La protección de datos personales en el sector privado de Paraguay

Un estudio exploratorio

Luis Alonzo Fulchi
Maricarmen Sequera

TEDIC
TECNOLOGÍA & COMUNIDAD

Tabla de contenidos

Esta investigación fue realizada con el apoyo de **Privacy International**, una organización del Reino Unido que monitorea las invasiones a la privacidad por parte de los gobiernos y corporaciones.

Autores:

- Luis Alonzo Fulchi
- Maricarmen Sequera Buzarquis

Colaboración:

- Eduardo Carrillo

Introducción

El avance de las tecnologías digitales ha generado múltiples instancias en las cuales los datos personales se encuentran sujetos a tratamientos automatizados por parte del sector público y privado para realizar de forma rápida y efectiva servicios comerciales y estatales.

La protección de datos personales protege a las personas de toda afectación en sus derechos con motivo del tratamiento de su información personal. Este derecho les otorga la facultad de oponerse a todo tratamiento perjudicial de sus datos personales por parte de terceros.

La ausencia o limitada protección de los datos personales abre lugar a prácticas que afectan a los derechos humanos como la intimidad, privacidad, libertad de expresión, libertad de asociación entre otros. Para que haya un balance entre tecnología y derechos humanos en Paraguay, resulta imprescindible **realizar un diagnóstico** sobre el estado actual del tratamiento de datos personales de todos los sectores para luego pasar a un debate amplio y participativo entre todas las múltiples partes interesadas.

En este sentido, desde TEDIC presentamos esta segunda parte de la investigación sobre la protección de los datos personales del año 2017. La primera parte incluyó el estado del marco legal vigente en el país y la gestión de bases de datos personales en el sector público: los hallazgos llevaron a explorar rápidamente y generar preguntas similares sobre las bases de datos de algunas empresas del sector privado en Paraguay.

En lo referente a las entrevistas realizadas, cabe señalar que tomamos empresas del área de la salud y finanzas. En algún caso la empresa es relativamente pequeña y en otros entrevistamos voceros de empresas con datos personales de millones de personas, todas de Paraguay.

Antecedentes

Paraguay es uno de los pocos países de la región que no cuenta con una ley integral de protección de datos personales (Acuña, Alonzo, & Sequera, 2017). Desde el ingreso de Paraguay a la Organización para la Cooperación y Desarrollo Económico (OCDE) en enero de 2017[1] y la actual negociación de tratado de libre comercio entre el MERCOSUR y la Unión Europea[2], el país se encuentra rodeado de directrices y estándares internacionales sobre la protección de la privacidad y el flujo transfronterizo de datos personales que deberán adecuarse normativamente a los volúmenes y múltiples usos de datos personales que se generan de forma sencilla y cada vez más de bajo costo resultante de la recolección, almacenamiento, procesamiento, agregación, análisis y transferencias de los mismos.

Dada a la ausencia de normativas de protección de datos en Paraguay, el negocio de la venta de bases de datos personales de los créditos bancarios y financieros ha crecido de forma indiscriminada. De entre los datos que venden de forma ilegal están cédula de identidad, número de teléfono móvil, antecedentes policiales y judiciales entre otros, violando así principios

1 OCDE. Paraguay se convierte en miembro de la OCDE https://www.oecd.org/dev/paraguay-convierte-miembro-centro-desarrollo-ocde.htm [Fecha de consulta: 8 de febrero, 2018]

2 El observador. Figurita repetida: Mercorsur y UE no cerraron acuerdo de TLC en Asunción. Fecha del 2 de marzo de 2018. https://www.elobservador.com.uy/figurita-repetida-mercosur-y-ue-no-cerraron-acuerdo-tlc-asuncion-n1177396 [Fecha de consulta: 3 de marzo, 2018].

fundamentales de la protección de datos personales como son el consentimiento y la autonomía de las personas sobre su información.

Ante la falta de aplicación de regulaciones, las personas nos vemos expuestas a todo tipo de problemas y riesgos como el *spam*, llamadas invasivas, intentos de extorsión, etc..

