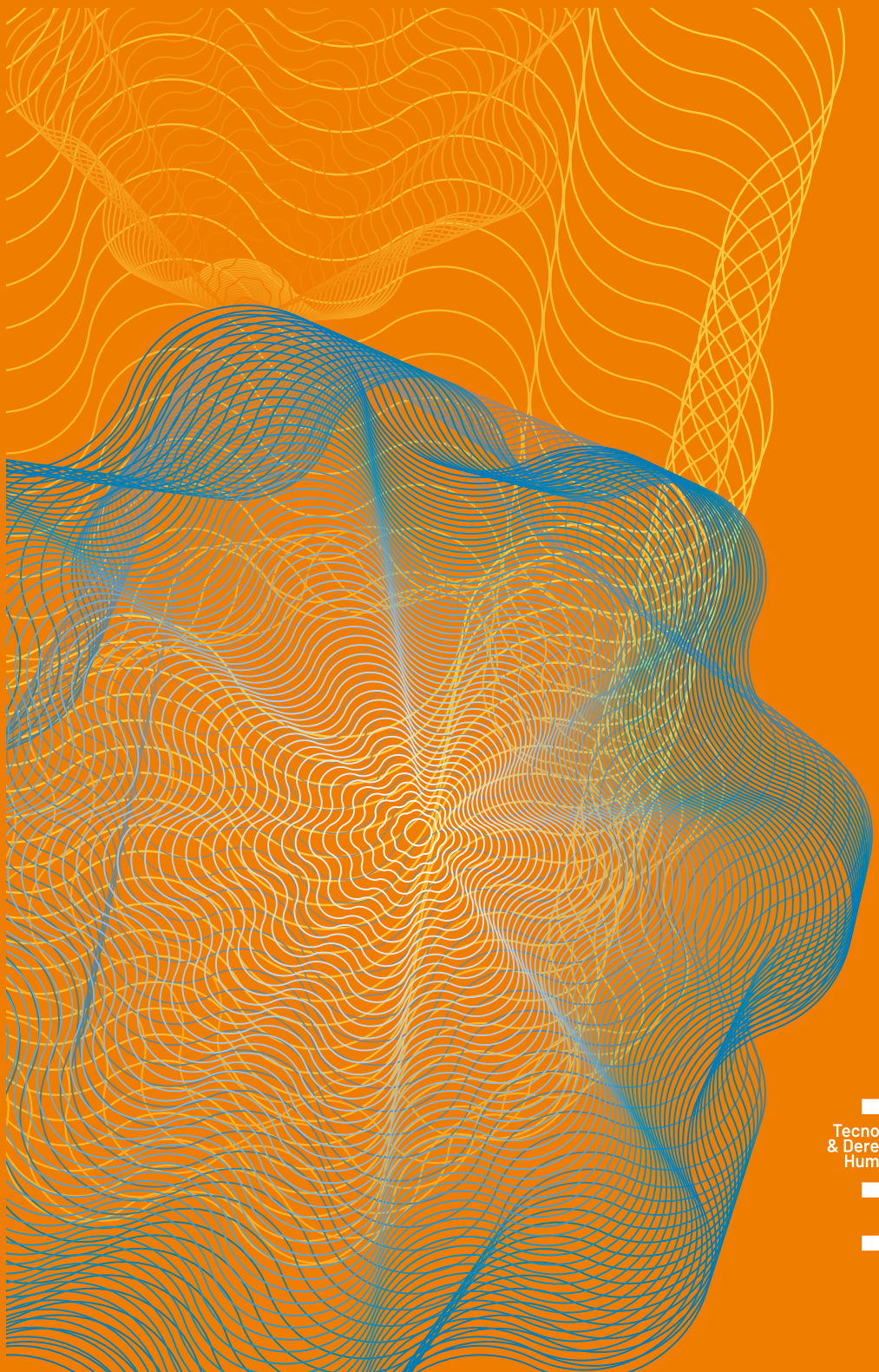
PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR PRIVADO EN PARAGUAY

Un estudio exploratorio



Tecnología & Derechos Humanos

TEDIC

PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR PRIVADO EN PARAGUAY

Un estudio exploratorio

Tecnología & Derechos Humanos

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

Esta investigación fue posible con el apoyo de:
INDELA (Iniciativa por los derechos digitales en Latinoamérica) financia, capacita y brinda apoyo a organizaciones que promueven los derechos digitales en Latinoamérica. La iniciativa está conformada por la Fundación Avina, Luminate y Open Society Foundations (OSF), con el apoyo de Fundación Ford y el Centro Internacional de Investigaciones para el Desarrollo (IDRC).

PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR PRIVADO EN PARAGUAY

Un estudio exploratorio

JUNIO 2024

INVESTIGACIÓN
Giuliana Galli

ASISTENCIA DE INVESTIGACIÓN
Gabriela Galilea

COORDINACIÓN
Eduardo Carrillo

EDICIÓN Y REVISIÓN
Eduardo Carrillo y Maricarmen Sequera

DISEÑO Y DIAGRAMACIÓN
Horacio Oteiza

COMUNICACIÓN
Araceli Ramírez

TABLA DE CONTENIDOS

RESUMEN EJECUTIVO

La presente investigación consiste en un estudio exploratorio que sistematiza prácticas en materia de protección de datos personales de empresas del sector privado entrevistadas, principalmente tomando en consideración el proyecto de ley de protección de datos personales, que a la fecha se encuentra en proceso legislativo, con el objeto de evaluar el grado de cumplimiento que existe respecto a los principios establecidos en este proyecto de ley, así como los principales desafíos ante su entrada en vigencia y efectiva aplicación.

Se aborda asimismo, el marco legal que acoge el derecho a la protección de datos personales a nivel jurídico internacional y nacional, así como las limitaciones existentes en el esquema legal y normativo vigente en Paraguay sobre este derecho, resaltando la necesidad de contar con un marco de protección integral de datos personales, que preserve adecuadamente esta dimensión del individuo.

Entre los principales hallazgos de la investigación:

- El derecho a la protección de datos personales en Paraguay cuenta con reconocimiento de rango constitucional, derivando conceptualmente de otros derechos fundamentales expresamente consagrados, cuyos bienes jurídicos tutelados garantizan este derecho.

- En Paraguay, la protección de datos personales se limita formalmente a la protección de datos personales de naturaleza *crediticia*, omitiéndose una perspectiva integral del derecho. La protección o tutela actualmente disponible, resulta insuficiente para constituir un marco integral acorde a los estándares internacionalmente establecidos en la materia.

- La legislación referente al derecho al libre acceso a la información pública en Paraguay y sus medidas de protección vigentes, refuerzan la necesidad de una debida tutela jurídica por parte del Estado en materia de protección de datos personales, a fin de equilibrar la protección jurídica sobre ambas dimensiones de derechos fundamentales.

- El proyecto de ley de protección de datos personales actualmente en proceso legislativo, apunta a instaurar un conjunto de normas reguladoras del derecho a la protección de datos personales de forma integral, estableciendo una Autoridad de Control con competencias suficientes y adecuadas para supervisar y controlar su implementación, un régimen sancionatorio y un procedimiento para su aplicación.

- Como resultado de las entrevistas, se evidencia la imperiosa necesidad de avanzar en materia de concienciación y sensibilización acerca del derecho a la protección de datos personales, a la ciudadanía en general. Las personas deben identificarse como adjudicatarias de éste derecho, entendiendo su gravitación dentro de la esfera de derechos fundamentales y la protección mínima exigible a los responsables del tratamiento de sus datos personales.

- Asimismo, es apremiante la necesidad de concientización sobre las garantías que la aplicación de la ley de protección de datos personales trae a las empresas, a fin de disipar preconceptos y percepciones erradas sobre la implementación de la ley, dando paso a las ventajas que contrariamente pondría a disposición para las mismas.

- Se evidencia que no se comprende a la protección de los datos personales como un derecho fundamental de los Titulares de estos datos, ni como una obligación ineludible para los responsables del tratamiento. Las medidas de protección que puedan llegar a aplicarse actualmente, en su caso responden de forma incompleta a los principios y enunciados en la materia y en atención a otros intereses.

- Existe un alto grado de incomprensión sobre conceptos principales de la materia, como el consentimiento, la necesidad de contar con una base legal para el tratamiento, la responsabilidad de seguridad que compete a quienes realizan el tratamiento, entre otros.

- Resulta inaplazable la sanción de una ley integral de protección de datos personales, para establecer las bases legales para la vigencia y garantía adecuada de este derecho fundamental. Es urgente destrabar el tratamiento del proyecto de ley de protección de datos personales en proceso legislativo, generar un debate basado en la evidencia, que permita sentar las bases de una digitalización responsable por parte de actores privados y públicos.

INTRODUCCIÓN

El derecho a la protección de datos personales reviste en la actualidad un indiscutible carácter de derecho fundamental, pasando a integrar el catálogo de derechos humanos reconocidos en ordenamientos supranacionales y nacionales.

