La protección de datos personales en bases de datos públicas en Paraguay

Un estudio exploratorio

Jazmín Acuña
Luis Alonzo Fulchi
Maricarmen Sequera

TEDIC
TECNOLOGÍA & COMUNIDAD

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.

Asunción, Paraguay – 2017

Tabla de contenidos

Introducción

La presente investigación busca explorar el estado de la protección de los datos personales almacenados en bases de datos en algunas instituciones de carácter público en Paraguay. Específicamente, identificar los usos, manejos, procedimientos, riesgos, regulaciones y legislación que definen la administración de dichas bases.

Para la exploración se realizó un análisis jurídico de la legislación nacional vigente así como la legislación internacional y jurisprudencia vinculantes para el país. Además se estudiaron 9 instituciones públicas que manejan bases de datos con datos personales, a saber: la Secretaría Técnica de Planificación (STP), el Ministerio de Salud y Bienestar Social (MSPBS), el Centro Nacional de Computación (CNC), la Secretaría de Acción Social (SAS), el Ministerio de Industria y Comercio (MIC), la Dirección Nacional de Aduanas (DNA), la Subsecretaría de Estado de Tributación (SET), la Secretaría Nacional de la Vivienda y el Hábitat (SENAVITAT) y el Ministerio de Educación y Ciencias (MEC).

El marco teórico de la investigación se sustenta en la literatura de las ciencias de la información y el derecho. Específicamente, tratados internacionales, legislación, normativas y regulaciones locales vigentes. El marco metodológico es cualitativo. Se realiza un análisis jurídico y se llevan a cabo entrevistas semi-estructuradas a funcionarios de instituciones públicas encargados del manejo de bases de datos e informantes calificados.

Con esta investigación, se busca indagar qué principios y estándares de protección aplican las instituciones públicas en el manejo de bases de datos que contengan datos de carácter personal. Además, se busca dar un insumo analítico inicial para el diseño de políticas públicas en torno a la protección de los datos personales.

La investigación se divide en cinco capítulos. El primer capítulo contiene el marco teórico, en el que se desarrollan los conceptos principales del estudio, un breve comentario sobre las tensiones que existen entre los derechos al acceso a información pública y la protección de datos personales y los estándares de protección de datos personales. En el segundo capítulo, se detallan los objetivos y el marco metodológico, con la presentación de las preguntas guía de la investigación y los casos de estudio seleccionados para las entrevistas. En el tercer capítulo, se presenta el análisis del marco normativo que aplica a Paraguay. En el siguiente se avanza sobre los hallazgos de las entrevistas de los nueve casos de estudio. Estos hallazgos se miden con indicadores relacionados a los estándares de protección consensuados a nivel internacional. Finalmente, en el último capítulo se entrega una conclusión y recomendaciones para políticas públicas.

Marco Teórico

Definiciones de concepto

En las discusiones sobre protección de datos personales en bases de datos de instituciones públicas, se manejan los conceptos de *información pública*, *bases de datos públicas*, *datos de carácter personal*, entre otros. Las definiciones de estos conceptos son relevantes porque sirven para comprender mejor los alcances y desafíos de la materia. A continuación se provee un acercamiento a estos conceptos que son base de la presente investigación.

Información pública

Organismos internacionales y academia han establecido definiciones de lo que es *información pública*. La Corte Interamericana considera que el artículo 13 de la Convención Americana de Derechos Humanos protege el derecho de las personas a acceder a información pública. Especifica que esta información es aquella que "se encuentra bajo el control del Estado"(CIDH, s/f).

La directiva 2003/98/EC del Parlamento Europeo y el Consejo de la Unión Europea del 17 de noviembre de 2003, sobre el re-uso de información pública establece algunas definiciones de lo que constituye dicha información (Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público, 2003). En su artículo 2 detalla qué significa el re-uso de información pública, especificando lo que es información pública: *"[…] documentos en poder de las instituciones del sector público [...]"(*Directiva 2003/98/CE, 2003). En el párrafo 3 del mismo artículo se explica que *documentos* refiere a *"cualquier contenido independiente al medio (escrito en papel o almacenado en formato electrónico o como registro sonoro, visual o audiovisual); cualquier parte de ese contenido" (*Directiva 2003/98/CE, 2003).

Por su parte la Organización para la Cooperación y el Desarrollo Económicos (OCDE) establece que *información y contenido del sector público* es cualquier tipo de información producido y/o recolectado por instituciones públicas, y forma parte del rol asignado a la institución aiend(Organización para la Cooperación y Desarrollo Económicos, 2006).

Raed M. Sharif, profesor e investigador de Syracuse University, en una disertación sobre la utilización y el valor de la información pública para la creación de conocimientos, considera que información pública está compuesta por:

> *"datos e información que son producidos por o para las instituciones públicas que incluyen, por ejemplo, datos de educación y salud, datos geográficos, reportes financieros, estadísticas sociales y económicas, procedimientos legislativos y judiciales, datos de recursos de agua y alimentos, y muchos otros tipos de datos e información, y que colectivamente son referidos como 'información del sector público"(Sharif, 2013)*

De los principios contenidos en las definiciones de *información pública* se podría inferir que toda información en poder del Estado es pública y por tanto debe ser accesible. Sin embargo, los principios de protección de datos personales, que se detallan más adelante en la investigación, limitan dicho acceso. Por ello, el manejo de las bases de datos públicas que contienen datos de carácter personal debe hacerse atendiendo a dichos principios.

Bases de datos públicas

Debido a las ambigüedades que presenta la ley sobre "Datos Privados"(Congreso Nacional, 2001) en Paraguay, vale detenerse en la definición de base de datos y en particular aquellas que están en poder de las instituciones estatales:

> *"[...] un conjunto organizado de datos que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso, cuyo titular sea una persona jurídica de naturaleza pública". (Congreso Nacional, 2001)*

A partir de esta definición, observamos que un conjunto organizado de datos almacenados en carpetas físicas, en cajones de una institución pública, también es una base de datos. Mas el objeto del interés de esta investigación son las que se encuentran digitalizadas.

Datos personales

Para especificar el concepto de datos personales, se puede recurrir a la Resolución de Madrid ("Estándares internacionales sobre protección de datos personales y privacidad", 2009) del año 2009, donde se establece una *Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad*, en relación con el *Tratamiento de Datos de carácter personal*. Allí se definen los Datos Personales como:

> *"cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados".(2009)*

Por su parte el Reglamento de la Unión Europea (UE) 2016/679[1], sobre la protección de las personas físicas, en lo que respecta al tratamiento de Datos Personales y su libre circulación, *amplía la definición* para adecuarla a los nuevos desafíos que imponen los avances tecnológicos. En el nuevo Reglamento, se consideran datos personales a:

> *"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*)*

Otros conceptos relevantes para este estudio serán esbozados en la exposición de los *principios generales* que rigen la *protección de Datos Personales* en bases de datos. Antes de ello, es pertinente reconocer las tensiones y las limitaciones que existen entre el derecho al acceso a la información y el derecho a la privacidad de las personas, a través de la protección de datos personales.

Derecho a Acceso a Información Pública / Derecho a la Privacidad

El tema de las bases de datos con datos personales, sean estas de naturaleza pública o privada, se encuentra con la tensión entre dos derechos: el derecho al acceso a la información pública y el derecho a la privacidad de las personas.

1 Esta deroga la Directiva 95/46/CE

El derecho a la información deriva del derecho a la libertad de expresión que se encuentra en el artículo 19 de la Declaración Universal de los Derechos Humanos:

> *"Todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y de recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión"* (ONU, 1948).

La *Convención Americana sobre Derechos Humanos del Pacto de San José de Costa Rica*, en el artículo 13 sobre la *"Libertad de pensamiento y de expresión"*, establece el derecho de las personas *"a buscar, recibir y difundir informaciones e ideas de toda índole"*(CIDH, s/f). Es importante notar que en el mismo artículo, también se establecen los *límites* a este derecho, entendidos como responsabilidades ulteriores. Allí se especifican que estos límites deben ser expresados por la Ley para asegurar *"a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas"*.

Por otro lado, el derecho a la privacidad es reconocido como derecho universal en el artículo 12 de la Declaración. Se entiende como el derecho a la "vida privada". Expresa cuanto sigue:

> *"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"* (ONU, 1948).

Este derecho también ha sido reconocido en otros tratados internacionales y en legislaciones locales con algunas variaciones. David Banisar lo relaciona *"a la protección de la autonomía individual y la relación entre el individuo y la sociedad, incluyendo gobiernos, compañías y otros individuos"*(Banisar, 2011). Distingue 4 dimensiones que sirven para entender la amplitud del concepto, entre ellas la *privacidad informativa*, *"que involucra las reglas para gestionar los datos personales"*(Banisar, 2011). Esta es la dimensión se explorará en este estudio.

Los conflictos entre el *acceso a información* y la *privacidad* se dan porque mucha información de carácter personal se encuentra en manos del gobierno. Banisar cita algunas resoluciones al respecto. Por ejemplo, explica que hay consenso de que la información de funcionarios electos tiene menos garantías de protección. También, la información personal de funcionarios públicos que se genere en sus capacidades oficiales no necesariamente es sujeta de resguardo. Sin embargo, existen otros ejemplos que evidencian desencuentros o disensos. En países de Europa, los gobiernos mantienen reservada la información de las personas que son parte de programas de apoyo social. Por el contrario, en países del hemisferio Sur, esta información es pública para evitar casos de corrupción y para el monitoreo social de estos programas. No hay acuerdo sobre el manejo de los registros judiciales.

En un estudio sobre la legislación chilena, Renato Jijena propone algunas formas de resolver algunas tensiones entre el tratamiento de datos personales en fuentes públicas y el derecho al acceso a información, contenido en la Ley 20.285. A su criterio,

> *"el tratamiento de los datos personales de los ciudadanos es y debe ser, jurídica, constitucional y legalmente una limitante al ejercicio del derecho de acceso a los actos, contratos, documentos, resoluciones y procedimientos de la Administración del Estado"*(Jijena, 2013).

Jijena plantea la necesidad de hacer un estudio “caso por caso” a la hora de conciliar el derecho al acceso a la información y la protección de datos personales. Advierte que no debería usarse la protección de datos personales de forma “general y sistemática” para no abrir información del Estado. De ser así, hechos de corrupción podrían ampararse y quedar impunes.

Principios de protección de datos personales

Para la protección de datos personales, organismos internacionales, academia y gobiernos han trabajado y establecido principios y estándares para el manejo de dichos datos. David Banisar sintetiza dichos principios en un trabajo sobre derecho al acceso a la información y el derecho a la privacidad(Banisar, 2011), que se detallan a continuación:

- 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.
- 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 desarrollo, prácticas, y normativas relacionadas a los datos personales. 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:
    a) Obtener de un controlador de datos (u otra persona) una confirmación que el controlador de datos tiene o no datos relacionados al individuo;
    b) Obtener esa información en un tiempo razonable a un costo (o ninguno) que no sea excesivo, de una manera razonable y un formato que sea inteligible para la persona;
    c) Si la solicitud de información es denegada, recibir una explicación, y tener la posibilidad de apelar la denegación;
    d) 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.

El Reglamento de la Unión Europea (UE) 2016/679 (Parlamento Europeo, Consejo de la Unión Europea, 2016), que es una de las normativas más recientes sobre protección de Datos Personales, incluye en su artículo 5 una serie de principios relativos al tratamiento de dichos datos. Los principios allí establecidos son en gran medida los mismos que se presentaron más arriba. Sin embargo, se citan a continuación para tenerlos como referencia de esta investigación y el análisis posterior de los hallazgos:

- **Licitud, lealtad y transparencia:** Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.
- **Limitación de la finalidad:** El Reglamento dice que los datos personales deben ser recogidos con fines "determinados, explícitos y legítimos". No podrán ser usados para propósitos incompatibles con los fines explicitados. El Reglamento expresa que fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos no se consideran como incompatibles con los fines iniciales de la recolección.
- **Minimización de datos:** El Reglamento expresa que los datos personales deberán ser "adecuados, pertinentes y limitados" a los fines para los que son tratados.
- **Exactitud:** Los datos personales deberán ser exactos y actualizados, dice el Reglamento. Especifica que todas las medidas razonables deberán ser tomadas para rectificar o suprimir los datos personales que sean inexactos con respecto a los fines del tratamiento.
- **Limitación del plazo de conservación:** El Reglamento establece que los datos personales deberán ser mantenidos para la identificación de los interesados durante "no más tiempo del necesario para los fines del tratamiento de los datos personales". Se podrán conservar por más tiempo solo con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de acuerdo con el artículo 89, apartado 1 del Reglamento.
- **Integridad y confidencialidad:** El tratamiento de los datos personales deberá garantizar la seguridad de los datos personales, incluida según el Reglamento, "la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".
- **Responsabilidad proactiva:** El apartado 2 del artículo 5 se refiere al responsable del tratamiento de los datos. Expresa que debe cumplir con lo establecido en los principios establecidos en el apartado 1 y tiene la obligación de demostrarlo.

Objetivo de la Investigación

El objetivo de esta investigación es generar un insumo de información y análisis para fortalecer las normas y las prácticas de protección de los datos personales contenidos en bases de datos públicas en Paraguay.

Específicamente, la investigación apunta a sentar las bases argumentativas necesarias para diseñar una propuesta de reforma de la Ley de protección de datos personales. Actualizar la normativa vigente a los desafíos que imponen las nuevas tecnologías es imperante para resguardar el derechos de millones de ciudadanos y ciudadanas de Paraguay. Además, a medida que se implementa la Ley 5282/14 de libre acceso a información pública, emergen tensiones con la necesidad de proteger los datos personales y el resguardo de la intimidad de las personas. Dichas tensiones se dan por la ausencia de normas claras, derivando en situaciones en las que los funcionarios dirimen qué hacer en cada caso de acuerdo a sus criterios.

Un objetivo secundario de la investigación es proveer un documento que sirva para producir más trabajos académicos relacionados a los temas que aquí se abordan. Es necesario ampliar el repositorio de conocimientos en esta área. Al momento, no se han encontrado estudios locales sobre protección de datos personales, bases de datos públicas, derecho a la privacidad y otros tópicos que si se indagan en la presente investigación.

Para alcanzar el objetivo principal del estudio, se identifican los usos, manejos, procedimientos, riesgos, regulaciones y legislación que definen la administración de bases de datos que incluyan datos personales en el sector público. Se realiza un análisis jurídico de la normativa vigente en el país. Por otro lado, se hacen entrevistas a responsables de las bases de datos en nueve instituciones públicos para indagar qué principios y estándares de protección aplican en el manejo de dichas bases.

Los resultados de la investigación se difunden en los canales de comunicación de la organización y se acercan a las autoridades del Estado que tienen la capacidad promover cambios en las normas y las prácticas de manejo de datos personales en bases de datos públicas.

Estrategia Metodológica

Justificación de elección metodológica

La investigación 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. No se manejan teorías previas a refutar o reafirmar con los hallazgos de la investigación. Tampoco se plantea una hipótesis para comprobar o descartar. Lo que se busca es conocer el estado de la administración de los datos personales en bases de datos públicas en Paraguay. 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.

Se realizará un abordaje exploratorio utilizando 2 herramientas metodológicas. Por un lado, un análisis jurídico que servirá como insumo para el resto de la investigación. Este análisis nos permitirá tener un marco conceptual sobre el tratamiento de datos personales a la vez que servirá para establecer una especie “estado del arte” legal. La segunda herramienta metodológica – entrevistas semi-estructuradas - viene de la mano de las metodologías cualitativas.