Por otra parte, suele aparecer la figura del *chivo expiatorio*, como el caso de los jóvenes del interior del país[3], que distribuyen bases de datos a empresas crediticias y aparecen como únicos responsables del problema.

Cabe destacar que la venta de las bases es solo el emergente: existe fuerte responsabilidad en la recolección, almacenamiento, cruzamiento, divulgación y también en la compra de esas bases de datos, y es el Estado el que no tiene la capacidad de cumplir su rol de *tutela efectiva*, ni de sanciones a los responsables de las filtraciones y abusos cometidas contra las bases de datos personales.

Marco Teórico

Datos Personales

Para esta investigación tomaremos la definición de datos personales redactada en el nuevo reglamento sobre datos personales de la Unión Europea (UE) 2016/679:

> *"toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (Parlamento Europeo, Consejo de la Unión Europea, 2016)*

Principios de protección

Además aplicaremos los mismos principios de la investigación de bases de datos del sector público a la bases de datos del sector privado (Banisar, 2011), como el estándar más elevado y por el que Paraguay debe abogar para la protección efectiva de los datos personales. Estos principios son:

- Principio de **recolección**: la recolección de datos personales debe ser limitada y contar con un objetivo específico. Los datos sólo pueden ser recolectados a través de instrumentos legales con el permiso de los titulares de los datos, en caso que sea necesario.
- Principio de **calidad de los datos**: los datos recolectados deben servir el objetivo de su recolección. Los datos deben ser exactos y actualizados.
- Principio de **especificación de finalidad**: el objetivo de la recolección de la información debe ser preciso al momento del relevamiento de los datos. Dicha finalidad debe guiar el uso de los datos.

3 La Nación. Privacidad ciudadana a la venta. Fecha del 22 de mayo de 2017. Disponible en: http://www.lanacion.com.py/destacado_edicion_impresa/2017/05/22/privacidad-ciudadana-a-la-venta/ [Fecha de consulta: 18 de Febrero, 2018].

- Principio de **limitación en el uso**: los datos personales no deben ser publicados, difundidos o entregados por motivos distintos al objeto de la recolección. El titular de los datos debe consentir o autorizar de forma expresa para que la difusión sea permitida.
- Principio de **seguridad**: La información recolectada debe ser protegida frente a eventuales riesgos como pérdida, sabotajes, destrucción, etc.
- Principio de **apertura**: debe existir una política general de apertura sobre procesos, prácticas, y normativas relacionadas a los datos personales. Se deben establecer formas de identificar la existencia y la naturaleza de datos personales, y las razones principales de uso deben estar disponibles, al igual que la identidad del controlador y el lugar de almacenamiento de los datos.
- Principio de **participación individual**: una persona debe tener el derecho a:
    - Obtener de un controlador de datos (u otra persona) una confirmación de que dicho controlador tiene o no datos relacionados al individuo;
    - Obtener esa información en un tiempo razonable a un costo que no sea excesivo (o ningún costo), de una manera razonable y un formato que sea inteligible para la persona;
    - Si la solicitud de información es denegada, tiene derecho a recibir una explicación, y tener la posibilidad de apelar la denegación;
    - Poder solicitar una corrección de la información contenida en la base, ya sea rectificándola, completándola, amendándola o borrándola.
- Principio de **rendición de cuentas**: Un controlador de datos debe estar sujeto a rendición de cuentas sobre su adhesión a medidas que materialicen los principios de protección de datos personales.

Objetivo

Esta segunda parte de la investigación tiene como finalidad complementar el diagnóstico del estado de las bases de datos de la investigación principal, incluyendo a tres bases de datos del sector privado para así generar mas insumos de información y mayor debate desde una mirada integral y ampliada del tratamiento de datos personales en Paraguay.

Metodología

Es la replica de la investigación principal, es de carácter exploratorio, teniendo en cuenta que a nivel local existen pocos trabajos académicos que aborden el tema de la protección de datos personales. Como referencia para el análisis de los hallazgos, se utilizarán los estándares de protección resumidos en el trabajo de David Banisar y lo estipulado en el nuevo Reglamento de la Unión Europea (UE) 2016/679. La herramienta metodológica a utilizar es la entrevista semi-estructuradas.