Sin embargo, haber alcanzado este reconocimiento es el resultado de un proceso abierto y dinámico de transformación[1], que fue definiendo sus principales caracteres y el alcance de su ámbito de protección, a través de su ejercicio y delimitación frente a distintas situaciones que pusieron a prueba su conceptualización. Tales pruebas permitieron comprobar sus rasgos autónomos e independencia respecto a derechos que le dieron origen, como el derecho a la privacidad e intimidad. Como resultado de este proceso, se construyó el consenso social suficiente sobre la importancia de proteger esta dimensión de la persona humana, inherente a sus valores más propios como la libertad, la dignidad y la intimidad.

En las últimas décadas, este proceso fue apuntalado por el vertiginoso desarrollo de las nuevas Tecnologías de Información y Comunicación (TICs), que impuso un ritmo nunca antes visto en el tratamiento de datos personales mediante la utilización de herramientas TIC en prácticamente todas las áreas de la vida cotidiana. La creciente exposición al tratamiento de datos personales ha puesto de resalto la necesidad de reconocer este derecho en la legislación de cada país, de manera a establecer el marco de derechos y responsabilidades necesario para su efectiva protección.

En Paraguay, la protección de datos personales ha avanzado hasta la fecha, únicamente respecto a la protección de datos personales de naturaleza ***crediticia***[2] y no así desde una perspectiva integral del derecho. Actualmente existe un proyecto de ley de protección de datos personales[3], en estudio ante el Poder Legislativo, cuya redacción:

> *Está basada en la normativa y los estándares internacionales y se tuvieron en cuenta regulaciones existentes a nivel internacional específicas en la materia como el Reglamento (UE) 2016/679, y legislación comparada que ha sido sancionada en los últimos años*[4].

Paraguay es uno de los pocos países de la región que aún no cuenta con un marco normativo integral de protección de datos personales. Por ello, resulta imperiosa la sanción de esta ley para establecer las bases legales para la vigencia y garantía de este derecho fundamental.

---

1 Ver más en Graciela Romero Silvera, «Interés público y protección de datos personales con especial referencia a los Derechos Humanos», 2010, 2010, https://www.redipd.org/sites/default/files/2020-01/Graciela_Romero.pdf.

2 «Ley 6534/2020 "De protección de Datos Personales Crediticios"» (s. f.). artículo 3.-Definiciones, inciso h) establece: "Información crediticia: Es aquella información, positiva y negativa, relacionada con el historial crediticio de personas físicas y jurídicas, acerca de actividades crediticias, comerciales y otras de naturaleza análoga, que sirva para identificar correcta e inequívocamente a la persona, su domicilio, actividad comercial, determinar su nivel de endeudamiento, de cumplimiento de sus obligaciones y, en general, de riesgos crediticios en un determinado momento." Este sería el ámbito de protección efectiva de la Ley, a través de sus mecanismos de control, reclamos y sanción.

3 «Proyecto de Ley de Protección de Datos Personales en Paraguay», accedido 11 de abril de 2024, https://silpy.congreso.gov.py/web/expediente/123459.

4 Ídem. Exposición de motivos del Proyecto de Ley presentado ante el Congreso de la Nación.

Esta investigación pretende ser un pequeño aporte, con particular atención a prácticas del sector privado en Paraguay en materia de recolección y tratamiento de datos personales. La investigación pretende caracterizar, en primer lugar, el encaje legal que acoge este derecho a nivel jurídico nacional, y dejar expuestas ciertas conclusiones a las que se ha arribado como resultado de las entrevistas llevadas a cabo con diferentes empresas del sector privado. El escenario que se presenta, deja ver la necesidad de proteger adecuadamente esta dimensión del individuo, estableciendo un marco legal de protección integral de los datos personales para los habitantes del Paraguay.

Sobre el proyecto de Ley de Protección de Datos Personales

El proyecto de Ley de Protección de Datos Personales se constituye en un esfuerzo colectivo liderado por la Coalición de Datos Personales[5]. La misma lidera el proceso de debate, escritura y cabildeo de un proyecto de ley de protección de datos personales que, de ser aprobado, plantea un cambio paradigmático en la recolección y tratamiento de datos personales en el Paraguay.

En estrecha colaboración con la Comisión de Ciencia y Tecnología de la Cámara de Diputados[6], la Coalición alcanzó el hito de presentar en marzo del 2021, el proyecto de ley en la mesa de entrada de la Cámara de Diputados. Desde entonces, el proyecto aún se encuentra en su primer trámite constitucional[7], a pesar de numerosos esfuerzos de la Coalición de Datos Personales[8] para aclarar dudas de parte de hacedores de políticas públicas a nivel ejecutivo y legislativo, así como de abordar las implicancias del proyecto y facilitar su avance. Esto con el objetivo de lograr un proyecto de ley consensuado entre las múltiples partes interesadas, que permita preservar la integridad del texto inicialmente presentado y la fortaleza de sus disposiciones, inspiradas en legislación a nivel regional e internacional.