Las entrevistas buscan explorar la situación del tratamiento de datos personales en las instituciones estatales. Se busca saber donde se encuentran algunas de las bases de datos de la administración actual y conocer en qué situaciones se encuentran los datos contenidos en ellos. Para esta investigación contemplamos realizar entrevistas con el sector privado, pero debido a su variedad y cantidad, así como posibles problemas metodológicos de este tipo de instrumentos, decidimos acotar nuestro marco muestral y tomar solamente a entidades públicas de la administración central.

Además realizamos *dos entrevistas con informantes calificados* para poder construir la muestra teórica y para encontrar aquellas instituciones públicas con las bases más importantes y también las más vulnerables. Estas entrevistas permiten tener un panorama general sobre el manejo de BBDD en el sector privado, que como ya se mencionó, es mucho más amplio en cuanto a la diversidad de actores y más complejo en lo referente a la veracidad y conveniencia de las respuestas de los entrevistados. Pretender que las empresas privadas responderán sin reservas las preguntas que están previstas en el guión de entrevistas sería de poco rigor metodológico.

Las entrevistas con las instituciones estatales buscan indagar sobre la cantidad y estado de las bases de datos con datos personales que manejan ciertas áreas de la administración pública. Es decir, saber la cantidad, calidad de dichos datos, así como los procedimientos que utiliza cada institución 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

A partir de las entrevistas con los servidores públicos e informantes calificados construimos un marco muestral teórico conteniendo las siguientes instituciones: Secretaría Técnica de Planificación (STP), Ministerio de Salud y Bienestar Social (MSPBS), Centro Nacional de Computación (CNC), Secretaría de la Acción Social (SAS), Dirección General de Encuestas Estadísticas y Censos (DGEEC), Dirección Nacional de Identificaciones, Ministerio de Industria y Comercio (MIC), Dirección Nacional de Aduanas (DNA), Subsecretaría de Estado de Tributación (SET), Centro de Respuestas Ante Incidentes Cibernéticos (CERT), Banco Central del Paraguay (BCP), Secretaría Nacional de la Vivienda y el Hábitat (SENAVITAT), Ministerio de Educación y Ciencias (MEC).

A medida que se avanzó en las entrevistas, a partir de las dificultades y posibilidades de contactar a los entrevistados, el número de instituciones se redujo a 9. 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.

La categorías pre-definidas se dividen en 3 conjuntos preliminares que luego se desglosan de la siguiente forma:

Principios de protección:

- Recolección
  - Notificación
- Finalidad
- Limitación del uso
- Calidad
- Conservación

Acceso y transferencia:

- Niveles de acceso
- Transferencias nacionales
- Transferencias internacionales

Infraestructura:

- Seguridad informática
- Buenas prácticas
- Recursos humanos de sostenimiento

Casos de estudio

Se estudiaron 9 casos, es decir 9 instituciones públicas que manejan bases de datos con datos personales, a saber: la Secretaría Técnica de Planificación (STP), el Ministerio de Salud y Bienestar Social (MSPBS), el Centro Nacional de Computación (CNC), la Secretaría de la Acción Social (SAS), el

Ministerio de Industria y Comercio (MIC), la Dirección Nacional de Aduanas (DNA), la Subsecretaría de Estado de Tributación (SET), la Secretaría Nacional de la Vivienda y el Hábitat (SENAVITAT) y el Ministerio de Educación y Ciencias (MEC).

Se debe notar que fue mayor el número inicial de instituciones que se buscó explorar. Sin embargo, a medida que se avanzó en las entrevistas, a partir de las dificultades y posibilidades de contactar a los entrevistados, el número de instituciones se redujo a 9. En ese punto se consideró saturada la muestra para los objetivos fijados en la investigación.

Las bases de datos que manejan las 9 instituciones estudiadas se especifican en la sección de los hallazgos de las entrevistas. En esta sección se podrá notar sus decretos o normativas de creación, los datos que las bases recolectan y qué datos de carácter personal contienen, además de las limitaciones o prácticas de protección que sus responsables aplican para resguardarlas.

Análisis jurídico de la Normativa Nacional e Internacional

Lo que sigue a continuación es un análisis legal sobre la normativa nacional vigente que protege la vida privada de las personas y que tiene relación directa con nuestro objeto de estudio, que son las bases de datos que contienen datos personales en el país.

La Constitución Nacional y Tratados Internacionales

En el ámbito internacional existe una serie de tratados que expresamente contemplan la protección de la vida privada como por ejemplo, la Declaración Universal de Derechos Humanos (ONU, 1948), en cuyo artículo 12 señala que nadie será objeto de injerencias arbitrarias en su vida privada, lo que es recogido por el Pacto Internacional de Derechos Civiles y Políticos de Naciones Unidas (art. 17 inc. 1) (ONU, 1966) y la Convención Americana de Derechos Humanos (art. 11 inc. 2) (OEA, 1969). Todos estos tratados y convenciones han sido ratificados por Paraguay, lo que implica que pasa a ser parte de su sistema nacional legal.

En la reforma constitucional del año 1992, se incorporan a la Constitución Nacional (CN)(Asamblea Constituyente, 1992) las siguientes figuras:

> *Art 33 - Derecho a la Intimidad - "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública.*
> *Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".*
>
> *Art 36 – Inviolabilidad del patrimonio documental y de la comunicación privada: "El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios.*
> *Las pruebas documentales obtenidas en violación a lo prescripto anteriormente carecen de valor en juicio.*
> *En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado".*
>
> *Art 23 – De la prueba de la verdad: "La prueba de la verdad y de la notoriedad no serán admisibles en los procesos que se promoviesen con motivo de publicaciones de cualquier carácter que afecten al honor, a la reputación o a la dignidad de las personas, y que se refieran a delitos de acción penal privada o a conductas privadas que esta Constitución o la ley declaran exentas de la autoridad*

> *pública. Dichas pruebas serán admitidas cuando el proceso fuera promovido por la publicación de censuras a la conducta pública de los funcionarios del Estado, y en los demás casos establecidos expresamente por la ley".*
>
> *Art 28 - Del derecho a Informarse (párrafo final): "(...) Toda persona afectada por la difusión de una información falsa, distorsionada o ambigua tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios".*

Como puede observarse, Paraguay cuenta con fuerte protección constitucional a la intimidad y la inviolabilidad de la comunicación de las personas, así como el derecho a la autodeterminación informativa.

En lo referente a la privacidad, el único antecedente de protección en nuestro país corresponde a la época del régimen totalitario de Alfredo Stroessner y se encontraba en la Constitución del 1967, enmendada en 1977. En su artículo 50 hablaba de "la protección del honor y la reputación" (Pappalardo Zaldívar, 1992).

Hábeas Data

El derecho a la protección de datos tiene reconocimiento constitucional. El artículo 135 de la CN de 1992 consagra la garantía del hábeas data, que dispone lo siguiente:

> *"Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad".*

Además la persona podrá requerir la actualización, rectificación o destrucción de los datos personales, que fueran erróneos o que afecten de forma ilegítima sus derechos ante las autoridades competentes.

El primer caso por el cual se utilizó esta garantía fue en 1992 cuando el Abogado Martín Almada, defensor de los derechos humanos y exiliado político, solicitó acceder a sus datos almacenados en los archivos de la dictadura de Stroessner[2].

Actualmente la acción de hábeas data se promueve ante un juez de primera instancia y la jurisprudencia nacional sobre este recurso es vasta. Curiosamente la mayoría de las acciones son promovidas para eliminar datos personales de casos judiciales que han finiquitado[3]. En la actualidad esta eliminación de datos personales fue modificada por la Ley que Reglamenta la Información de Carácter Privado (1682/2001) (Congreso Nacional, 2001).

2 Estos archivos, una vez recuperados resultaron incluir más de 700.000 registros de interrogatorios, torturas y vigilancia estatal. Este archivo fue bautizado como "Archivo del Terror", actualmente declarado patrimonio intangible de la humanidad por la UNESCO.

3 Ver buscador de jurisprudencia de la Corte Suprema de Justicia: http://www.csj.gov.py/jurisprudencia/default.aspx?AspxAutoDetectCookieSupport=1

La protección constitucional no es suficiente, debido a interpretaciones judiciales ambiguas o equivocadas, o ausencias de *Stare decisis et non quieta movere*[4] de las sentencias judiciales, ineficiencia en la prevención de incumplimientos y costos transaccionales. Por todo esto, es necesario una regulación *in extenso* que incluya la autodeterminación informativa[5].

Información de Carácter Privado – Ley 1682/2001 y modificaciones

El titular de los datos personales –que se concibe como persona natural respecto de la cual se predica cierta información– puede acudir a un tribunal para ejercer sus derechos constitucionales a través de habeas data u otras de amparo ante infracciones cometidas en su contra. Pero lo central en la discusión es la necesidad o no de que el Estado adopte una Institucionalidad que vele ex-ante el cumplimiento de la normativa sobre tratamiento de datos personales y que no quede sólo a la gestión de agentes intervinientes. Es decir, que el Estado genere mecanismos y garantías para la gestión de los datos personales.

En Paraguay los datos personales están regulados por la Ley N.° 1682/2001(Congreso Nacional, 2001) "Que reglamenta la información de carácter privado" y su posterior modificación[6] por la Ley 1969 del año 2002(Congreso Nacional, 2002) y 5.543/2015 . Dicha Ley asume que la acción de protección recae en la persona afectada, siendo más cercana a la doctrina norteamericana que implica dejar el cumplimiento de la normativa a las partes involucradas y evitar la intervención del Estado, salvo en cuanto al rol que compete a los tribunales de justicia.

Esta opción no contempla la calificación de estándares de protección de datos personales de la Directiva de la Unión Europea 95/46(Unión Europea, 1995) y el nuevo reglamento general de protección de datos de la Unión Europea 2016/279[7], en especial la figura la autodeterminación informativa. También se observa que no existen definiciones legales acerca de "datos personales", "tratamiento de datos" y "titular de datos".

La Ley 1682/2001 (y sus modificaciones) tiene un enfoque meramente economicista, ya que regula casi exclusivamente los sistemas de información crediticia en las entidades bancarias y financieras, sin cubrir enfoques social y comunitario de la información personal. Actualmente consta de 12 artículos de los cuales 5, 7, 9 y 10 regulan los informes crediticios. No obstante para el análisis de esta Ley vigente utilizamos los principios propugnados por el sistema europeo de protección de datos personales.

4 Se traduce interpretativamente como "*mantenerse con las cosas decididas*", utilizada en derecho para referirse a la doctrina según la cual las sentencias dictadas por un tribunal crean precedente judicial y vinculan como jurisprudencia a aquellas que, sobre el mismo objeto, se dicten en el futuro.

5 Según Rodríguez Palop, el *"Derecho a la autodeterminación informativa (…) cuenta con una doble dimensión, una individual o negativa, formulado como el derecho a la intimidad de la vida privada el cual parece aproximarse a los derechos de primera generación que tienen un carácter individualista y se inspiran en el valor de la libertad; en su dimensión social o positiva, en la medida en que exige una mayor participación de los ciudadanos, un control por parte de éstos de las tecnologías de la información y la comunicación , y una ampliación de sus posibilidades reales de intervenir en los procesos sociales y económicos en condiciones de igualdad, puede asemejarse a un derecho de participación política derivado de la libertad de informarse"*(Rodríguez Palop & Universidad Carlos III de Madrid, 2002).

6 Se puede acceder a un documento con la evolución de la Ley, en el siguiente enlace: https://www.informconf.com.py/docs/Comparativo_ley_1682-01_y_modificatorias.pdf

7 http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

En los apartados que siguen se hará un desglose temático y un análisis jurídico de dicha ley y sus modificaciones.

Tutela Efectiva

La figura de tutela efectiva no está contemplada en la Ley 1682/2001 ya que como se explicó más arriba, la protección no se realiza ex-ante por parte del Estado.

Con la Ley actual se ha logrado que las sentencias del Poder Judicial se limiten a eliminar la información bajo la figura de "derecho al olvido" transcurrido el tiempo de la divulgación de datos de carácter personal y no a través de *habeas data*, como se hacía anteriormente[8].

Ámbito de aplicación

El ámbito de aplicación de la Ley es el tratamiento de la información de carácter privado en general, cualquiera sea la forma en que éste se lleve a cabo: "en archivos, registros, banco de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informe" (art. 1). Sin embargo, excluye específicamente a las bases de datos de su ámbito de aplicación, que es la forma más generalizada y masiva de almacenamiento de datos en la actualidad.

La redacción del artículo 1 genera confusión ya que por un lado afecta a los bancos de datos, pero excluye a las bases de datos y en ningún caso define qué es una u otra cosa. Según la Real Academia Española, un banco de datos es un "archivo de datos referidos a una determinada materia, que puede ser utilizado por diversos usuarios", mientras que base de datos es un "conjunto de datos organizado de tal modo que permita obtener con rapidez diversos tipos de información". Como puede observarse, y al no estar definidos uno u otro concepto, la Ley prácticamente cae en una contradicción.

Si interpretamos que la Ley excluye las bases de datos, se produce una contradicción con el concepto de "autodeterminación informativa". Es decir, es necesario proveer al individuo de facultades que vayan más allá del la simple búsqueda del resarcimiento económico y otorgarles también instrumentos de actuación que les permitan a los titulares controlar y determinar el destino u otros aspectos del tratamiento de sus datos personales. Esta Ley no contempla el derecho que busca el disfrute la privacidad y que engloba la voluntad del individuo de determinar el fin para el cual se utilizarán sus datos, así como el tratamiento que se dará a los mismos en los registros públicos y privados almacenados principalmente en medios informáticos.

Excluir las bases de datos de la protección jurídica puede demostrar una falta de voluntad política de ese momento o un completo desconocimiento de las potencialidades de uso de las mismas. Esta negligencia expone a las personas a ser individualizadas a través de sus datos personales, lo que provoca una invasión del ámbito de la intimidad que se debería proteger. Esto ha provocado la proliferación y el negocio de bases de datos de información de carácter personal y/o sensible, difundidas sin consentimiento y con fines comerciales. Además, se suman los riesgos a que se

8 Ver sentencias relacionadas a contra Informconf sobre hábeas data: http://www.pj.gov.py

realicen cruzamientos y almacenamiento a través de lo que se conoce como Big Data[9], poniendo en un riesgo mayor a la población, individualizando aún más y dejando espacio a posibles discriminaciones en su contra.

Cabe agregar que la Ley también carece de garantías ante la cesión y la comunicación de datos a terceros y que no contempla disposiciones relativas a la transferencia internacional de datos.

Principios de Protección de Datos Personales

La Directiva Europea de Protección de Datos de 1995 es calificada como el estándar más alto en temas de protección de datos. Por ello, se han utilizado los criterios de la directiva para analizar la normativa local.

Principio de Recolección

El objeto de la Ley se encuentra en la redacción dada por el artículo 1 de la Ley 1682/01, modificada por la Ley 1969/02:

> *Art. 1°.- "Esta Ley tiene por objeto regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares. No se aplicará esta Ley en ningún caso a las bases de datos ni a las fuentes de informaciones periodísticas ni a las libertades de emitir opinión y de informar"*

A continuación se enumeran una serie de elementos que refieren al tratamiento de datos y se observan en el articulado de la Ley 1682/01 en su redacción modificada por las leyes 1969/02 y 5543/2015:

- Se permite que cualquier persona pueda efectuar el tratamiento de datos personales siempre que sea de uso exclusivamente privado (art. 2)
- No se requiere autorización del titular del dato cuando el tratamiento de datos provenga de las fuentes públicas (art. 2)
- La ley considera lícita la publicación de dichos datos, cuando "se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudios de mercados, siempre que no individualicen las personas o entidades investigadas" (art. 3)
- Cuando se enuncia "el titular de los datos personales" se hace referencia a los datos de carácter personal de la persona natural que incluye datos sensibles inherentes a la persona física (art. 4) pero quedando excluida la categoría de personas jurídicas[10]. No se encuentra expresamente prohibido el tratamiento de datos sensibles.
- El titular de los datos tiene derecho a exigir al responsable de los datos la modificación, cancelación, bloqueo y eliminación de sus datos (arts. 7 y 9)
- La responsabilidad recae en el que realiza el tratamiento de datos, es decir, el que colecta, almacena y mantiene los datos y supone la indemnización del daño patrimonial y moral en caso de tratamiento indebido (art. 10)

9 Big Data es la capacidad para aplicar análisis algorítmicos a la crecientes volúmenes de información que tanto empresas como gobiernos recolectan de las personas, lo que permite inferir, a través de correlaciones, información útil no contenida explícitamente en dichas bases de datos.