Las entrevistas buscan explorar la situación del tratamiento de datos personales en tres empresas privadas y buscan indagar sobre la cantidad y estado de las bases de datos con datos personales que manejan dichas empresas. Se busca saber la cantidad y calidad de dichos datos, así como los procedimientos que utilizan las empresas para gestionar dichas bases. Además, saber cómo se almacenan, cómo se actualizan, cómo se protegen, cómo se recolectan dichos datos, etc..

Las entrevistas tienen una duración de al menos media hora y son de carácter anónimas para lograr cierto grado de confianza en los entrevistados y protegerlos contra posibles represalias en sus lugares de trabajo.

Marco muestral y casos de estudio

Se solicitaron a cuatro empresas privadas: una relacionada a bases de datos del sector de la salud, las otras tres relacionadas al sector financiero con diferentes finalidades como créditos, ahorros y pago de impuestos a través de servicios digitales.

Sobre este último punto, la empresa que se dedica a ofrecer servicios digitales, no se ha mostrado interesada en participar de las entrevista. Por tanto el total de empresas entrevistadas se redujo a 3. En ese punto se consideró saturada la muestra para los objetivos fijados en la investigación.

Categorías de análisis

A partir de un guión de entrevista o preguntas guía –disponible en el anexo A.1.– se elaboró un conjunto primario de categorías de análisis que se fue enriqueciendo y mejorando durante el mismo procedimiento analítico.

Análisis de hallazgos

A partir de los actores entrevistados podemos inferir que hay una gran variedad de situaciones en lo referente a los datos personales.

Esta variación es preocupante, ya que aparecen casos de una total ausencia de protocolos y estándares, fallando en la amplia mayoría de los “principios de protección” hasta un cumplimiento casi total.

Un hallazgo importante y preocupantes es que las empresas suelen recolectar la información sin **instrumentos legal específicos** y en general sin conocer los límites y las “buenas prácticas” en la recolección, elemento establecido en el **principio de recolección** que desarrollamos anteriormente.

Lo mismo ocurre con el **principio de finalidad:** sobre la recolección y finalidad, las empresas suelen justificarlas en la “necesidad para el desarrollo de su mandato”. Algunas empresas especifican su finalidad en el **contrato de adhesión**, aunque no queda claro a qué nivel lo especifican y si después cumplen con este principio y el de **limitación en el uso**. Un análisis de dichos contratos sería necesario para poder tener en claro si se respeta o no este principio en los casos que lo especifican, pero supera el alcance de este trabajo.

En lo que refiere al **principio de calidad de los datos,** la actualización y control de exactitud se suele realizar en momentos que los usuarios se acercan y no parece haber una forma sistematizada de controlar esto. Solo una de las instituciones recogidas afirmó una voluntad proactiva de actualizar los datos contenidos en sus bases.

En cuanto a la seguridad de la información, que denominamos **principio de seguridad**, vale la pena introducir el estándar ISO 27001. Esta norma emitida por ISO[4] fue creada en el 2005 y especifica los requisitos para gestionar la seguridad de la información de las empresas. También se puede aplicar a cualquier tipo de organización.

Estar certificado con esta norma implica tener protocolos y tomar una serie de medidas y recomendaciones que este consorcio de expertos a nivel internacional establecieron para la protección de la seguridad de la información. De las entrevistas surgen que muy pocas empresas están certificados con esta norma, que siempre son las mismas que aplican el resto de los principios, lo que quiere decir que la amplia mayoría de las empresas no tienen esta certificación y aplican solamente alguno de los principios de protección. El manejo de riesgos se realiza de una forma totalmente ad-hoc.

Cabe destacar que como política general de las empresas, todos los funcionarios encargados o involucrados en el manejo de base de datos están plenamente identificados en las acciones que realizan y poseen permisos de acuerdo a las necesidades de sus roles y nada más. Sin embargo esta medida parece no ser suficiente dada la cantidad de bases de datos con datos personales que circulan en el mercado ilegal de nuestro país.