5 «¿Quiénes somos? – Coalición de Datos Personales Py», accedido 11 de abril de 2024, https://www.datospersonales.org.py/quienes-somos/.

6 TEDIC, «Inician las Mesas de Trabajo para una Ley Integral de Datos Personales», TEDIC (blog), 20 de febrero de 2020, https://www.tedic.org/inician-las-mesas-de-trabajo-para-una-ley-integral-de-datos-personales/.

7 Coalición de Datos Personales Py, «Urgen tratamiento de proyecto que protege datos personales», accedido 11 de abril de 2024, https://www.datospersonales.org.py/urgen-tratamiento-de-proyecto-que-protege-datos-personales/.

8 Coalición de Datos Personales Py, «Comunicado de la Coalición de Datos Personales en respuesta a las publicaciones y declaraciones hechas en medios periodísticos sobre el proyecto de ley de protección de datos personales», accedido 11 de abril de 2024, https://www.datospersonales.org.py/comunicado-de-la-coalicion-de-datos-personales-en-respuesta-a-las-publicaciones-y-declaraciones-hechas-en-medios-periodisticos-sobre-el-proyecto-de-ley-de-proteccion-de-datos-personales/.

MARCO METODOLÓGICO

La investigación objeto de este trabajo, se propone sistematizar las actuales en materia de protección de datos personales, de empresas paraguayas de distintos sectores, a través de entrevistas[9]. A partir de tal exploración, se busca evidenciar la necesidad de contar con un marco legal integral en el territorio nacional, que garantice la protección de los datos personales, la debida tutela jurídica de los derechos derivados de esta protección, el ejercicio libre e irrestricto de los derechos por parte de sus titulares y el tratamiento adecuado de los datos personales por los distintos sectores de la sociedad.

Partiendo del reconocimiento de que la legislación vigente se encuentra aún distante de establecer un marco integral de protección de datos personales, se incorpora al contexto de exploración de esta investigación, el proyecto de ley de protección de datos personales que a la fecha se encuentra en proceso legislativo[10], a fin de identificar los desafíos para el sector privado en miras a la entrada en vigencia y efectiva aplicación de este marco normativo. Concretamente, se propone un instrumento de entrevista que busca medir el grado de cumplimiento de estas empresas respecto a los principios mencionados en el proyecto de ley de protección de datos personales, que son los principios de licitud del tratamiento, exactitud de datos, finalidad, minimización, lealtad, transparencia, conservación, responsabilidad proactiva, seguridad, confidencialidad, consentimiento; así como los Derechos de Acceso, Rectificación, Oposición, Supresión y Portabilidad de los datos personales del titular[11]. El mismo se encuentra como Anexo a este informe.

La investigación se realiza con un enfoque principalmente cualitativo, que busca comprender y describir los hallazgos encontrados, a partir de las experiencias y perspectivas compartidas por las personas entrevistadas. Para ello se llevaron a cabo entrevistas con personal de empresas de, al menos, cada uno de los tres rubros elegidos.

La muestra seleccionada para este estudio consiste en sectores del ámbito privado que, en distintos grados y para diversas aplicaciones, manejan o tratan datos personales. Por tanto, pueden ser consideradas representativas del sector privado para determinar el contexto de prácticas actuales, arrojando una perspectiva que ayude a comprender los desafíos de cara al cumplimiento de los principios incorporados en el proyecto de ley ya mencionado. Las entrevistas son de carácter anónimo, para garantizar un ambiente de confianza a las personas entrevistadas y acceder así a información relevante sobre el tema en estudio.

Se consideran dentro del contexto de esta investigación, también aquellos hallazgos identificados en trabajos de investigación anteriores sobre el estado de la protección de los datos personales en Paraguay en el sector público[12] y privado[13].

---

9 Las empresas pertenecen a rubros de fintech, sector de bienes raíces y de recursos humanos, siendo escogidas por su el grado de representatividad en sus respectivos rubros, con un plantel de empleados de entre 1 a 20 personas, en promedio.

10 «Proyecto de Ley de Protección de Datos Personales en Paraguay», accedido 11 de abril de 2024, https://silpy.congreso.gov.py/web/expediente/123459.

11 Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos, «Principios actualizados sobre la privacidad y la protección de datos personales / [Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos]», 2022., p.59.

12 Jazmín Acuña, Luis Alonzo Fulchi, y Maricarmen Sequera, «La Protección de Datos Personales en Bases de Datos Públicas en Paraguay - Un estudio exploratorio» (Paraguay: TEDIC, 2017), https://www.tedic.org/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay/.