10 Si bien en la ley estos conceptos no están claramente diferenciados, se interpreta de tal manera porque en el Art 4 se consideran datos sensibles los referentes a pertenencias raciales o étnicas, políticas, religiosas, imagen privada entre otros, que son inherentes a la persona física.

- El objeto de la ley excluye explícitamente las bases de datos, fuentes periodísticas, y a las libertadas de emitir opinión y de informar (art. 1). Cabe aclarar nuevamente que se realiza una confusa distinción entre banco de datos y base de datos.

El artículo 1 de la presente Ley resalta el tratamiento de datos como el objeto principal de regulación de la ley. Sin embargo, no distingue entre recolección de datos por organismos públicos y privados. Lo que sí hace es establecer las reglas para el tratamiento de datos en esfera pública, estableciendo que las fuentes públicas de información son de libre acceso, sin limitar el tratamiento de datos personales a la materia de su competencia, naturaleza y duración de los mismos.

En este sentido, en su artículo 2, la Ley afirma que:

> *"Toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos, incluso los creados por la Ley 879/81 y la Ley 608/95 y sus modificaciones"*

El artículo precedente permite el acceso a la *información de carácter privado* por parte del titular del dato, sin embargo no contempla los mecanismos de seguridad en las operaciones de tratamiento de los datos. Tampoco se establece la obligación del responsable de los datos de cuidar de ellos con la debida diligencia, haciéndose responsable de los daños causados –en caso que el titular dé expresamente su consentimiento para los registros.

Principio de Finalidad y la Limitación de la Finalidad

La actual Ley carece del principio de finalidad sobre el uso de los datos recolectados, lo que significa que la norma debe establecer los fines por los cuales los datos hubieren sido recolectados. Es decir, el tratamiento de los datos personales debe ser cierto, adecuado, pertinente y no excesivo en relación al ámbito y finalidad para los que se hubieren obtenido.

Por otra parte, la misma Ley considera lícita toda recolección, almacenamiento, procesamiento de datos personales para uso exclusivamente privado (art. 2) y solamente contempla su publicación cuando "se realice con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudios de mercado, siempre que no individualicen las personas o entidades investigadas" (art. 3). Es decir limita el principio de finalidad considerando excepciones con los fines iniciales de la recolección.

Principio de Integridad y Confidencialidad

La presente Ley no contempla seguridad legal ante tratamiento no autorizado o ilícito o contra la pérdida o destrucción o daño accidental. La única medida actual cae a cargo del afectado o titular del dato a través de la garantía constitucional.

Principio de Rendición de Cuentas

Tanto el sector público como privado que realiza tratamientos de datos deben estar sujetos a rendición de cuentas sobre medidas que toman para el manejo de los datos personales. A falta de un órgano especializado que garantice el cumplimiento de la rendición de cuentas, de transparencia y la aplicación de los estándares en la presente Ley, este principio se encuentra ausente en la legislación paraguaya.

Principio de Seguridad y Apertura

Estos principios tampoco se observan en la actual Ley. La información recolectada debe ser protegida frente a eventuales riesgos como pérdida, sabotajes, destrucción, etc.. Actualmente, el Plan Nacional de Ciberseguridad (CERT, SENATICS, 2016)[11] incluye una serie de estándares para la protección de la infraestructura que almacena bases de datos para evitar tecnológicamente estos eventos, sin embargo la protección radica en la infraestructura y no en la persona[12].

Por otra parte, en lo que respecta a apertura, no existen políticas públicas sobre la apertura de información que guarde relación con el desarrollo, prácticas, y normativas relacionadas al manejo de los datos personales.

Categorías de datos

A continuación se analizan cada una categorías que la Ley define en cuanto a las características de los datos.

Datos personales de carácter público: Se especifican las características principales de los datos personales de carácter público según la Ley (art. 6) que podrán ser "publicados y difundidos a) Los datos que consistan únicamente en nombre, apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional"

Datos sensibles: La Ley contempla la definición de datos sensibles, adaptándose a la doctrina internacional y jurisprudencias que buscan prevalecer el derecho de intimidad y el respeto sobre la información sensible (art. 4). Estos son: "pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias".

Sobre los datos sensibles se prohíbe su publicación o divulgación, pero no se observan sanciones en caso de abusos por cualquier entidad pública o privada. Por lo tanto, la acción de defensa ante un abuso queda exclusivamente en manos de la persona afectada.

De lo anterior se deduce que para la Ley existen datos personales de carácter no público, que tampoco son sensibles, como podrían ser número de teléfono particular, número de celular, estatura, tipo de sangre, etc.

Además se presentan dos categorías de datos más, pero que no están claramente definidas: *dato caduco y dato estadístico*[13]. El primero es aquel que ha perdido actualidad por disposición de la Ley, cumplimiento de la condición o expiración del plazo señalado para su vigencia, cambio de los hechos

11 El Plan Nacional de Ciberseguridad está disponible en http://gestordocumental.senatics.gov.py/share/s/m2uDswEUTDmrDBY2NFttIg

12 Ver artículo con comentarios acerca del Plan Nacional de Ciberseguridad en Paraguay en: https://www.tedic.org/aspecto-positivos-y-negativos-del-plan-de-ciberseguridad-en-paraguay/

13 Según Alberto Cerda un dato caduco es *"aquel que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna". Por su parte, dato estadístico es "el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable. Este último queda, por tanto, fuera del ámbito de aplicación de la ley" (Cerda Silva, 2011).*

o circunstancias que consigna si no hay norma expresa. Por su parte, un dato estadístico es aquel que no puede ser asociado a un titular identificado o identificable. Esto último se aparta de los estándares actuales de protección de datos dejando libre interpretación y mucha vulnerabilidad para la efectiva protección de la privacidad de las personas.

Principio de Calidad del Dato

El requisito de calidad del dato forma parte de los principios rectores de la Ley y se encuentra en el artículo .Pero nuevamente se limita a los informes crediticios, tales como situación patrimonial, solvencia económica y cumplimiento de obligaciones comerciales y financieras, obligando la actualización constante por parte de las empresas .

El artículo 7 de la Ley Nº 1682/2001, modificado por la Ley No 1969/2002, dispone en el párrafo final:

> *"En caso que los datos personales fuesen erróneos, inexactos, equívocos o incompletos y así se acredite, el afectado tendrá derecho a que se modifiquen. La actualización, modificación o eliminación de los datos será absolutamente gratuita, debiendo proporcionarse, además, a solicitud del afectado y sin costo alguno, copia auténtica del registro alterado en la parte pertinente".*

Relacionado con esto, se encuentran los derechos arco que se explican a continuación.

Principio de participación individual: Derechos ARCO

El concepto de derechos ARCO hace referencia a los derechos de acceso, rectificación, cancelación y oposición sobre los datos de carácter personal. En la Ley actual son de aplicación exclusiva a los sistemas de información crediticia en las entidades bancarias y financieras. Cualquier ejercicio fuera de este ámbito se deberá llevar a cabo mediante el procedimiento de hábeas data. Si bien la presente Ley no contempla la definición legal de "Titular del dato", sí considera derechos al titular del dato como en los derechos ARCO.

El derecho de acceso (o de información) se encuentra en al artículo 8 de la Ley, que dispone lo siguiente:

> *"Toda persona podrá acceder a la información y a los datos que sobre sí misma, sobre su cónyuge, sobre personas que acredite se hallen bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, así como conocer el uso que se haga de los mismos o su finalidad."*

Los derechos ARCO son personalísimos[14], lo que indica que deben ser ejercidos por el titular de derechos o por su representante legal, pero en el artículo 8 se establece que cualquier persona puede solicitar información sobre su cónyuge, abriendo la posibilidad a confusiones a la hora de interpretar este derecho como personalísimo.

14 "Personalísimo" se dice de aquel tan íntimamente consustanciado con la persona, que no es transmisible por serle inherente. (Montoya Melgar, 1995)

Otra carencia es la del requisito de consentimiento expreso: derecho principal y personalísimo del titular del dato personal. Esto implica que toda persona debe ser informada sobre el propósito del almacenamiento de sus datos y su eventual publicación. Además debe haber una autorización de forma expresa y/o por escrito, y puede ser revocada sin necesidad de causa justificada (sin efecto retroactivo).

El derecho de rectificación y cancelación[15] se observa en el artículo 7 de la ley, modificado por la Ley N° 1969/2002 y expresa lo siguiente:

> *"Serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales y financieras que, de acuerdo con esta Ley, pueden difundirse. La obligación de actualizar los datos mencionados pesan sobre las empresas, personas y entidades que almacenan, procesan y difunden esa información..."*

Este artículo explica que las modificaciones a los datos personales, se realizarán a partir del reclamo realizado por parte del afectado, o titular del dato, a los responsables del dato que están obligados a mantenerlos actualizados.

El derecho de oposición no se contempla expresamente en la Ley. Consiste en la facultad que posee el titular de los datos para dirigirse al responsable del archivo, registro o banco de datos públicos o privados y solicitar la cancelación del tratamiento de sus datos. Puede ser por las siguientes razones: cuando no existe consentimiento (salvo las fuentes públicas), cuando el tratamiento lo realiza con fines publicitarios y cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada unicamente en un tratamiento automatizado de sus datos personales. Ninguno de estos aspectos están contemplados en la Ley ni en sus modificaciones.

Principio de Responsabilidad Proactiva: Acciones y Responsabilidad

El deber de mantener actualizado los archivos, registros en cualquiera de sus formas de tratamiento de datos destinados a dar informes recae en los responsables del tratamiento de datos que pueden ser: personas físicas, empresas o entidades que suministran información.

El artículo 9 de la Ley, en su párrafo final establece que:

> *"Las empresas o entidades que suministren información sobre la situación patrimonial, la solvencia económica y el cumplimiento de compromisos comerciales y financieros deberán implementar mecanismos informáticos que de manera automática eliminen de su sistema de información los datos no publicables, conforme se cumplan los plazos establecidos en este artículo".*

Principio de Limitación del plazo de conservación

La presente ley establece limitaciones en el tiempo necesario para los fines del tratamiento de los datos personales, pero solo limita su transmisión y divulgación según lo expresado en el Art 9 de la Ley 5543/2015 y el mismo artículo en la ley 1969/02. Por el cual las empresas, personas o entidades que suministran información sobre la situación patrimonial, la solvencia económica o

15 La Ley tuvo modificaciones en 2015, que complementan al art 7 de la ley 1969/02. A partir de entonces se obliga a actualizar las bases de datos y actualizar la información de los deudores sobre los jornales mínimos que no deberán ser incorporadas en la lista de Informconf (deudas menores a 50 jornales mínimos -poco más de 3 millones de guaraníes). También tuvo una rectificación sobre información demostrable a través de cualquier documento idóneo, cuando la deuda es saldada, http://www.abc.com.py/nacionales/modifican-ley-de-informconf-1312696.html

sobre el cumplimiento de obligaciones comerciales no podrán transmitir ni divulgar. Sin embargo no se habla de la eliminación de los datos una vez transcurrido un tiempo determinado, esta acción podrá realizarse a pedido del titular del dato.

Código penal

Esta legislación aplicable en materia penal contempla normas jurídicas punitivas que protegen la intimidad en la jurisdicción paraguaya y que complementa a las salvaguardas que el Estado debe tener para la protección de los datos personales en el país.

El Código Penal, Ley N° 1160/97 tipifica en el capítulo VII los hechos punibles contra el ámbito de vida y la intimidad de la persona. Entre ellos se encuentran, artículo 141.- Violación de domicilio, artículo 144.- Lesión del derecho a la comunicación y a la imagen, artículo 146.- Violación del secreto de la comunicación y el artículo 143.- Lesión a la intimidad de la persona. Este último hace alusión directa a la exposición pública de la intimidad de la persona, de su vida familiar, sexual y su estado de salud.

El código penal también se utiliza para sancionar el incumplimiento de las empresas y entidades que suministran información sobre la situación patrimonial, la solvencia económica y el cumplimiento de compromisos comerciales y financieros. Además suele servir para forzar a las empresas a que implementen mecanismos informáticos que eliminen de manera automática la información de los datos no publicables, conforme a la Ley 1682/01 y modificaciones.

Código de Organización Judicial

La ley 1682/01 modificada por la Ley 1969/02, en su artículo 2 establece que todo lo asentado en los registros públicos son de libre acceso, incluyendo la Ley 879 Código de Organización Judicial. Por lo tanto, los registros creados por esta última, son públicos y accesibles “para quien tenga interés justificado en averiguar el estado de los bienes inmuebles o derechos reales inscriptos” (art. 328 (Congreso Nacional, 1981)).

Estos registros del órgano judicial revelan la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales y financieras de las personas. Asimismo según este código, estos registros pueden ser difundidos si el titular del dato otorga su consentimiento por escrito, salvo el cumplimiento de las obligaciones legales de la autoridad pública o justificadas en el interés público.

Ley N° 642/95 de Telecomunicaciones

Dicha ley regula todo tipo de emisión y propagación de las señales de comunicación electromagnéticas que son de dominio público del Estado. Asimismo crea al ente regulador denominado Comisión Nacional de Telecomunicaciones (CONATEL) que deberá velar por el cumplimiento de la ley.

La misma incluye aspectos de tratamientos de datos en el Título IX Régimen de protección a abonados y usuarios:

> *Artículo 91.-Es obligación de los titulares de la explotación de servicios públicos de telecomunicaciones publicar y distribuir en forma gratuita las guías y nómina de sus respectivos usuarios abonados, de conformidad con las normas reglamentarias correspondientes. Los usuarios tendrán derecho a la no inclusión de sus nombres en dichas guías y nóminas.*

Esta ley implica que cualquier licenciatario de las frecuencias de dominio de telecomunicaciones como por ejemplo la Telefónica, tiene la facultad de publicar su registro de abonados a través de su guía telefónica. Sin embargo cualquier titular del dato podrá oponerse en la publicación de sus datos personales.

Resolución 1350/2002 Por el cual se establece la Obligatoriedad de registro de detalles de llamadas por el plazo de seis (6) meses

La Resolución 1350/2002 de Conatel[16] contradice la Ley 642/95 de Telecomunicaciones expresados en los artículos 89 y 90 sobre la inviolabilidad de de la correspondencia de las telecomunicaciones y el Decreto del Poder Ejecutivo 14135/96[17]. Esta Resolución otorga facultades a las compañías operadoras de servicios de telefonía a almacenar por un periodo de seis meses el registro de detalles de llamadas de todos los usuarios en Paraguay:

> *Artículo. 1.- Establecer el plazo de seis (6) meses, como periodo obligatorio de conservación del registro de detalles de llamadas entrantes y salientes de todas las líneas que conforman la cartera de clientes de las diferentes operadoras del servicio de telefonía móvil celular (STMC) y/o Sistema de Comunicación Personal (PCS).*

Los registros de llamadas telefónicas, los SMS y los datos de localización de dispositivos móviles ya son almacenados por un periodo de 6 meses mediante la Resolución de Conatel que data del año 2002, tiempo donde ocurrieron varios secuestros extorsivos que sacudieron a la sociedad paraguaya[18].