Sobre **transferencia**, suele haber solo consulta de datos específicos, es decir, la ejecución remota de un script que permite obtener solamente información concreta y específica sobre registros

4 ISO es la Organización Internacional de Normalización, fundada en 1947 y cuenta con reconocimiento del Consejo Económico y Social de la ONU.

individuales y no la información en forma de base de datos. Dicho esto, las empresas declararon no tener mecanismos ni protocolos de transferencia de bases de datos a nivel nacional ni internacional.

En lo que refiere a la **limitación del plazo de conservación**, todas las empresas entrevistadas dijeron no **destruir los datos,** es decir que se conservan por tiempo ilimitado.

Tampoco está estandarizada la entrega de información a las autoridades de **persecución penal**. En algunos casos afirmaron entregar la información con nota fiscal, en vez del debido proceso de una orden judicial emitida por un Juez. Al respecto un entrevistado mencionaba:

> *"En líneas generales la información confidencial se entrega bajo orden judicial"*

Es preocupante la parte de la frase donde dice “En líneas generales”, lo que de alguna forma evidencia que hay casos que quizás se entregue solo con nota fiscal, como ya mencionamos.

Salvo en uno de los casos, se confirma lo mismo que se había constatado para el sector público y es que las **unidades encargadas de informática** suelen ser pequeñas. Estas unidades son las que tienen a cargo la infraestructura de almacenamiento, respaldo y protección de las bases de datos con datos personales.

Conclusiones

Existe una completa **heterogeneidad** de situaciones en lo que refiere a la protección de datos personales, tanto a nivel jurídico como humano y tecnológico. Muy pocas empresas tienen aprobada la norma ISO 27001 y algunas otras apenas ha desarrollado protocolos y buenas prácticas. Es decir, hay una **discrecionalidad**, en la protección de dichas bases.

Prácticamente no hay apego a los **estándares internacionales** de protección de base de datos que se desarrollaron en la introducción y en el marco teórico de la investigación sobre bases de datos públicas en Paraguay (Acuña et al., 2017).

Paraguay corre serios riesgos de **ataques informáticos** por parte de agentes nacionales o extranjeros como ya ha ocurrido en numerosas ocasiones. Esto es mucho más complejo y riesgoso para la seguridad y privacidad de las personas, en el contexto de la recolección masiva de datos personales tanto por parte de las empresas privadas como de las instituciones públicas.

En este sentido, se constata cierto recelo y ciertos temores del sector privado a la hora de compartir la información sobre los ataques informáticos sufridos. Esto debe ser abordado en el marco del Plan Nacional de Ciberseguridad (CERT, SENATICS, 2016), pues un sistema de alerta e intercambio de información sobre los ataques se vuelve imprescindible para fortalecer al resto de las empresas e instituciones contra dichos ataques.

Se evidencia la imperiosa necesidad de la **creación de una Ley Orgánica de Datos Personales** (varios de los entrevistados hicieron énfasis en esto). Es necesario generar ámbitos de discusión pluri participativos que permitan determinar mejores prácticas para enfrentar los desafíos asociados a la defensa del derecho a la protección de datos personales a nivel global.

Bibliografía

Acuña, J., Alonzo, L., & Sequera, M. (2017). La protección de Bases de Datos en Paraguay. *Setiembre*, *2017*, *1*(1). Recuperado a partir de https://www.tedic.org/wp-content/uploads/sites/4/2017/09/La-protecci%C3%B3n-de-Bases-de-Datos-en-Paraguay_Documento-Final.pdf

Banisar, D. (2011). The right to information and privacy: Balancing rights and managing conflicts. *The World Bank, Access to Information Program*. Recuperado a partir de https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf

CERT, SENATICS. (2016, noviembre 9). Plan Nacional de Ciberseguridad. Recuperado a partir de http://gestordocumental.senatics.gov.py/share/s/m2uDswEUTDmrDBY2NFttIg

Parlamento Europeo, Consejo de la Unión Europea. (2016, abril 27). Reglamento (UE) 2016/679 del Parlamento Europeo. Recuperado a partir de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

"No quiero vivir en un mundo donde
todo lo que digo, todo lo que hago,
todo lo que hablo, toda expresión
de creatividad o de amor o de amistad
queda grabada" Edward Snowden