13 Luis Alonzo Fulchi y Maricarmen Sequera, «La protección de datos personales en el sector privado de Paraguay - Un estudio exploratorio» (Paraguay: TEDIC, 2018).

Limitaciones en el marco de la investigación

La población determinada para esta investigación es limitada y selectiva. Si bien se busca obtener una lectura que parte de sectores diversos y heterogéneos, y arrojar elementos para diagramar las prácticas vigentes en materia de protección de datos personales en el sector privado, esta investigación de carácter cualitativo no podrá describir con la profundidad necesaria, cuál sea el estado definitivo en la materia.

En ese orden, podrán existir otros rubros, otras empresas e incluso la interpretación de las personas entrevistadas puede diferir a la práctica real, pudiendo alcanzarse conclusiones distintas bajo otro marco metodológico. No obstante, el resultado obtenido resulta consistente a los efectos exploratorios definidos para esta investigación.

MARCO LEGAL

El derecho a la protección de datos personales está reconocido como un derecho fundamental. Su vigencia en el territorio nacional deviene tanto de los instrumentos de derecho internacional aprobados y ratificados por la República del Paraguay, así como al integrarse y derivarse conceptualmente de otros derechos fundamentales expresamente consagrados en la Constitución Nacional, cuyos bienes jurídicos tutelados guardan directa relación y garantizan la vigencia de este derecho. A partir de éstos, se reconoce el derecho a la protección de datos personales como un derecho personalísimo[14].

Como derivación de este carácter fundamental del derecho a la protección de datos personales, el respeto, la responsabilidad y la garantía de su vigencia, compete tanto al Estado como a la sociedad toda, adjudicándose de forma especial un activo rol en la protección y prevención de su vulneración, a las empresas y el sector privado[15].

Carácter fundamental del derecho a la protección de los datos personales

Si bien nuestro marco constitucional no reconoce de forma expresa el derecho a la protección de datos personales, en el ámbito internacional es indiscutible su consagración como derecho fundamental, desde hace largo tiempo.

La Declaración Universal de Derechos Humanos de 10 de diciembre de 1948, expresa en su Artículo 12 que: *"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".*

Establece por otra parte, el Artículo 19: *"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."*

La evolución del reconocimiento del derecho a la protección de datos personales ha tenido como punto de partida, el derecho a la protección a la privacidad o intimidad[16]. Este derecho humano consagra los pilares que permiten arribar posteriormente, al derecho a la protección de datos personales como derecho fundamental.

---

14 Marcela BASTERRA, Protección de Datos Personales, 2018.a ed. (Buenos Aires: Editora AR, s. f.)., p. 29: *"...son definidos como las prerrogativas de contenido extrapatrimonial, inalienables, perpetuas y oponibles erga omnes [oponibles a todos], que corresponden a toda persona por su sola condición de tal desee antes de su nacimiento y hasta después de su muerte, de las que no puede ser privado por la acción del Estado ni de otros particulares porque ello implicaría desmedro o menoscabo de la personalidad"*, citando a RIVERA, Julio César.

15 Principios Rectores Sobre las Empresas y los Derechos Humanos: Puesta en Práctica del marco de las Naciones Unidas para "proteger, Respetar y Remediar" (United Nations, 2011), https://doi.org/10.18356/3b7fe68b-es.
"Las empresas deben respetar los derechos humanos. Eso significa que deben abstenerse de infringir los derechos humanos de terceros y hacer frente a las consecuencias negativas sobre los derechos humanos en las que tengan alguna participación", éste constituye uno de los Principios Rectores enunciados en el documento elaborado por las Naciones Unidas.

16 Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos, «Principios actualizados sobre la privacidad y la protección de datos personales / [Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos]». p. 21: *"El concepto de privacidad está consagrado en el derecho internacional. Se basa en los conceptos fundamentales del honor personal y la dignidad, así como en la libertad de expresión, pensamiento, opinión y asociación, reconocidos por los principales sistemas de derechos humanos del mundo. En las Américas, estos conceptos están claramente establecidos en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre (1948) y en los artículos 11 y 13 de la Convención Americana sobre Derechos Humanos ("Pacto de San José") (1969) (apéndice A) y en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer ("Convención de Belém do Pará") (1994). Asimismo, la Corte Interamericana de Derechos Humanos ha confirmado el derecho a la privacidad"*.

Asimismo, la dimensión de la protección de datos personales que se desarrolla en aras de proteger el acceso a la información, la libre expresión, la libre disposición, intercambio y tratamiento de datos, en una sociedad de la información globalizada e informatizada, toma como punto de partida el derecho humano a la libertad de opinión y de expresión.