Esta medida pre-investigativa para cualquier tipo de ilícito no sólo refleja una desproporción en cuanto al fin perseguido. Y obviamente deja de lado el ideal de una intervención mínima a través del aparato punitivo del Estado, propio de lo que se denomina “derecho penal mínimo”.[19]

Ley de Comercio Electrónico y su el decreto reglamentario

El objetivo de la Ley 4868/2013 de Comercio Electrónico es regular todo lo concerniente al comercio y contrataciones realizados a través de Internet o medios tecnológicos equivalentes. En el capítulo primero sobre “Principio de libertad de concurrencia” se contemplan una serie de

16 Comisión Nacional de Telecomunicaciones (CONATEL). RESOLUCIÓN Nº 1350/2002.- Por la cual se establece la obligatoriedad de registro de detalles de llamadas por el plazo de seis meses. (Comisión Nacional de Telecomunicaciones (CONATEL), s. f.)

17 Por el cual se aprueba las normas reglamentarias («Ley Nº 642/95 “De telecomunicaciones”.», s. f.)

18 Última Hora. Los casos de secuestros en Paraguay. Disponible en: http://www.ultimahora.com/los-casos-secuestros-paraguay-n460811.html [Fecha de consulta: 5 de enero, 2017].

19 “Derecho penal mínimo significa la reducción al mínimo de las circunstancias penales y su codificación general mediante la despenalización de todas aquellas conducta que no ofendan bienes fundamentales y que saturan el trabajo judicial con un dispendio inútil e inocuo de aquel recurso escaso y costoso que es la pena y tienen el triple efecto del debilitamiento general de las garantías, de la ineficacia de la maquinaria judicial y de la devaluación de los bienes jurídicos merecedores de tutela penal.” Ferrajoli, Luigi. Crisis del sistema político y jurisdicción: la naturaleza de la crisis italiana y el rol de la magistratura. Revista Pena y Estado año 1 número 1–Argentina 1995: Editores del Puerto s.r.l. p. 113.

restricciones que se consideran invulnerables, entre las que se encuentran la protección de las personas en condición de consumidores o usuarios y la protección de los datos personales, intimidad personal y familiar de las partes o terceros, y la confidencialidad de los registros y cuentas bancarias (art. 6).

En la ley se establecen condiciones mínimas para la protección, como las responsabilidades de los proveedores (capítulo III), notificación de infracción a derechos de terceros (art. 18) y los derechos de los consumidores o usuarios (art. 30).

Por otro lado, se obliga a las empresas a almacenar los metadatos de sus usuarios por un mínimo de 6 meses según el artículo 10 de la ley de Comercio Electrónico 4868/2013[20]. Para salvaguardar el derecho constitucional que hemos descrito como "autodeterminación informativa"[21] es imprescindible, que las ISP comuniquen a sus usuarios qué información personal están reteniendo así como las medidas para salvaguardar sus datos personales ante posibles ataques o amenazas sobre dicha información.

El artículo 10 de la mencionada ley establece:

> *"Los Proveedores de Servicios de Intermediación y los Proveedores de Servicios de Alojamiento de Datos deberán almacenar los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio, por un período mínimo de 6 (seis) meses, en los términos establecidos en este artículo. Para el cumplimiento de lo dispuesto en este artículo, los datos serán almacenados únicamente a los efectos de facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.*
> *Los Proveedores de Servicios de Alojamiento de Datos deberán almacenar sólo aquéllos datos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.*
> *No podrán utilizar los datos almacenados para fines distintos a los que estén permitidos por la ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos".*

Por otro lado, la ley 4868/2013 de Comercio Electrónico y su decreto reglamentario 1165/14, obliga a informar y proteger los datos de los usuarios compulsivamente; en su artículo 9 establece:

> *"Obligación de los Proveedores de Servicios de Intermediación. Los Proveedores de Servicios de Intermediación consistentes en la prestación de servicios de acceso a Internet, estarán obligados, sin perjuicio de las disposiciones vigentes sobre los Servicios de Acceso a Internet y Transmisión de Datos establecidas por la Autoridad Competente, a: a) informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de*

20 Esta legislación sirvió como antecedente para crear el proyecto de ley de "Conservación obligatoria de datos de tráfico" que pretendía obligar a las ISP al almacenamiento masivo de metadatos de comunicaciones de todos los usuarios por un periodo de 12 meses con fines de "investigación criminal". La iniciativa llegó a tener media sanción en el Congreso a finales del año 2014 pero tras una fuerte campaña de concientización y rechazo de los riesgos implicados, el Senado rechazó la propuesta. La campaña se llamó "Pyrawebs" y está disponible en https://pyrawebs.tedic.org/

21 La autodeterminación informativa complementa de manera positiva el derecho a la privacidad/intimidad, ya que no sólo se trata de la imposibilidad que tienen terceros de entrometerse en lo que sucede en la vida de una persona, sino en la posibilidad que la persona tiene de controlar la información concerniente a ella misma y excluirla del conocimiento de aquellos, con antelación o aún una vez que dicha información se ha hecho circular.

> *la seguridad de la información y permitan, entre otras cosas, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados; b) informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios no deseados en Internet o que puedan resultar nocivos para la niñez y la adolescencia; Esta obligación de información se tendrá por cumplida si el correspondiente Proveedor incluye la información exigida en su página o sitio principal de Internet. a) suspender el acceso a un contenido o servicio cuando un órgano competente, en ejercicio de las competencias que legalmente tenga atribuidas, requiera que se interrumpa la prestación de un servicio o que se retire algún contenido que vulnere lo dispuesto en el Artículo 6°".*

En el artículo 11 del decreto reglamentario 1165/14 establece:

> *"Deber de Informar y Protección de Datos. El proveedor de bienes y servicios por vía electrónica a distancia, debe poner a conocimiento del consumidor o usuario la finalidad y el tratamiento que se le daría sus datos personales, conforme a la Ley vigente relativa a la materia. Así mismo, debe comunicar el destinatario de los datos suministrados y el responsable de custodiar o almacenar la información proporcionada. El proveedor de bienes y servicios empleará sistemas seguros para evitar la pérdida, alteración y acceso de terceros no autorizados a los datos suministrados por el consumidor o usuario".*

La Institución garante y responsable del monitoreo del cumplimiento de la Ley de Comercio Electrónico es el Ministerio de Industria y Comercio, que tiene como atribución la coordinación de inspecciones y controles a los distintos proveedores de Internet. Inclusive debe aplicar sanciones por las faltas no previstas específicamente en la Ley de Defensa del Consumidor y las establecidas en la Ley de Comercio Electrónico.

Ley 861/96 General de Bancos, Financieras y otras entidades de crédito

El capítulo II de la ley 861/96 del Deber secreto, en su artículo 84 – Secreto sobre las operaciones - establece:

> *"Prohíbese a las Entidades del Sistema Financiero, así como a sus directores, órganos de administración y fiscalización y trabajadores, suministrar cualquier información sobre las operaciones con sus clientes, a menos que medie autorización escrita de éstos o se trate de los supuestos consignados en los artículos siguientes. La prohibición no alcanzará a los casos en que la divulgación de las sumas recibidas de los distintos clientes resulte obligada para los fines de liquidación de las entidades bancarias o financieras".*

Este artículo y subsiguientes establecen reglas mínimas en la publicación y divulgación de información de carácter personal incluyendo sanciones administrativas en caso de incumplimiento sin perjuicio de las responsabilidades penales establecidas por las leyes.

Ley 125-1991 Que establece el Nuevo Régimen Tributario

En el Capítulo VI de los Deberes de la administración en artículo 190[22] expresa:

> *"Secreto de las actuaciones: Las declaraciones, documentos, informaciones o denuncias que la Administración reciba y obtenga tendrán carácter reservado y sólo podrán ser utilizados, para los fines propios de la Administración. Los funcionarios de ésta no podrán, bajo pena de destitución y sin perjuicio de su responsabilidad personal, civil y/o penal, divulgar a terceros en forma alguna datos contenidos en aquellas. El mismo deber de reserva pesará sobre quienes no perteneciendo a la Administración Tributaria, realicen para ésta trabajos o procesamientos automáticos de datos u otras labores que importan el manejo de material reservado de la Administración Tributaria.*
>
> *Las informaciones comprendidas en este articulo, solo podrán ser proporcionadas a los órganos jurisdiccionales que conocen los procedimientos sobre tributos y su cobro, infracciones fiscales, débitos comunes, pensiones alimenticias y causas de familia o matrimoniales, cuando entendieran que resulta imprescindible para el cumplimiento de sus fines y lo soliciten por resolución fundada. Sobre la información así proporcionada regirá el mismo secreto y sanciones establecidas en el párrafo segundo"*

La Institución responsable del tratamiento de los datos de recaudación fiscal del Paraguay y de la aplicación de la Ley es el Ministerio de Hacienda. El acceso a los datos personales recolectados por esta ley sólo se podrá realizar a través de los titulares de los datos o sus representantes legales.

Resolución N° 77/16 de la Secretaría de Estado de Tributación – Ministerio de Hacienda

La resolución N° 77 vigente desde febrero de 2016 pretende mejorar la verificación de información de los contribuyentes a través de tecnología, y así evitar operaciones fraudulentas. La misma se enmarca en el cumplimiento del plan estratégico de la Subsecretaría de Estado de Tributación (SET). Algunas de estas operaciones fraudulentas que se pretenden combatir son las grandes evasiones a través de inscripciones de RUC sin consentimiento y que llevan a la emisión de facturas falsas. Según publicaciones periodísticas (Color, 2017) entre los años 2013 al 2016 se reportaron unos 100 de estos casos, que actualmente se encuentran judicializados.

Asimismo, las declaraciones oficiales explican que el registro actual de datos biométricos es gratuito y que dicha actualización es voluntaria, conforme lo dispone el Art 8 de la Res 77/16. Sin embargo, el sistema "marangatu" del SET bloquea los perfiles de acceso a las personas jurídicas, obligando la actualización en el sistema de forma presencial. Una vez que las personas se presentan, se realiza la inscripción compulsiva de los datos biométricos de los apoderados legales. Esto contradice claramente el carácter voluntario que expresa el comunicado oficial.

Con respecto a medidas proporcionales y datos biométricos, El ex Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales, Martin Scheinin, determinó en su informe publicado en el año 2009, que el uso de biometría puede ser legítimo para ciertas circunstancias como casos de terrorismo, le preocupa especialmente:

22 Ley Régimen Tributario (Congreso Nacional, 1991, p. 91).

"*los casos en que la biometría no se almacena en un documento de identidad, sino en una base de datos centralizada, incrementando los riesgos para la seguridad de la información y dejando a los individuos vulnerables. A medida que aumenta la información biométrica, las tasas de error pueden aumentar significativamente [...] El incremento en las tasas de error puede llevar a la criminalización ilícita de individuos o a la exclusión social"*

Por otra parte el Relator destaca un elemento clave sobre la irrevocabilidad de los datos biométricos:

"*Una vez copiados y/o utilizados fraudulentamente por un actor malicioso, no es posible emitirle a un individuo una nueva firma [identidad] biométrica"*

Por tanto se vuelve indispensable pensar una ley de protección de datos personales que contemple estos avances tecnológicos y que apunten a limitar los focos de posibles abusos y se analice con perspectiva de derechos.

Ley de Acceso a la Información Pública

El derecho a la información y el derecho a la protección de datos personales son derechos complementarios que se definen en leyes "hermanas". A priori no existe una verdadera colisión o conflicto entre ambos derechos, sin embargo la necesidad de transparencia debe conciliar con el interés jurídico tutelado por las leyes, tales como los derechos fundamentales de las personas, y en especial con el derecho a la privacidad.

El acceso a la información generada en la administración pública se rige por la Ley 5282/14, que está vigente desde abril de 2015 a través del decreto su reglamentario 4064/15. La misma se encuentra íntimamente relacionada con el artículo 28 de la CN. El artículo 1 de la mencionada Ley dispone que su objeto es:

> *"[...] garantizar a todas las personas, el efectivo ejercicio del derecho al acceso a la información pública, a través de la implementación de las modalidades, plazos, excepciones y sanciones correspondientes, que promuevan la transparencia del Estado"(Congreso Nacional, 2014).*

En su artículo 2, se define información pública y al mismo tiempo se establece las excepciones: información pública es aquella "producida, obtenida, bajo control o en poder de las fuentes públicas, independientemente de su formato, soporte, fecha de creación, origen, clasificación o procesamiento, salvo que se encuentre establecida como secreta o de carácter reservado por las leyes"(Congreso Nacional, 2014).

El artículo 22 por su parte se refiere a la información pública reservada, pero sin profundizar en su significado indicando alguna norma legislativa. Se limita a definirla como "aquella que ha sido o sea calificada o determinada como tal en forma expresa por la ley"(Congreso Nacional, 2014).

De igual manera, las instituciones están obligadas a seguir el principio de transparencia activa según el artículo 14 del reglamento 4064/15 de la Ley, mediante el cual deben publicar progresivamente en sus sitios web oficiales "toda la información pública que obre en su poder, salvo la que se encuentre establecida como secreta o de carácter reservado por las leyes"(Presidencia de la República, 2015)

Cabe notar que la definición de información secreta o de carácter reservado no se encuentra disponible en las leyes, lo que podría generar ambigüedades en la aplicación de la Ley. Sin embargo, los límites de la Ley se encuentran bien establecidos en su artículo 18 y en los artículos 34 y 35 del reglamento. El artículo 18 se refiere a las bases de datos públicas, y es explícito en la prohibición de la salida de datos o "… registros originales de los archivos de las fuentes públicas en los que se hallen almacenados [...]"(Congreso Nacional, 2014). El artículo 34 del reglamento establece el mecanismo de rechazo a una solicitud de información pública, la cual debe estar fundada "en una norma jurídica con una jerarquía no inferior a la de la ley"(Presidencia de la República, 2015), como por ejemplo la Ley 1969/02 que reglamenta la información de carácter privado. Mas es el artículo 35 del reglamento el que sienta las bases para la resolución de controversias entre el acceso a la información y la protección de la privacidad o la gestión de los datos personales.

Los criterios para el rechazo a una solicitud de información pública se sustentan en lo que propone la Ley Modelo de Acceso a la Información de la OEA (Torres, s. f.). Incorpora efectivamente el test de interés público como guía máxima para la aplicación de las excepciones. Afirma en el artículo 35 que la fuente pública deberá fundamentar una denegatoria demostrando que la información se ajusta a un caso de excepción, teniendo en consideración:

> *"a) que la excepción es legítima y estrictamente necesaria en una sociedad democrática sobre la base de los estándares y jurisprudencia del sistema interamericano de protección de los derechos humanos;*
>
> *b) que la divulgación de la información podría causar un daño sustancial a un interés protegido por la ley; y*
>
> *c) que la probabilidad y el grado de dicho daño es superior al interés público en la divulgación de la información"*(Presidencia de la República, 2015)

El artículo 36 ofrece otro camino de resolución en caso de tensión entre el derecho al acceso a la información y la protección de la privacidad o la gestión de datos personales. En línea con la Ley Modelo de OEA para cumplir con los estándares del sistema interamericano sobre el régimen de excepciones, establece el principio de "in dubio pro acceso". Esto es, en palabras del reglamento:

> *"en caso de duda razonable entre si la información solicitada está amparada por el principio de publicidad, o se encuentra alcanzada por una causal de excepción, se debe optar por la publicidad de la información"*(Presidencia de la República, 2015).

Finalmente, el artículo 37 promueve la divulgación parcial de la información en caso que un documenta contenga información que debe ser publicada e información que es causal de excepción. En tal situación, se debe divulgar la información que puede ser conocida(Presidencia de la República, 2015).

