methods-to-target-voters/

Masciotra, M. (2018). Protección de datos personales y su integración en el marco de los derechos humanos. SAIJ. Accesible en (Ultima fecha de acceso: 08/12/2019): http://www.saij.gob.ar/mario-masciotra-proteccion-datos-personales-su-integracion-marco-derechos-humanos-dacf180264-2018-12-10/123456789-0abc-defg4620-81fcanirtcod?q=fecha-rango%3A%5B20180918%20TO%2020190318%5D&o=12&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B5%2C1%5D%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Doctrina&t=60

Oxford Analytica. (2019). Navigating a Dangerous World. Long-view, in-depth analysis of trends and developments from the Oxford Analytica Daily Brief. Accesible en (Ultima fecha de acceso: 08/12/2019): https://www.oxan.com/media/2606/oxford-analytica-e3-briefing-book.pdf

Pérez de Achá, G. (2016). El auge del software de vigilancia en América Latina. Accesible en (Última fecha de acceso: 08/12/2019): https://www.derechosdigitales.org/9880/el-auge-del-software-de-vigilancia-en-america-latina/

Quiroz, R. (2016). El *Hábeas* Data, protección al derecho a la información y a la autodeterminación informativa. Letras vol.87 no.126 Lima jul./dic.

RIPD (2017). Estándares de protección de datos personales para los Estado Iberoamericanos. Accesible en (Última fecha de acceso: 08/12/2019): http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

Uciferri, L. #ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires. Accesible en (Ultima fecha de acceso: 08/12/2019): https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

Violler, P. (2017). ¿Quién defiende tus datos?. Derechos Digitales. Accesible en (Última fecha de acceso: 08/12/2019): https://www.derechosdigitales.org/wp-content/uploads/qdtd-2018.pdf

Zuazo, N. (2019). Nada es privado. Accesible en (Última fecha de acceso: 08/12/2019): https://www.lanacion.com.ar/tecnologia/nada-es-privado-big-data-politica-oportunidad-nid2285255?utm_campaign=meetedgar&utm_medium=social&utm_source=meetedgar.com

Zuboff, S. (2019). The age of surveillance capitalism. The fight for a human future a new frontier of power. New York: Public Affairs.

iNTERNET BOLIVIA .ORG

DERECHOS DIGITALES América Latina

FRIEDRICH EBERT STIFTUNG