En el Convenio N° 108 del Consejo de Europa *"Convenio para la Protección de las personas con respecto al Tratamiento Automatizado de datos de carácter personal"*[17], del 28 de enero de 1981, adoptado en Estrasburgo y ratificado por 55 países a la fecha, se establece expresamente el carácter fundamental del derecho a la vida privada, ligándose a la realidad del tratamiento automatizado de datos, como una problemática que cobraba relevancia y demandaba protección ya en aquel tiempo:

> *"Artículo 1. Objeto y fin. El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)."*

Alrededor de este mismo tiempo, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) reconoce igualmente el derecho a la protección de datos personales, elaborando en 1980 las *"Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales"*[18]. Esta organización cuenta con recomendaciones que constituyen documentos para orientar a sus Estados miembros.

En esta línea, en la OCDE existe una agenda de protección de datos con el fin de establecer regulaciones básicas de protección de datos que garanticen el libre flujo de la información, así como evitar regulaciones que creen barreras proteccionistas en el comercio internacional. La OCDE emitió la *"Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información"*[19], la *"Declaración sobre el acceso de los gobiernos a los datos personales en poder de las entidades del sector privado"*[20] (traducción no oficial), así como propició la firma de Acuerdos y otras recomendaciones sobre temas que abordan a la protección de datos personales.

Actualmente, el instrumento internacional de mayor referencia en materia de protección de datos, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, conocido como General Data Protection Regulation ("GDPR" por sus siglas en inglés), afirma de forma categórica el carácter de derecho fundamental del derecho a la protección de datos personales, con total autonomía:

---

17 Consejo de Europa, «Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981», Pub. L. No. Acuerdo Internacional (1985), https://www.boe.es/eli/es/ai/1981/01/28/(1).

18 OECD, Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales Resumen (OECD, 2002), https://doi.org/10.1787/9789264196391-en.

19 OCDE, Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información, 2021., elaborada por la Secretaría del Foro Global sobre Transparencia e Intercambio de Información con Fines Fiscales (Foro Global). La Guía fue elaborada "con el objeto ayudar a los países interesados en participar en el intercambio automático de información (AEOI, por sus siglas en inglés), asegurando que cumplan con las buenas prácticas y estándares en materia de confidencialidad y protección de datos. Ofrece orientación general sobre la adopción de un marco jurídico y un sistema de GSI que garanticen la confidencialidad de la información sobre los contribuyentes, incluida la que se intercambia en virtud de acuerdos internacionales…".

20 «Declaration on Government Access to Personal Data Held by Private Sector Entities», OECD Legal Documents, OCDE, accedido 22 de abril de 2024, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

> *"La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen."*[21]

La Organización de Estados Americanos (OEA), de la cual Paraguay forma parte como miembro permanente[22], ha venido ocupándose asimismo sobre la protección de datos personales, aportando importantes documentos elaborados con el objeto de erigirse como punto de referencia para el desarrollo de un marco jurídico de protección de datos personales en los países, su fortalecimiento y protección armónica en la región.

En esa línea, el Comité Jurídico Interamericano (CJI) de la Organización de Estados Americanos (OEA), adopta en el año 2012 la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas, que *"tiene por objeto proporcionar una guía para la preparación e implementación de leyes nacionales y normas conexas en los Estados Miembros de la OEA"*[23].

En este documento, se conceptualiza a los datos personales como: *"información que identifica o puede usarse de manera razonable para identificar a una persona física de forma directa o indirecta, especialmente por referencia a un número de identificación, datos de localización, un identificador en línea a uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social. Incluye información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo. La frase no abarca la información que no identifique a una persona en particular (o no puede usarse de manera razonable para identificarla)."*[24]

Como ámbito de referencia en la región, también se ha constituido la Red Iberoamericana de Protección de Datos (RIPD)[25], conformada por Jefes de Estado y de Gobierno de países iberoamericanos, incluyendo doce países miembros y otros tantos en calidad de observadores, entre ellos Paraguay, representada a través de la Secretaría de la Función Pública. En 2017 esta Red aprueba los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos" [26], con el apoyo de la Comisión Europea.

Estos estándares constituyen un conjunto de directrices orientadoras a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana, así como referente para la modernización y actualización de las legislaciones existentes. En ellos se reconoce asimismo el carácter fundamental del derecho a la protección de datos personales de las personas físicas, expresando: *"(1) Considerando que la protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental que se encuentra reconocido con rango máximo en la mayoría de*

---

21 Parlamento Europeo y del Consejo, «REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016 - relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos)» (Diario Oficial de la Unión Europea, 2016)., Considerando (1).