El órgano de aplicación de la Ley son las Oficinas de Acceso a Información, según el artículo 10 del reglamento, que deben ser creadas por cada institución pública y que dependen de su máxima autoridad. Las denegatorias de acceso a información pública deben ser dictadas por esta autoridad(Presidencia de la República, 2015). ga

La Ley “Que prohibe la publicidad no autorizada por los usuarios titulares de telefonía movil”.

La presente ley[23] fue sancionada en el congreso en mayo de 2017, actualmente se encuentra en etapa de publicación en el Poder Ejecutivo, por tanto no se cuenta con la numeración y la vigencia hasta el cierre de esta investigación.

Según los proyectistas, esta ley anti-spam está inspirada en la la normativa argentina coloquialmente denominada “No me llames”[24], que establece un listado de personas que no desean recibir la publicidad no solicitada. En Paraguay dicho listado será administrado por la Secretaria del Defensa al Consumidor y el Usuario (SEDECO). En caso que esta solicitud sea ignorada y la persona reciba publicidad no deseada, será ella misma que podría accionar legalmente contra el emisor del mensaje (Art 6).

Sin embargo, esta nueva Ley vigente no soluciona el problema de fondo, pues carece de un enfoque integral para el tratamiento de datos personales. Un problema tan complejo como el de los datos personales en la actualidad, no se puede abordar con regulaciones que simplemente prohíban el spam, que no tomen acciones contra la venta descontrolada de bases de datos personales y que dejen en soledad a las personas en el caso de posibles abusos. La protección de los datos personales debe ser enfrentada con un enfoque de derechos, aplicando como piedra angular, la estructura del sistema de protección de datos personales que son: el consentimiento y la autodeterminación informativa.

Por otro lado, no se tuvo en cuenta la Ley 4868/13 de Comercio Electrónico sobre regulación de publicidad no autorizada, que está vigente y tiene un apartado específico sobre publicidad no deseada en sus artículos 20 al 23. Lo que establece es que en caso que los proveedores de bienes y servicios deseen enviar comunicaciones no solicitadas, deben indicar expresamente que la misma no fue solicitada; incluir formas sencillas de salida del usuario de la lista de destinatarios; y que los mismos no hayan infringido los derechos de privacidad (art 23), buscando un balance entre “*prohibición al envío sin autorización*” y “*comercio*”.

Con relación a esta Ley anti-spam, el consentimiento debe ser previo a una lista del tipo “*No me llames*”. El mismo debe aplicar al tratamiento de los datos personales desde su misma recolección. La persona debe consentir de manera previa, expresa, libre e informada sobre el tratamiento de sus datos, en el momento mismo de la recolección, es decir los fines para los cuales son recolectados y almacenados independientemente de estar o no en una lista “*No me llames*”.

Este debate debe contemplar también los problemas que podría generar una cesión de datos personales, si se recolectan o usan fuera de la competencia del sector público o privado.

23 Sistema de Información Legislativa (SILPY) Trámite de la ley http://sil2py.senado.gov.py/formulario/FichaTecnicaExpediente.pmf?q=FichaTecnicaExpediente%2F107665

24 La Cámara de Diputados aprueba ley contra mensajes molestos. Fecha 6 diciembre 2016 http://www.ultimahora.com/diputados-aprueba-ley-contra-mensajes-molestos-n1045679.html

Jurisprudencia nacional e internacional

A continuación se desarrolla una serie de casos tanto a nivel nacional como internacional, que sientan precedentes sobre cómo aplicar las normas referentes al tema en estudio; esto es lo que se conoce como jurisprudencia y puede ser de gran utilidad para la creación de nueva legislación en la materia, así como para futuros casos judiciales.

CIDH: Caso Escher y otros vs. Brasil.

La Corte Interamericana de Derechos Humanos (CIDH) sobre el caso contencioso en el que se condenó a Brasil (CIDH, 2009) por el uso ilegal de escuchas telefónicas en un proceso penal. La Corte señaló que el derecho a la privacidad protege tanto al contenido de la comunicación electrónica como a otros datos propios del proceso técnico de la comunicación. Estos incluyen los metadatos o datos de tráfico, entendidos éstos como "el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar contenido de la llamada mediante la grabación de las conversaciones."

Esta jurisprudencia es vinculante a nuestra jurisdicción nacional ya que Paraguay reconoce a la corte como una instancia Internacional de tratamiento de derechos humanos. Además el Artículo 31.1 de la Convención de Viena (OEA, 1961), dispone que si un Estado firma un tratado Internacional –particularmente en el ámbito de los derechos humanos– tiene la obligación de realizar sus mejores esfuerzos para aplicar los pronunciamientos de los órganos supranacionales correspondientes (Fuenzalida Bascuñán, 2015).

Por tanto esta sentencia de la CIDH debe tomarse en cuenta para el cumplimiento de la protección de los Derechos Humanos. Por otra parte, implica el acatamiento de los tratados y directivas de San José que imponen la responsabilidad internacional del Estado en cualquiera de sus tres poderes. (art. 1.1 y 2 del Pacto de San José).

La sentencia de la Corte Suprema N°674/10, Caso Cecilia Cubas

La sentencia de la Corte Suprema del Poder Judicial paraguayo N° 674/10[25] sobre el recurso extraordinario de casación solicitado por los acusados del secuestro y asesinato de Cecilia Cubas, fue declarado *no ha lugar*. Este emblemático caso involucró a la hija del ex Presidente de la República, Raúl Cubas Grau (agosto 1998 – marzo 1999) quien fue secuestrada el 21 de septiembre de 2004, cuando un grupo de criminales rodeó su vehículo a metros de su domicilio en las afueras de la capital Asunción. Cubas fue hallada muerta el 16 de febrero de 2005 (ABC Color, s. f.).

La Corte Suprema expresó que se cumplieron todas las garantías procesales y que no hubo violación de las comunicaciones por parte de la Fiscalía, al solicitar sin orden judicial, los metadatos de las llamadas telefónicas producidas por los sospechosos autores del secuestro.

> *"La respuesta brindada por el Tribunal de Alzada fue expresa y satisfactoria. De conformidad al articulo 228 del CPP, el Ministerio Público puede solicitar informes a cualquier persona o entidad pública o privada. El artículo 316 del CPP dentro de las facultades del Ministerio Público, reafirma*

25 Acuerdo y Sentencia Nº 674/10 "Recurso Extraordinario De Casación Interpuesto Por La Defensora Pública Sandra Rodríguez Samudio En La Causa Anastacio Mieres Burgos Y Otros S/ Secuestro Y Otros". Expte. N° 773, Folio 245

> *que "podrá exigir informaciones de cualquier funcionario o empleado público, conforme a las circunstancias del caso. Todas las autoridades públicas están obligadas a colaborar con la investigación, según sus respectivas competencias y a cumplir las solicitudes o pedidos de informes que se realicen conforme a la ley"* [26].

Además, el Ministerio Público accedió a los informes, para luego procesarlos, y esto no implicó vulneración alguna, ya fuera de orden constitucional o legal. Como bien se ilustró, la información brindada facilitó acceder a los datos de los titulares de línea, la fecha, hora, número de teléfono entrante y saliente, y el lugar geográfico de donde se realizaban. A lo que se accedió fue al detalle del cruzamiento de llamadas, y no al contenido de las mismas. En caso que se hubiese accedido al contenido, sí se hubieran vulnerado la *inviolabilidad de las comunicaciones* y el *derecho a la intimidad*.

En resumen, el análisis de la Corte Suprema sobre la inviolabilidad de la comunicación y acceso a datos personales es[27]:

- Lo prescrito por el artículo 36 de la Constitución de la República, sobre del derecho a la inviolabilidad del patrimonio documental y la comunicación privada, protege la comunicación en sí: las palabras que pudieron haberse dicho las partes acusadas en este proceso a través de un teléfono. No así los consecuentes de estas comunicaciones, que fueron el objeto de trabajo por parte del perito.
- Prueba pericial sobre cruce de llamadas: En el peritaje del cruce de llamadas, se colige que los datos aludidos son las anotaciones de la telefónica consistentes en el número telefónico investigado, las llamadas entrantes y salientes de dicho número así como los horarios de las mismas; nada de esto hace a la comunicación telefónica que consiste en el mensaje que una persona dice y otra escucha por medio de un aparato telefónico.
- Prueba de peritos: En el peritaje del cruce de llamadas se trabaja sobre los datos que quedan asentados en las llamadas telefónicas de manera posterior a una comunicación, y no sobre las comunicaciones que generaron dichos datos. La CR protege la comunicación, pero no el cruce de llamadas que fue el objeto del peritaje.
- En el peritaje del cruce de llamadas, dado que la comunicación en sí no fue objeto de peritaje sino los datos que arrojó dicha comunicación, la orden judicial no era obligatoria pues el trabajo pericial no afectaba al ámbito de protección constitucional.
- En el peritaje del cruce de llamadas la comunicación telefónica no fue examinada, no se sabe con certeza lo que se pudieron haber dicho las personas poseedoras de los números investigados. Se concluye que no fue interceptada, ya que no consta que un tercero haya estado escuchando dicha comunicación con tecnología apropiada para ello. Por lo tanto tampoco ha podido grabarla ni reproducirla.

Es preocupante que la Corte haya tenido estas consideraciones sin evaluar los criterios internacionales que se deberían aplicar sobre el tema de los metadatos. Analizando desde la perspectiva de la aplicación de los Derechos Humanos en la Vigilancia de la Comunicaciones, se considera que el Ministerio Público no posee la atribución de requerir informes de tal característica, porque vulnera la privacidad y los datos personales, más aún habiéndolos solicitado sin orden judicial.

26 Corte Suprema de Justicia. Sala Penal: Materia Penal. Inviolabilidad De La Comunicación Privada. Pruebas. Medios De Prueba. Prueba De Peritos. Cruce De Llamadas. Acuerdo Y Sentencia N° 711 Del 20/08/14.

27 Basado en el análisis (Jorge Rolón Luna, Maricarmen Sequera Buzarquis, 2016)

Ricardo Canese vs Paraguay (Fondo, Reparaciones y Costas)

Corte Interamericana de Derechos Humanos Caso Ricardo Canese Vs. Paraguay Sentencia de 31 de agosto de 2004 (Fondo, Reparaciones y Costas). El presente caso se refiere a la responsabilidad internacional del Estado por la condena en un proceso de difamación y calumnia, y las restricciones para salir del país impuestas en perjuicio Ricardo Nicolás Canese Krivoshein.

Los hechos del presente caso se iniciaron en agosto de 1992, durante el debate de la contienda electoral para las elecciones presidenciales del Paraguay de 1993. El señor Ricardo Canese, quien era candidato presidencial, declaró en contra de Juan Carlos Wasmosy, también candidato, por presuntas acciones ilícitas cuando era el presidente de un consorcio. El 23 de octubre de 1992, los directores del consorcio presentaron una querella criminal ante el Juzgado de Primera Instancia en lo Criminal en contra del señor Ricardo Canese, por los delitos de difamación e injuria. El 22 de marzo de 1994, fue condenado en primera instancia, y el 4 de noviembre de 1997 fue condenado en segunda instancia a una pena de dos meses de pena privativa de la libertad y a una multa de 2,909,000 guaraníes. Como consecuencia del proceso penal en su contra, el señor Canese fue sometido a una restricción permanente para salir del país. El 11 de diciembre de 2002, la Sala Penal de la Corte Suprema de Justicia del Paraguay anuló las sentencias condenatorias contra el señor Canese dictadas en 1994 y 1997.

Cabe destacar que este litigio es transcendental para reafirmar el derecho al acceso a al información pública y los límites de la protección de los datos personales en pos del interés público. La sentencia hace hincapié en la necesidad de que los ciudadanos conozcan la información de los candidatos a puestos públicos para que les permita tomar las decisiones acertadas a la hora de votar en las elecciones nacionales, sin restricciones y que de ese modo se respete la libertad de expresión como herramienta esencial para la formación de la opinión pública.

Instancias Internacionales

La agenda sobre la protección de datos personales se encuentra en discusión hace bastante tiempo en instancias Internacionales. Paraguay forma parte de varios grupos de trabajo, con el compromiso de adecuar la ley de 1682/2001 a los estándares de la Directiva de la Unión Europea y al nuevo escenario de economía digital.

Mercado Común del Sur

La constitución del Mercado Común del Sur (MERCOSUR) busca la libre circulación de personas, bienes y capitales y se realizó a través del Tratado de Asunción. La cualidad de este organismo que buscar regular esta circulación que incluye la transferencias de datos a otros países, en sectores como recursos humanos, servicios financieros, comercio electrónico, educación que forman parte de la economía digital global trae aparejada la protección de los derechos fundamentales de los ciudadanos, adecuando los instrumentos legales al proceso de innovación tecnológica, económica, social y cultural.

En este marco se creó la iniciativa MERCOSUR Digital para el tratamiento de datos entre el bloque y la Unión Europea; actualmente este proceso se encuentra sin muchos avances (MERCOSUR, 2008).

Organización de Estados Americanos

El Departamento de Derecho Internacional dependiente de la Secretaría de Asuntos Jurídicos (SAJ) de la OEA, se encuentra liderando el trabajo de La Red de Protección de Datos (RID).

Nuestro país es observador de la red a través de la Secretaría de la Función Pública[28]. Uno de sus objetivos es la creación de una "ley modelo Interamericana sobre Protección de datos personales"[29]. Además de participar como observadores el Supervisor Europeo de Protección de Datos Personales en representación de la Unión Europea, entre otros organismos internacionales.

A esto se suma la *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas*, adoptadas en 2012 por el Comité Jurídico Interamericano de la Organización de Estados Americanos (OEA)[30]. Sin embargo esta propuesta no se establecen líneas altas de protección, quedando por debajo de los estándares de la Directiva de al Unión Europea y otros países que se encuentran alineados con los estándares europeos previstos inicialmente por la anterior Directiva 95/46/CE.

Red Iberoamericana de Protección de datos (RIDP)

Esta red surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) entre representantes de 14 países iberoamericanos, celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003.

Es un grupo de trabajo integrado por los países de América latina y España, del sector público y privado. En nuestro país está conformado por el Ministerio Público, Poder Judicial, Asociación Paraguaya de Derecho Informático y el Ministerio de Industria y Comercio.[31]

Este junio 2017 se lanzó oficialmente un documento de "Estándares de protección de datos personales para los Estados Iberoamericanos"(Red Iberoamericana de protección de datos, s. f.). El mismo busca articularse con los foros internacionales con la altura e inminencia del tema.

Organización para la Cooperación y el Desarrollo Económicos

Paraguay forma parte de la OCDE oficialmente desde el 2017[32]. Esta organización cuenta con recomendaciones que constituyen documentos para orientar a sus Estados miembros. En esta línea, existe una agenda de protección de datos con el fin de establecer regulaciones básicas de protección de datos que garantice el libre flujo de la información así como evitar regulaciones que creen barreras proteccionistas en el comercio internacional. La OCDE emitió las guías sobre Circulación Internacional de Datos Personales para la Protección de la Intimidad y la Seguridad de los Sistemas de Información[33].

28 Observadores acreditados al RIPD http://www.redipd.es/la_red/Miembros/index-ides-idphp.php
29 Documentación que han formado y formarán parte del proceso de preparación, discusión y aprobación de la Ley Modelo Interamericana sobre Protección de Datos Personales de la OEA disonible en http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp
30 http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf
31 Miembros de la Red Iberoamericana – Paraguay: http://www.redipd.es/paises/paraguay-ides-idphp.php
32 Paraguay ya forma parte de países miembros de la OCDE http://www.lanacion.com.py/2017/01/26/paraguay-ya-forma-parte-los-paises-miembros-la-ocde
33 "Directrices sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales" de la Organización para la Cooperación y el Desarrollo Económico - («2013 OECD Privacy Guidelines - OECD», s. f.)