22 Cfr. en el sitio de la OEA: https://www.oas.org/es/estados_miembros/estado_miembro.asp?sCode=PAR

23 Organización de Estados Americanos (OEA) Comité Jurídico Interamericano, «INFORME DEL COMITÉ JURÍDICO INTERAMERICANO - PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES» (Río de Janeiro, Brasil, 2015), https://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf.

24 Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos, «Principios actualizados sobre la privacidad y la protección de datos personales / [Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos]».

25 Sitio de la Red Iberoamerica de Protección de Datos, visitado en el siguiente enlace: https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd

26 Red Iberoamericana de Protección de Datos (RIPD), «Estándares de Protección de Datos de los Estados Iberoamericanos», 2017, https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

las Constituciones Políticas de los Estados Iberoamericanos, bajo la forma del derecho a la protección de datos personales o habeas data, y que en algunos casos ha sido definido jurisprudencialmente por sus Tribunales o Cortes Constitucionales"[27].

También, se define dato personal como: *"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"*[28].

Las declaraciones y reconocimientos de este derecho a nivel internacional, supranacional, que han sido traídas a vista, dan cuenta del innegable carácter fundamental que lo inviste. Así también, de los conceptos elaborados de *datos personales* puede extraerse como condición esencial, que se trata de información capaz de identificar con precisión y asociarse en forma unívoca a la ***identidad*** de una determinada persona, a la cual el dato pertenece. Los datos personales se integran y funden con el núcleo esencial e inherente de la persona humana, la identidad misma.

De ello se desprende que toda persona, por su sola calidad de tal, goza del derecho a ser protegida en éste ámbito[29]. Tal como lo menciona la Declaración Americana de los Derechos y Deberes del Hombre: *"los derechos esenciales del hombre no nacen del hecho de ser nacional de determinado Estado sino que tienen como fundamento los atributos de la persona humana"*[30].

Este principio también se ve afirmado por lo establecido en el artículo 45 de la Constitución Nacional, que dispone:

> *Artículo 45.- DE LOS DERECHOS Y GARANTÍAS NO ENUNCIADOS. La enunciación de los derechos y garantías contenidos en esta Constitución no debe entenderse como negación de otros que, siendo inherentes a la personalidad humana, no figuren expresamente en ella. La falta de ley reglamentaria no podrá ser invocada para negar ni para menoscabar algún derecho o garantía.*

En el entramado constitucional de la República del Paraguay, el derecho a la protección de los datos personales integra el ámbito de protección de la dignidad del hombre y su derivación de los derechos fundamentales de libertad, intimidad, privacidad, honor, hábeas data, inviolabilidad del patrimonio documental y la comunicación privada.

Su reconocimiento deviene inherente a la misma dignidad humana y su falta de consagración de forma expresa en el texto constitucional, tal como lo advierte el artículo 45 citado, no podría conllevar su negación o menoscabo, bajo ninguna circunstancia.

---

27 Ídem, Considerando 1.

28 Ídem.

29 Asamblea General de las Naciones Unidas, «Declaración Universal de Derechos Humanos», 1948, https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf.
Artículo 1: "Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros".

30 Ídem. Texto invocado en el "Considerando" de la Declaración.

Dos grandes dimensiones del derecho a la protección de datos personales

El derecho a la protección de los datos personales se proyecta hacia dos grandes objetivos: por un lado, como derecho fundamental que integra el respeto de la dignidad humana, personalísimo e inherente a toda persona, inserto en el derecho a la libertad, la intimidad, la privacidad y el honor; y, desde este prisma de derechos fundamentales, como derecho a la autodeterminación informativa, la inviolabilidad del patrimonio documental, la comunicación privada y el *hábeas data*[31].

Por otro lado, este derecho se proyecta hacia la libertad de expresión y pensamiento, el derecho a informarse y acceder libremente a información, garantizando la libre circulación o libre flujo de los datos e información. La autodeterminación informativa, considerada no solamente desde una visión negativa, de impedir la vulneración o el avance no consentido hacia la esfera de lo que se considera íntimo y parte de la persona misma; sino también considerada en su faz positiva, de libre disposición de sus derechos de intercambio, acceso y tratamiento de datos, en una sociedad de la información globalizada e informatizada.

Contar con un marco adecuado de protección de los datos personales, favorece el intercambio de información en forma segura, el tratamiento para diversos fines realizado de forma legítima, la calidad de la información, la libre disposición de información y otros aspectos sustanciales para la dimensión de la persona humana en los tiempos actuales, de la sociedad de la información[32].

Protección constitucional del derecho a la protección de datos personales

Para comprender el marco legal del derecho a la protección de datos personales en Paraguay, es fundamental recurrir en primer lugar a las disposiciones de la Constitución Nacional, como ley suprema de la Nación (Artículo 37) y en tal carácter *"destinada a ordenar e infundir los principios rectores del resto del ordenamiento jurídico"*[33].