Organización de las Naciones Unidas

Existe directrices de la ONU para la regulación de los archivos de datos personales informatizados a través de su resolución 45/95 de la Asamblea General del 14 de diciembre de 1990 *"Directrices concernientes a Archivos Computarizados de Datos Personales adoptada por resolución por la Asamblea General de la Organización de las Naciones Unidas" (ONU, 1995)*. La misma contempla cuestiones básicas de protección que se deberán seguir como guía para las normas internas. Y se actualiza y complemente con la Resolución sobre *Privacidad en la Era Digital* adoptada por la Asamblea General de la ONU en 2016 (ONU, 2016).

Análisis de Entrevistas

Los datos personales en bases de datos de instituciones públicas

Para tener una aproximación a cómo se gestionan las bases de datos en la práctica, se realizaron entrevistas a funcionarios públicos que tienen responsabilidad directa sobre la administración de dichas bases y expertos calificados. En estas entrevistas se buscó indagar si las instituciones tienen o no incorporados principios y prácticas de protección de datos personales que se contienen en sus bases. En este capítulo se resumen los hallazgos principales, que se organizan bajo categorías asociadas a los estándares de protección resumidos en el trabajo de David Banisar (Banisar, 2011) y lo estipulado en el nuevo Reglamento de la Unión Europea (Parlamento Europeo, Consejo de la Unión Europea, 2016).

A continuación se describen la naturaleza de las bases de datos –qué bases de datos tienen bajo su responsabilidad las instituciones, qué datos de carácter personal contienen–, cómo se aplican o no principios de protección –recolección, notificación, finalidad, limitación del uso, etc.– y se añaden comentarios sobre otros hallazgos que surgieron en el curso de las entrevistas.

Naturaleza de las bases de datos

Todas las instituciones entrevistadas poseen bases de datos que contienen datos de carácter personal. Estos datos están relacionados a la implementación de políticas educativas, habitacionales, aduaneras, comerciales, fiscales y de ayuda social. La mayoría de ellas se encuentran digitalizadas, aunque aparecieron casos que aún contienen datos personales en formato físico.

Entre instituciones, las bases de datos coinciden en algunos datos personales, como nombre y apellido, fecha de nacimiento, lugar de nacimiento, cédula de identidad, dirección de domicilio, correo electrónico. Difieren de acuerdo a las actividades que desempeñan. Por ejemplo, para la implementación de políticas habitacionales, las bases de datos contienen información sobre los ingresos de las personas, su estado laboral y datos filiatorios. Es decir, poseen información sobre si las personas tienen hijos, si están a cargo de adultos mayores, etc.

A través de las entrevistas, se identifican datos de carácter personal en las siguientes instituciones públicas:

Base de datos	Datos personales	Propósito de creación	Normativa de creación	Institución pública
Registro Único del Contribuyente (RUC)	Nombre y apellido, correo electrónico, domicilio, actividades económicas, empleo, RUC (Registro Único del Contribuyente), declaraciones juradas, pagos realizados	Gestión tributaria[34]	Ley 125/91[35] que establece el nuevo régimen tributario y sus modificaciones	Subsecretaria de Estado de Tributación del Ministerio de Hacienda

Base de datos	Datos personales	Propósito de creación	Normativa de creación	Institución pública
Registro Único del Estudiante (RUE)	Nombre y apellido, fecha y lugar de nacimiento, cédula de identidad, datos de padre madre o tutor, historial académico de estudiantes de educación media, institución educativa	Historial de estudiantes del sistema educativo paraguayo[36]	Resolución N° 8655[37] por la cual se autoriza la implementación del registro único del estudiante, en las instituciones educativas de todos los niveles y modalidades de gestión oficial, privada y privada subvencionada de este ministerio.	Ministerio de Educación y Cultura
Datos registrados para aplicación del plan habitacional de la institución	Nombre, apellido, lugar de vivienda, actividades económicas, empleo o estado laboral, capacidad económica (ingresos), cantidad de hijos/as, estado de salud de hijos/as, adultos mayores a cargo	Aplicación del plan habitacional de la institución; evaluación de beneficiarios[38]	Ley 3909[39] que crea la Secretaría Nacional de la Vivienda y el Hábitat "Senavitat"	Secretaria Nacional de la Vivienda y el Hábitat
Datos registrados para actividades del comercio exterior de la institución	Nombre y apellido, cédula de identidad, RUC, dirección, teléfono, correo electrónico	Los datos son utilizados para la gestión de las áreas operativas y administrativas de la entidad como por ejemplo, declaración sumaria, declaración detallada, percepción de tributos, garantías bancarias y seguros por operaciones aduaneras, entre otras[40]	Ley No 2422[41] Código Aduanero	Dirección Nacional de Aduanas

34 Entrevista con un funcionario de la Subsecretaria de Estado de Tributación
35 Disponible en http://www.impuestospy.com/Leyes/Ley%20125_91_art1_25.php
36 Entrevista con funcionario del MEC
37 https://mec.gov.py/cms_v4/documentos/ver_documento/?titulo=8655-2016-LAFUENTE
38 Entrevista con funcionario de Senavitat
39 https://www.senavitat.gov.py/blog/leyes/ley-no-3-909

Base de datos	Datos personales	Propósito de creación	Normativa de creación	Institución pública
Datos registrados para los programas sociales que brinda la institución	Nombre, apellido, cédula de identidad, dirección, salario, cantidad de habitantes del hogar	Evaluar el "nivel de pobreza" de la familia para otorgar o no los beneficios sociales	Ley 1602/01[42] y manual operativo de la institución.	Secretaría de Acción Social
Datos clínicos de los pacientes	Nombre, apellido, dirección, estado de salud, histórico de consultas (muy fragmentada), internaciones	Llevar el registro de salud de la población	Ley 1602/01	Ministerio de Salud Pública y Bienestar Social
Programa social de la institución	Nombre, apellido, dirección, salario, cantidad de habitantes del hogar	Evaluar el "nivel de pobreza" de la familia para otorgar o no los beneficios sociales	Un decreto y un protocolo que autoriza al programa social a hacer la recolección	Secretaría Técnica de Planificación
Datos académicos de estudiantes Datos laborales de los docentes Datos para la gestión de dominios de Internet	Nombre, apellido, cédula de identidad, matriculaciones, calificaciones, salario, correo electrónico	Gestionar el sistema académico, el sistema de pagos y el sistema de nombres de dominio de la Universidad Nacional de Asunción	Creación del CNC	Centro Nacional de Computación
Datos de exportaciones Datos de empresas	Nombre, apellido, domicilio, importador, ingresos	Operar sobre las importaciones y exportaciones Generar un registro de empresas	Ley 1602/01	Ministerio de Industria y Comercio

Ejemplos de bases de datos

Existen algunas bases de datos emblemáticas, como el Registro Único del Estudiante (RUE) y el Registro Único del Contribuyente (RUC). La primera base de datos es un sistema de información que identifica a todos los estudiantes del sistema educativo paraguayo a cargo de Ministerio de Educación y Ciencias. Fue desarrollada con el apoyo de dos organizaciones internacionales, - la Organización de Estados Iberoamericanos (OEI) y el Programa de Democracia y Gobernabilidad de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) a través del Centro de Estudios Ambientales y Sociales (CEAMSO). En el discurso de lanzamiento de la herramienta, el ministro de Educación Enrique Riera se refirió a la herramienta como una "base de datos gigantesca

40 Respuestas enviadas por correo electrónico por funcionario de Aduanas
41 Disponible en http://www.aduana.gov.py/uploads/archivos/codigo%20aduanero.pdf
42 Disponible en http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=1760

en una plataforma única". La vice-ministra de Educación María del Carmen Giménez agregó que el sistema genera una "cédula estudiantil, una identidad estudiantil que permitirá a docentes, familias y al Estado paraguayo gestionar todas las iniciativas y los recursos con mayor precisión"[43] (OEI, 2016).

Específicamente, el RUE contiene datos de cada estudiante y también de sus tutores (padre, madre, encargado legal). Incorpora además datos de estudiantes extranjeros que asisten a un centro educativo en Paraguay. Así, aparecía en una de las entrevistas[44]:

> *"El RUE (Registro Único del Estudiante) es (la base de datos) más sensible porque recoge información de menores de edad. Datos básicos como nombre, apellido, fecha de nacimiento, cédula, lugar de nacimiento -- todos datos de identificación propiamente. Adicionalmente, mantenemos información de alumnos extranjeros, o sea que hay alumnos que no tienen cédula paraguaya y sin embargo igual son educados aquí. Estructuralmente son las mismas informaciones. También tenemos datos de contacto, datos de padre, madre, tutor, información de contacto de éstos, lugar de nacimiento; tenemos a qué institución le corresponde, o sea dónde está matriculado y toda la información asociada [...] En lo que es gestión académica de Nautilus desde el 2012 nosotros ya tenemos el historial académico, pero solamente de los alumnos de educación media".*

Por su parte, el RUC, según el Ministerio de Hacienda, el ente a cargo de la aplicación de la política fiscal del país, es *"el número de identificación –personal e intransferible– de todas aquellas personas nacionales o extranjeras, y de todas las personas jurídicas (empresas, prestadoras de servicios, industrias, etc.) que realicen actividades económicas"* (Hacienda, 2017). Explicita que también deben tener RUC las entidades sin fines de lucro[45]. En una entrevista, se afirmaba lo siguiente[46]:

> *"Están todos los datos principales del contribuyente: actividades económicas que realiza, empleo, domicilio, correo electrónico [...] Desde su inscripción, toda la trazabilidad de los procesos que rigen al Sistema Tributario Nacional están dentro de esa aplicación. Tipo de contribuyente, las presentaciones, declaraciones juradas, los pagos que realiza, tiene una cuenta corriente del contribuyente [...]".*

El manejo de estas bases de datos y las que se administran en las demás instituciones exploradas en esta investigación son analizadas bajo los principios de protección que se enumeran a continuación.

Principio de recolección

Sobre este principio, se indaga en la existencia de marcos legales que regulen la recolección de los datos, asi como la debida notificación de las personas cuando sus datos son recolectados. Todos los entrevistados refieren a normativas que guían o regulan la recolección de datos en sus instituciones. Estas normativas son variadas, y en general ninguna refiere exclusivamente a la administración de los datos recolectados. Algunos entrevistados nombran a los decretos de creación de las mismas instituciones, como el caso de Senavitat y Aduanas. Otros entrevistados citan resoluciones ministeriales que establecen la creación de bases de datos específicas, como el Registro Único del Estudiante en el Ministerio de Educación y Cultura, y que indican procedimientos u organigramas

43 Disponible en http://www.oei.org.py/index.php/presentacion-del-registro-unico-del-estudiante-rue/
44 Entrevista con funcionario del MEC
45 Disponible en https://www.hacienda.gov.py/web-hacienda/index.php?c=77
46 Entrevista con funcionario de la Subsecretaria de Estado de Tributación

que delinean el manejo de dichas bases. También hacen referencia a dos leyes aprobadas en los últimos años como marco jurídicos que afectan su trabajo: la Ley 5282/2014 de libre acceso ciudadano a la información pública (Congreso Nacional, 2014) y la Ley 5189/2014 que establece la obligatoriedad de la provisión de información el uso de los recursos públicos sobre remuneraciones y otras retribuciones asignadas al servidor público.

> *"[En el Ministerio de Educación], las resoluciones ministeriales donde por ejemplo se implementa el Registro Único [del Estudiante] , y después lo que tenga que ver con recursos humanos"*
>
> *"[En la Secretaría Técnica de Planificación] yo tengo normativas internas que han sido aprobadas por el equipo de asesoría jurídica, que asumo que consideró las [normativas] nacionales e internacionales. También tuvimos una brevísima charla (con una experta en derechos digitales), que nos dio algunos tips sobre cosas que no podemos hacer como gobierno. También fue considerado en el momento de hacer el manual de continuidad operativa, que incluye la manera de proteger los datos personales"*

Encontramos un nivel insuficiente de conocimiento por parte de los técnicos y encargados de administrar o custodiar las bases de datos sobre normativas de protección. Para argumentar este desconocimiento, el entrevistado del CNC apela a su rol de técnico-informático:

> *" Lo que pasa que acá solo somos técnicos. […] Más que eso, tampoco, no tenemos…. No hay ninguna reglamentación".*

En otros casos, aceptan la situación actual de falta de claridad en cuanto a las normativas, sin reparos, como surge en la entrevista con el funcionario de la SAS:

> *"A nosotros nos rige un poco esa «norma institucional», que no está escrita, para qué te voy a mentir. Es un poco la visión de la máxima autoridad en decir: «esto se puede dar, esto no se puede dar», y siempre también un poco la cara del cliente".*

Por otra parte, como ya se citó anteriormente, algunos de los entrevistados explicaron que la recolección de datos está respaldada *"por la creación"* del organismo o por normas internas, siendo probable que en dichas normativas no haya especificación alguna sobre la gestión de datos personales[47]. Uno de ellos, declaraba lo siguiente:

> *"La Ley de creación de Senavitat es lo que rige el ámbito de acción de la institución. Pero no hay así puntos específicos en cuanto a los detalles de información, el resguardo y eso […] Claro, no está así explícito como que lo tiene la Abogacía del Tesoro, Tributaciones y eso".*

Un funcionario de Aduanas refuerza la idea de respaldo por reglamentos internos:

> *"El Código Aduanero en el artículo 8 donde autoriza la utilización de tecnologías de información y automatización […] en los artículos 17, 18, 19, 20, 31, 34, 36 y 40 donde define la actuación, derechos, obligaciones y régimen disciplinario de las personas vinculadas a la actividad [...]."*

47 La posibilidad de conocer la normativa interna de cada institución escapa los alcances de esta investigación

Como puede observarse, el entrevistado habla de actuación, derechos y obligaciones, pero no hace referencias a las cuestiones inherentes al tratamiento de datos personales.

Mientras tanto el entrevistado del MEC habla de una política interna de gestión de la información:

> *"Tenemos una política de gestión de información, tenemos implementados algunos procedimientos, hay resoluciones ministeriales que reglamentan la implementación de los sistemas y en consecuencia los roles de cada uno de los actores".*

De nuevo, algunas instituciones han avanzado más, creando sus normativas específicas sobre datos personales, mientras otras, se basan en normativas desactualizadas y otras en "normas no escritas". Uno de los entrevistados afirma conocer la ley vigente sobre "Información de carácter privado" (Congreso Nacional, 2001):

> *"[En el MSPBS] Yo creo que es la «información de carácter privado» y sensible habría. No conozco otra ley. Porque es privado y es sensible el tema de la salud. Cualquier tipo de información que individualice o permite individualizar..."*

En la entrevista con el funcionario del MIC también se menciona la ley de información de carácter privado:

> *"Hay una ley que rige para los datos personales. Están los que son confidenciales y los datos que son públicos. Para nosotros, por ejemplo, son datos confidenciales el importador, a quién le están vendiendo. Son datos que no podemos publicar porque la competencia puede utilizar para ganarle de mano. Ciertos datos como ingresos y demás, no podemos, porque son confidenciales. Pero después el resto de los datos, son todos datos de la balanza de pagos de país y que son datos públicos. Datos confidenciales no tenemos muchos".*

Se puede notar una tensión o una línea difusa que se plantea en el marco teórico de esta investigación sobre el acceso a la información pública y protección de datos personales. El entrevistado de la SAS lo planteaba así:

> *"No me recuerdo la ley, pero parte de esta ley, es la que a nosotros mismos como funcionarios públicos [usamos], hay una ley de transparencia que se hizo en el 2015".*

La transparencia y acceso a la información pública pueden colisionar con el tratamiento de datos personales y los puntos límites deben marcarse claramente. No habiendo una Ley Orgánica de Protección de Datos, estas líneas las establece cada institución actualmente.

Es cierto que esa es el área adecuada para tratar los temas legales, pero también se verifica un amplio desconocimiento, que puede entenderse porque las regulaciones están fragmentadas y la ausencia de una Ley Orgánica de Datos Personales, así cómo un organismo contralor independiente que otorgue mayores garantías de protección. Así, uno de los informantes calificados afirmaba que:

> *"Con los datos relacionados a la telefónica, la primera línea de defensa de todos nosotros debería ser la CONATEL. Pero fuera de eso, como no tenemos una ley orgánica de protección de datos que tendría que ser la que esté por encima de todo eso, entonces en realidad estamos huérfanos".*

Finalmente hay leyes nacionales que aplican a determinada institución, como surge de la entrevista con un funcionario de la SET:

> *"[De] la ley 125/91 básicamente se desprende en un montón de normas y en realidad siempre, cuando hablamos en ese sentido decimos: la Ley 125 y sus modificaciones. A partir de ahí se desprende un montón de normas propiamente. Y realmente a nosotros aplica toda la norma existente".*

De las entrevistas se infiere que la protección de datos personales en las instituciones a partir de las normas, leyes o reglamentos existentes es confusa. En la primera parte del Análisis de Hallazgos, se presenta un análisis jurídico que cubre la normativa nacional vigente, la internacional y la jurisprudencia vinculante. Este análisis echa luz sobre el estado de los marcos regulatorios de recolección y gestión de los Datos Personales y da cuenta de la existencia de importantes lagunas jurídicas. En palabras del entrevistado de CNC:

> *"Acá solemos tener grandes discusiones filosóficas sobre qué es publicable y qué no. Eso justamente ocurre porque no hay un marco legal bien establecido, que te diga hasta donde sí [publicar] y hasta donde no. Uno interpreta que el número de cédula es público, otro interpreta el nombre, ambos [...] Faltaría un poco más que los abogados estudien lo tecnológico, hay pocos abogados especialistas en esto".*

En cuanto a la **notificación**, la mayoría de los entrevistados afirman que se da a conocer a las personas cuando sus datos son recolectados y con qué propósitos. Sin embargo, no queda claro si las instituciones hacen esta notificación por principio de protección de los datos personales o por satisfacer una necesidad administrativa de identificación de beneficiarios.

Por ejemplo, para que las personas puedan acceder a los beneficios de programas sociales están obligados a proveer datos personales en documentos que tienen carácter de declaraciones juradas, como lo afirma un funcionario de la SAS:

> *"Se notifica previamente. Nosotros tenemos funcionarios en campo. En campo hay cerca de mil personas, que acompañan de cerca a las familias y ellos saben cuándo se van a ir a intervenir determinado distrito, a través de la intendencia. El formulario, actualmente se firma un documento paralelo, ya como te dije se hace con las tabletas, pero hay lugares donde todavía se hace en forma de papel; el jefe de familia que firma al pie, como una declaración jurada. Esto es lo que se hizo, lo leyó y si están seguros de todos los datos que están ahí, ellos autorizan que nosotros tomemos esos datos y los registremos"*

En la STP reafirman que para acceder a los programas sociales, las personas deben entregar sus datos personales y son consultadas previamente para que se concrete dicha entrega:

> *"Se le pregunta "¿Querés ser parte de esta encuesta y entregar tus datos para ser potencial beneficiario de los siguientes programas sociales?"*

Principio de especificación de finalidad

Sobre este principio, se busca identificar las razones por las que las instituciones recolectan información. Algunos entrevistados relacionan la recolección de los datos a la necesidad de cumplir con los objetivos y actividades de las instituciones donde se desempeñan. Sin embargo, no existen normas o reglamentos específicos que delineen el propósito de la recolección de datos personales, como lo grafican las siguientes entrevistas:

> *"[En Aduanas] los datos son utilizados para la gestión de las diferentes áreas operativas y administrativas de la esa entidad como por ej. declaración sumaria, declaración detallada, percepción de tributos, garantías bancarias y seguros por operaciones aduaneras, entre otras"*

> *"[En la SAS se recolecta] específicamente para dos cosas: uno es el seguimiento de las familias y dos es el pago en sí. Concretamente ellos reciben un pago, una cuota, que consta de 72 cuotas. Y para que yo sepa cuánto debo pagar a esa gente, debo analizarlo en forma electrónica. En total son miles"*

Principio de limitación del uso

Sobre este principio se busca conocer si los datos recolectados se utilizan con otros fines más allá del objetivo primario de recolección. Algunos entrevistados indican que los datos que contienen las bases no se utilizan para propósitos distintos a los que fueron recolectados. Pero al no existir marcos regulatorios específicos sobre los propósitos de recolección de los datos, se generan dudas en torno al cumplimiento íntegro de este principio. Solo un entrevistado especifica que los datos recolectados se ciñen solamente al uso estipulado en la normativa de creación de la institución. Otros, sin embargo, indican que los datos se utilizan con fines estadísticos o se comparten a otras instituciones.

> *"[En STP] no se ha usado esa información en ningún caso para algo distinto a ayudarles. Se ha compartido con los encargados de planificar los programas sociales, por ejemplo, que son explícitamente el fin por el cual fueron recolectados" (sobre uso de datos personales recolectados para programas sociales)*

> *"Los datos registrados de las personas vinculadas a la actividad aduanera son utilizados para los fines previstos en el Código Aduanero. No se difunden ni comparten mas allá de los fines originales de su recolección"*

> *"[En la SAS] los programas son los que tienen mayor cantidad de datos, y cada uno por sus particularidades tienen su propia base de datos. Al mismo tiempo (…) aprovechamos para sacar análisis de estadística, entre otras cosas"*

Principio de calidad de los datos

El principio de **calidad** de los datos especifica que los mismos deben ser utilizados con el mismo objeto con el que fueron recolectados, así como también ser exactos y actualizados. Además, deben suprimirse los datos que sean inexactos con respecto a los fines del tratamiento.

Varios de los entrevistados coinciden en que sus instituciones tienen mecanismos de actualización de los datos, tanto en el caso que sean erróneos, como a lo largo del tiempo, a medida que los datos deban ajustarse a la realidad de los titulares de los datos. En entrevista con STP surge el hecho de que los propios titulares de datos tiene la posibilidad de actualizar su información:

> *"El contribuyente en sí tiene la posibilidad de actualizar. De hecho que no hace mucho hicimos unas modificaciones [...] para que tenga que actualizar sus datos como una obligación [...]. Lo que habilitamos ahí es que esa posibilidad sea a través de Internet: la mayoría de las actualizaciones, se están pudiendo realizar ya a través de Internet".*

También hay testimonios como el siguiente que surge en la entrevista con el MEC, donde los padres actualizan los datos de sus hijos:

> *"El padre mismo lo puede hacer, dentro del registro [...] el padre puede acceder a los datos de su hijo, esa es su población. Si puede acceder a los datos de su hijo puede modificarlos, evidentemente".*

Mientras que en otros casos son las mismas instituciones las que sistemáticamente los actualizan mediante procedimientos y protocolos:

> *"[En el MSPBS] entiendo que existe todo un protocolo aprobado para eso. No cualquiera puede decidir si un dato es erróneo o no, y hay trazabilidad en todos los cambios que se realizan".*

Hay un caso donde la institución que procesa los datos no es la misma que los recolecta. En esta situación se realiza un control de calidad:

> *"Todos los levantamientos del CENSO no los hicimos nosotros: una gran parte se hizo con la DG [DGEEC] (...) Entonces la calidad no era tan buena en algunos casos. Entonces la actualización también incluye la corrección de nombres, de documentos,etc."*

Podemos decir que la mayoría de las instituciones que estamos investigando cumplen el principio de calidad de los datos en lo referente a objeto y actualización.

Principio de conservación

En cuanto al principio de **conservación**, se refiere al plazo por el que los datos personales son almacenados. Vemos que la amplia mayoría de las instituciones no tienen establecidos límites de tiempo para la conservación de los datos. Carecen de protocolos, mecanismos, o normativas para la destrucción de los datos de carácter personal.

En la mayoría de los casos, esto se justifica por necesidades administrativas o de auditorías. El entrevistado de la SAS afirma lo siguiente:

> *"Entonces por eso no la borramos; para nosotros también es un dato histórico, (...) si tuviéramos un control, de contraloría, o alguna auditoria informática, relacionados con estas familias, por cada pago que se le hizo, por más que no esté activo".*

Otro ejemplo en el que se explica la razón por la que no se borran los datos, surge en la entrevista con el MEC:

> *"[…] Aquel chico que está entrando en el pre-jardín, se ingresa una sola vez la información, y cuando se reciba de ingeniero va a tener la misma información. Hoy hablamos básicamente de 20, 25 años. Entonces, no tenemos previsto eliminar datos. De hecho, por lo contrario, tenemos mecanismos de respaldo, apuntamos a la alta disponibilidad, más que a eliminar".*

Hubo un caso donde el entrevistado declaró que sí están establecidos los procedimientos y las reglas para la destrucción, pero no se cumplen:

> *"Hay un periodo de almacenamiento y un periodo de destrucción, se tiene que hacer bajo unos procedimientos jurídicos.: pero nunca se hace. Se almacenan, se guardan en depósito «for ever», hasta que se incendien o algo así. Es jodido destruir una historia, no se suele hacer el procedimiento de destrucción".*

Como puede observarse, siendo la administración pública, la mayoría de las bases y los datos recopilados tienen que ver con el otorgamiento de beneficios sociales, procedimientos administrativos o relaciones entre estado y ciudadanos. Entonces, por motivos de contralor, de no haber doble beneficio o justificaciones similares, se justifica dicha recolección.

Más allá de estas justificaciones, deben establecerse los períodos para cada caso. Es claro que la base de datos de cédulas de identidad no deben ser borrados, mientras que los antecedentes penales deben borrarse 3 años después de haber cumplido la pena correspondiente. Lo que se desprende de las entrevistas es que las instituciones estatales no están reparando en este principio de conservación.

Principios de seguridad

Sobre el tema del **acceso y transferencia** de las bases de datos, la mayoría de los entrevistados plantean que las instituciones manejan criterios estrictos sobre acceso y transferencias. Todos ellos tienen estrictas políticas de acceso a los datos, con roles establecidos y registro de los accesos. Por ejemplo, en entrevista con CNC se afirmaba lo siguiente:

> *"Puede tener acceso base de datos que son de administración o salarios. Pero los niveles están bien definidos y hay auditoría para cada uno de esos accesos; y los usuarios son individualizados".*

En otro caso, en la entrevista con la SAS se plantea lo siguiente:

> *"Cada programa tiene un administrador de base de datos, y por supuesto la dirección de TIC en este caso […] En la dirección hay otro administrador que soy yo, y hay un departamento desde TIC, que es la de desarrollo, donde también otra persona tiene acceso. Son tres así y nada más".*

En la entrevista con Senavitat, se plantea que aún está en proceso de definición el tema:

> *"Están definidos los roles: tenemos administrador de la base de datos, tenemos gente de desarrollo, la gente operativa. Está todo manejado por perfiles, que definen los niveles de acceso a la información o a los datos. Y eso también estamos trabajando en definir quiénes van a ser los que autorizan o desautorizan el acceso".*

En alguno de los casos se hace explícito un acuerdo de confidencialidad con los funcionarios, para tener un soporte legal en la protección de los datos personales, como aparece en la entrevista con el MEC:

> *"Le hacemos firmar acuerdo de confidencialidad inclusive a todo el equipo técnico. Nadie puede acceder a los servidores de producción. Solamente acceden a datos de prueba, más o menos tratamos de controlar los ambientes y los niveles de acceso de acuerdo a la función que cumple cada uno".*

En el tema de acceso hay indicios de un consenso y la adopción de ciertas "buenas prácticas" que tienen que ver con compartimentación, niveles de acceso y registro de acceso, para de esa forma asegurar que no existan accesos indebidos a los datos, o en caso de ocurrir, poder hacer un análisis correspondiente para la identificación de la falla.

Llama la atención que solamente uno de los entrevistados hizo referencia al *Modelo Estándar de Control Interno para las Entidades Públicas del Paraguay (MECIP)* que es una herramienta de control permanente para la gestión en las instituciones públicas. Como mencionamos, solamente el entrevistado de la STP lo citó como normativa y fuente de buenas prácticas:

> *"Tenemos un mapa de riesgos de hecho que el MECIP nos exige [...] A cada acción que realices tenés que hacer un mapa de riesgos. Entonces, por ejemplo, si tenes una acción que es "conceder acceso a una base de datos", a eso le tenés que poner tu mapa de riesgos.*

Por otro lado, con respecto a **transferencias**, encontramos que prácticamente no se realizan **transferencias internacionales** de datos, y en algún caso aparece la posibilidad de transferencia pero de una forma muy agregada y anonimizada.

En cuanto a la **transferencia nacional** e interinstitucional, aparecen varias formas de intercambiar datos e información entre las instituciones públicas: existen formas más precarias e inseguras como el envío mediante dispositivos extraíbles como discos compactos, pero también aparecen formas sistemáticas e interconectadas para realizar los intercambios.

Un ejemplo es el Sistema Integrado de Información de SENATICS (SII), en el que las instituciones públicas ponen a disposición de sus pares varios conjuntos de datos relevantes que permite acelerar ciertos procesos y pretende reducir los errores. Así lo explica el entrevistado del MEC:

> *"No sé si ya te comentaron del sistema de intercambio de información entre instituciones públicas que es gerenciado por SENATICs. Es una vía de comunicación entre entidades públicas, en donde las entidades públicas pueden disponibilizar datos para que sean utilizados entre todos. Un ejemplo: Identificaciones disponibiliza su base de datos y nosotros consumimos información a través de un servicio, en ese caso nosotros estamos siendo consumidores. También existe la posibilidad de ser proveedores de información y nosotros ahora estamos proveyendo el grado académico, por ejemplo".*

En la entrevista con Senavitat, aparece uno de los beneficios de esta forma de compartir:

> *"[...] Hoy se esta tratando de minimizar esos errores, ahí si accediendo a información de otras instituciones, a través del Sistema Integrado de Información de SENATICS".*

Pero también aparecen ciertos límites en la entrevista con la SAS,

> *"Pero cuando yo quiero saber de alguien, me pide el número de cédula y la fecha de nacimiento: a mí no me sirve eso, a mí me sirve la base completa para poder cruzar. Los cruces que se hacen son son permanentes, son grandes [...]".*

Por otra parte está el Sistema Integrado de Información Social (SIIS), que gestiona la STP y que aglutina la información sobre beneficiarios de los diferentes programas sociales del gobierno:

> *"Son instituciones del programa «sembrando oportunidades» que tienen acceso al «tablero de control presidencial», es decir a las instituciones que trabajan en el área social. El acceso está controlado por un sistema, [...] sistematizado y controlado y tiene auditoria informática también".*

En la entrevista con SAS, sobre el mismo sistema, se afirma que:

> *"Ellos, viste que hay distintas instituciones que tienen programas sociales. Ellos lo que buscan es que no estén accediendo a más de un programa social, de la misma persona o del mismo grupo familiar".*

Además, se especifica que:

> *"Ese sistema que ellos tienen que es un sistema de información integrada social, la visión del gobierno ya al anterior a este, era que yo pongo «Luis» y tu número de cédula, yo sepa en dónde estás: en que entidad estás beneficiado vos".*

Por su parte, el Ministerio de Hacienda maneja un sistema de intercambio de información tributaria, llamado SIARE,

> *"De hecho que el tema de sueldo todos los meses se carga [...] luego eso al cargarse todo se transfiere al sistema integrado SIARE, para que Hacienda pueda pagar"*[48].

Como se puede ver, hay una variedad de formas de intercambio pero aparece una interesante tendencia a hacerlo de forma sistemática y centralizada, de modo de no duplicar información y de forma que las bases no estén proliferando en las diferentes instituciones. Esto también tiene sus límites y sus riesgos, como el entrevistado que plantea la necesidad de hacer cruces de bases de datos.

Esta complejidad tiene resguardos informáticos, pero hace falta un soporte legal integral que permita a los funcionarios una mayor garantía y respaldo sobre sus acciones, así como que establezca las sanciones en caso de incumplimiento de los procedimientos y protocolos.

Relacionado con los principios de calidad y seguridad, está el tema de la **infraestructura** que permite el mantenimiento y protección de estas bases de datos. Existen claramente dos tipos de instituciones, algunas que cuentan con un departamento de informática con 20 o más personas, mientras otras que tienen un número muy inferior en torno a las 10 personas.

El cambio de paradigma del papel al dato digital, de las carpetas físicas a las bases de datos relacionales, se ha venido desarrollando de diferentes formas en diferentes áreas del Estado. Lo que aparece en las entrevistas es que algunas instituciones trabajan con un número inadecuado de expertos informáticos y esto puede aumentar los factores de riesgo en algunos casos.

48 Quisimos explorar este sistema, pero el sitio Web se encontraba fuera de servicio al momento de esta investigación

Conclusiones y recomendaciones

Los hallazgos de las entrevistas a funcionarios públicos y expertos de instituciones del Estado arrojan un panorama mixto en cuanto a la existencia de estándares y prácticas adecuadas de protección de datos personales contenidos en bases de datos públicas. Si bien hay indicios de la aplicación de algunas buenas prácticas, la ausencia de una normativa robusta que aplique a todas las instituciones es el principal problema que se encuentra y que expone a la ciudadanía cuyos datos se encuentran almacenados a riesgos.

Los responsables a cargo de las bases de datos tienen un nivel bajo de familiaridad con estándares de protección, ya sean regulaciones internas, nacionales o internacionales. Algunos se rigen por decretos de creación de las instituciones y otros por “normas no escritas”. También se evidencia una leve tensión con el alcance de la Ley 5282/14 de acceso a información pública. Al no haber una Ley de protección de datos personales actualizada e integral, cada institución establece o resuelve por si sola las tensiones que se generan con la Ley 5282/14 a la hora de otorgar información. Se puede inferir que las excepciones establecidas en el reglamento de la Ley de acceso a información pública son desconocidas o no son tomadas en cuenta a la hora de dirimir controversias.

Otro principio que no se cumple de acuerdo a los hallazgos de las entrevistas es el de establecer un límite al almacenamiento de los datos personales. Casi todas las instituciones carecen de protocolos, mecanismos o normativas para la destrucción de dichos datos. Manifiestan diversas razones para no hacerlo. Sin embargo, se deben establecer criterios dependiendo de la naturaleza de las bases de datos.

Existen dudas sobre la aplicación de principios de notificación, especificación de finalidad y limitación en el uso. La mayoría de los entrevistados afirman que se da a conocer a las personas cuando sus datos son recolectados y con qué propósitos. Lo que no queda claro es si las instituciones notifican por principio de protección de datos personales o por satisfacer una necesidad administrativa de recolectar los datos de potenciales beneficiarios de programas sociales, por ejemplo.

Sobre la especificación de finalidad, si bien algunos entrevistados explican que los datos son recolectados para cumplir con los objetivos y actividades de las instituciones, las afirmaciones son vagas cuando no existen normas o reglamentos específicos que regulen la recolección de datos personales.

En cuanto a la limitación en el uso de los datos, aunque los funcionarios manifiestan que sus instituciones utilizan los datos estrictamente para el objeto que son recolectados, de nuevo la ausencia de reglamentos específicos generan dudas sobre el espíritu y la efectividad de la aplicación de este principio.

Se desprende de las entrevistas que las instituciones tienen mecanismos de actualización de los datos, lo que está directamente vinculado a la calidad de los datos. La mayoría de los funcionarios fueron específicos en explicar como funcionan dichos mecanismos en caso de que los datos sean erróneos o necesiten modificaciones por el transcurrir del tiempo. Se puede inferir que las instituciones entrevistadas cumplen con este principio.

En cuanto al acceso y transferencia de los datos, también se puede identificar la aplicación de buenas prácticas. La mayoría de los entrevistados admiten contar con estrictas políticas de acceso a datos, con roles establecidos y en algunos casos, con registro de los accesos.

Sobre las transferencias, se identifican varias formas de intercambio de datos entre instituciones públicas sin un marco regulatorio donde se establezan protocolos y procedimientos para resguardar estos intercambios. Los mecanismos de intercambio son variados, aunque hay una tendencia de hacerlo de forma sistemática y centralizada para evitar la duplicación de información y para no proliferar bases de datos en distintas instituciones.

Sobre la creación de una Ley para la protección de datos personales

El derecho a la protección de datos personales deriva del derecho a la privacidad. Una legislación sobre este tema debe regular el modo en que los datos públicos y privados de los individuos son recolectados, procesados, almacenados y retirados electrónicamente o analógicamente de fuentes públicas y privadas.

Los datos personales deben ser tratados para las finalidades determinadas o específicas con base en el consentimiento y la autodeterminación informativa de cada titular del dato y con alguna base legítima y legal que transcienda tal necesidad. Además, se deben incluir los derechos ARCO para el cumplimiento de los estándares de protección.

Paraguay tiene varias normativas que abarcan de forma dispersa el tratamiento de datos personales: recolección, uso y autoridad de aplicación para cada caso. Sin embargo, se vuelve necesaria y urgente una Ley con un enfoque integral para evitar los posibles abusos que se realizan con los datos personales tanto en el sector público como el privado. Esta Ley debe limitar el tratamiento de los datos personales en lo que respecta a la recolección, tiempo de almacenamiento, proporcionalidad, calidad del dato, ámbito de aplicación, transparencia, rendición de cuentas y otros principios establecidos por los estándares más altos de protección de datos personales con perspectiva de derechos humanos, utilizados por la Directiva 95/46 de la UE y sus reglamentaciones. También, la futura Ley de protección de datos personales deberá contemplar los avances tecnológicos: datos biométricos, algoritmos, big data, transferencias internacionales de datos, entre otros.

Será necesario crear un órgano independiente como ente rector y responsable del control del tratamiento de datos, para analizar la finalidad de los mismos y hacer las revisiones preventivas de posibles errores o abusos que se dan en los tratamientos de datos. Es necesario auditar a los responsables de tratamientos de datos y elevar los estándares de protección de los mismos, acorde la Directiva de la UE 95/46. Ante la ausencia de un órgano de control, la retención de datos de tráfico puede afectar negativamente a la vida privada de las personas y contrarestrar el esfuerzo que

el consumidor o usuario debe hacer para proteger su información de los posibles abusos o errores que se puedan cometer, así como otras normativas vigentes expuestas en el análisis jurídico de esta investigación, que se desconocen su forma de recolección de información y datos personales.

Asimismo, la Ley no debe crear obstáculos a los avances de la ley 5282/14 de acceso a la información pública. La misma debe contener dispositivos legales que aseguren el acceso a los datos personales cuando el interés público fuera mayor que la necesidad de sigilo, como la divulgación de salarios de los servidores públicos, por ejemplo.

Uno de los desafíos en la agenda común de las mesas de trabajo en instancias internacionales es el debate de la protección de los datos personales relacionados directamente a lo derechos fundamentales como la libertad de expresión y la privacidad. Paraguay forma parte de estas redes y organizaciones internacionales que buscan un balance entre estos derechos incluyendo excepciones y provisiones sobre consideraciones relativas al interés público y los nuevos escenarios como la economía digital. El reto está en forzar desde la ciudadanía al cumplimiento de los compromisos asumidos en estos espacios: OECD, ONU, MERCOSUR, Red de Protección de datos Personales, entre otros.

Bibliografía

2013 OECD Privacy Guidelines - OECD. (s. f.). Recuperado 15 de febrero de 2017, a partir de https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

ABC Color. (s. f.). Especial Caso Cecilia Cubas - ABC Color. Recuperado 15 de junio de 2017, a partir de http://www.abc.com.py/multimedia/caso-cecilia-cubas/

Asamblea Constituyente. (1992). Constitución Nacional de la República del Paraguay. Recuperado 20 de enero de 2017, a partir de http://www.bacn.gov.py/constitucion-nacional-de-la-republica-del-paraguay.php

Cerda Silva, A. (2011). Autodeterminación informativa y leyes sobre protección de datos. *Revista Chilena de Derecho Informático*, *0*(3). https://doi.org/10.5354/0717-9162.2003.10661

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

CIDH. (2009, julio 6). Caso Escher y otros vs. Brasil. Sentencia de 6 de Julio de 2009. Recuperado a partir de http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

Comisión Nacional de Telecomunicaciones (CONATEL). Resolución 1350_2002. Por el Cual se establece la obligatoriedad de registro de detalles de llamadas por el plazo de seis (6) meses. Recuperado a partir de http://www.buscoley.com/pdfs/r_1350_2002.pdf

Congreso Nacional. CODIGO DE ORGANIZACION JUDICIAL (1981). Recuperado a partir de http://www.pj.gov.py/descargas/ID1-60_id482_codigo_organizacion_judicial.pdf

Congreso Nacional. LEY N°125/91 ESTABLECE EL NUEVO REGIMEN TRIBUTARIO (1991). Recuperado a partir de http://www.oas.org/juridico/spanish/mesicic3_pry_ley125.pdf

Congreso Nacional. Ley N° 1682/01 Que Reglamenta la información de carácter privado, 1682/01 § (2001). Recuperado a partir de http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=1760

Congreso Nacional. Ley N° 1969/2002 QUE MODIFICA, AMPLÍA Y DEROGA VARIOS ARTICULOS DE LA LEY N° 1682/2001 «QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO», 1969/2002 § (2002). Recuperado a partir de http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=2539

Congreso Nacional. Ley N° 5282 de Libre Acceso Ciudadano a la Información Pública y Transparencia Gubernamental (2014). Recuperado a partir de http://informacionpublica.paraguay.gov.py/public/ley_5282.pdf

Fuenzalida Bascuñán, S. (2015). La jurisprudencia de la Corte Interamericana de Derechos Humanos como fuente de derecho: Una revisión de la doctrina del "examen de convencionalidad. *Revista de derecho (Valdivia)*, *28*(1), 171-192. https://doi.org/10.4067/S0718-09502015000100008

Jorge Rolón Luna, Maricarmen Sequera Buzarquis. (2016, marzo). Vigilancia Estatal de las comunicaciones y derechos fundamentales en Paraguay. Recuperado a partir de https://www.tedic.org/wp-content/uploads/sites/4/2016/05/Paraguay-ES.pdf

Ley N° 642/95 “De telecomunicaciones”. (s. f.). Recuperado 22 de marzo de 2017, a partir de https://www.conatel.gov.py/images/iprincipal/LEY%20642/Ley_N_642-95.pdf

MERCOSUR. (2008). XX REUNIÓN ORDINARIA DEL SUBGRUPO DE TRABAJO N° 13 “COMERCIO ELECTRÓNICO”. Recuperado a partir de http://www.mercosur.int/msweb/SM/Noticias/Actas%20Estructura/DEPENDIENTES%20DEL%20GMC/Subgrupos%20de%20Trabajo/SGT%2013/2008_ACTA01/Acta0108.doc

Montoya Melgar, A. (1995). *Enciclopedia jurídica básica*. Madrid: Cívitas.

OEA. Convencion de Viena (1961). Recuperado a partir de http://www.oas.org/legal/spanish/documentos/convencionviena.htm

OEA. Convención Americana sobre Derechos Humanos Suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos (B-32), B-32 § (1969).

ONU. (1948, diciembre 10). Declaración Universal de los Derechos Humanos. Recuperado a partir de http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

ONU. (1966, diciembre 16). Pacto Internacional de Derechos Civiles y Políticos. Recuperado 20 de enero de 2017, a partir de http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

ONU. A/RES/45/95. Guidelines for the regulation of computerized personal data files (1995). Recuperado a partir de http://www.un.org/documents/ga/res/45/a45r095.htm

ONU. Privacidad en la Era Digital (2016). Recuperado a partir de

http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

Pappalardo Zaldívar, C. (1992). *Reforma constitucional: proyectos y aportes*. Asunción: Vive : Intercontinental.

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

Rodríguez Palop, M. E., & Universidad Carlos III de Madrid. (2002). *La nueva generación de derechos humanos: origen y justificación*. Madrid: Universidad Carlos III de Madrid, Instituto Universitario de Derechos Humanos «Bartolomé de las Casas» : Dykinson.

Unión Europea. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 95/46/CE § (1995). Recuperado a partir de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A31995L0046

Anexos

A.1. Guión de entrevista

La siguiente definición de Base de Datos fue leída al principio de cada entrevista, debido a la ambigüedad planteada por la legislación vigente y sirvió para tener un marco conceptual común con la persona entrevistada:

> "[...] un conjunto organizado de datos que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso, cuyo titular sea una persona jurídica de naturaleza pública".

A continuación se presentan las preguntas-guía que se utilizaron en las entrevistas.

Naturaleza de las bases de datos

- ¿Qué bases de datos públicas maneja? ¿Cuál/es está bajo su responsabilidad específicamente?
- ¿Qué tipos de datos contienen esas bases de datos?
- ¿Cuáles son los datos de carácter personal que contienen esas bases?

Aplicación de principios de protección

- ¿Qué instrumento legal, normativa le autoriza la recolección de esos datos? (principio de recolección)
- ¿Se notifica a las personas para la recolección de sus datos? (principio de recolección)
- ¿Por qué razones se almacenan esos datos? (principio de recolección; principio de especificación de finalidad)
- ¿Se utilizan esos datos para otros propósitos que no sean los fines originales (fines de archivo, estudios científicos, etc? ¿Se difunden, comparten o publican más allá de los fines originales de la recolección (principio de limitación en el uso)
- ¿Se actualizan esos datos? ¿Cómo? (principio de calidad)
- ¿Se modifican esos datos en caso de ser erróneos? ¿Cómo? (se rectifican, suprimen)? (principio de calidad; principio de participación individual; exactitud)
- ¿Se eliminan esos datos en algún momento? ¿Luego de cierto tiempo? ¿Con qué razones?; en caso que no se eliminen, ¿por qué? (limitación del plazo de conservación)

Normativas, protocolos de uso y manejo de las bases de datos (principio de seguridad)

- ¿Qué normativas se aplican para la protección de datos personales? ¿Normativas internas de la institución? ¿Normativas nacionales que se tenga en cuenta?

- ¿Qué riesgos a la seguridad de las bases de datos identifica? (jurídicos, tecnológicos, humanos)
- ¿Recuerda algún incidente donde se vio comprometida la seguridad de los datos? ¿Cómo respondieron ante la situación?
- ¿Cuál es el protocolo que tienen ante un evento donde se comprometa la seguridad de las bases de datos?
- ¿Cual es el estándar que se utiliza para la seguridad de la información? Utiliza el estándar ISO 27001?
- En caso que la respuesta sea negativa, ¿cuál es el procedimiento de seguridad de la información?

Autorización de acceso y transferencia a las bases

- ¿Quiénes están autorizados a acceder a esas bases de datos? ¿Existe un seguimiento o registro del acceso las bases de datos?
- ¿Por qué motivos se accede a esas bases de datos?
- ¿Se transfieren las BBDD? ¿Por qué motivos se transfieren esos datos? ¿Cómo se transfieren (desde el punto de vista técnico-informático)?
- ¿Las transferencias son nacionales y/o internacionales?
- ¿Existe un protocolo de entrega de información a las autoridades de persecución penal? ¿Se solicita por nota de la institución o por orden judicial?

Infraestructura

- ¿Cuántas personas trabajan en la unidad que se encarga del mantenimiento de la infraestructura que soporta las bases de datos?

"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