---

31 El Hábeas Data es una garantía constitucional reconocida en el Artículo 135, que expresa: Del Hábeas Data. *Toda persona podrá acceder a la información y a los datos que sobre sí 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. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.*
Esta institución jurídica protege la información y datos personales, garantizando el acceso, la actualización, rectificación e incluso supresión o eliminación, toda vez que su recolección y tratamiento pudiera afectar ilegítimamente derechos del Titular.

32 Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos, «Principios actualizados sobre la privacidad y la protección de datos personales / [Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos]»., p. 95: "La capacidad universal de acceder y contribuir a la información, las ideas y el conocimiento es un elemento indispensable en una Sociedad de la Información integradora. Es posible promover el intercambio y el fortalecimiento de los conocimientos mundiales en favor del desarrollo si se eliminan los obstáculos que impiden un acceso equitativo a la información para actividades económicas, sociales, políticas, sanitarias, culturales, educativas y científicas, y si se facilita el acceso a la información que está en el dominio público, lo que incluye el diseño universal y la utilización de tecnologías auxiliares. Un dominio público rico es un factor esencial del crecimiento de la Sociedad de la Información, ya que genera ventajas múltiples tales como un público instruido, nuevos empleos, innovación, oportunidades comerciales y el avance de las ciencias. La información del dominio público debería ser fácilmente accesible en apoyo de la Sociedad de la Información, y debería estar protegida de toda apropiación indebida. Habría que fortalecer las instituciones públicas tales como bibliotecas y archivos, museos, colecciones culturales y otros puntos de acceso comunitario, para promover la preservación de las constancias documentales y el acceso libre y equitativo a la información".

33 Alberto BIANCHI, Control de Constitucionalidad, 1992.a ed., vol. I (Buenos Aires: Ábaco, s. f.)., p.30.

En la Constitución de la República del Paraguay se reconoce la dignidad humana en el Artículo 1[34], como basamento de la forma de gobierno democrática de la nación como Estado Social de Derecho. La decisión constitucional de adoptar un Estado Social de Derecho, necesariamente implica reconocer el derecho a la protección de la libertad de decisión sobre aquello que integra la esfera personal e íntima de cada persona (como lo son los datos personales), considerando que *"la esencia del Estado de Derecho consiste en garantizar, por medio del Derecho, la libre determinación de las personas"*[35].

El derecho a la protección de datos personales está intrínsecamente ligado y se origina asimismo de forma inmediata, a partir del derecho a la libertad. El derecho a la libertad se encuentra expresamente consagrado en la Constitución Nacional:

> *Art. 9. De la libertad y de la seguridad de las personas. Toda persona tiene el derecho a ser protegida en su libertad y en su seguridad. Nadie está obligado a hacer lo que la ley no ordena ni privado de lo que ella no prohíbe.*[36]

Como parte de los derechos personalísimos e inherentes a la persona humana, el derecho a la protección de los datos personales se integra en el derecho a la intimidad, reconocido en el artículo 33 de la Constitución Nacional:

> *"Del 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, estará exenta de la autoridad pública. Se garantiza el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas."*

El honor y la reputación constituyen igualmente, bienes jurídicos de carácter fundamental, tutelados por la Constitución Nacional. Estos derechos pueden verse directamente vulnerados como consecuencia del tratamiento de datos personales que no observe las garantías de libertad de cada persona y el respeto a la intimidad. Se encuentran garantizados en virtud al Artículo 4 de la Constitución Nacional:

> *Artículo 4. Del derecho a la vida. El derecho a la vida es inherente a la persona humana. Se garantiza su protección, en general, desde la concepción. Queda abolida la pena de muerte. Toda persona será protegida por el Estado en su integridad física y psíquica, así como en su honor y en su reputación. La ley reglamentará la libertad de las personas para disponer de su propio cuerpo, sólo con fines científicos o médicos.*

---

34 Artículo 1 de la Constitución de la República del Paraguay, año 1992: *"De la forma del Estado y de gobierno. La República del Paraguay es para siempre libre e independiente. Se constituye en Estado social de derecho, unitario, indivisible y descentralizado en la forma que establecen esta Constitución y las leyes. La República del Paraguay adopta para su gobierno la democracia representativa, participativa y pluralista, fundada en el reconocimiento de la dignidad humana".*

35 Eberhard Schmidt-Assmann, La Teoría General del Dercecho Administrativo como Sistema (Madrid: Instituto Nacional de Administración Pública Marcial Pons, 2003)., p.52.

36 Este principio establecido en la Constitución, se refleja asimismo en el Artículo 283 del Código Civil, primera parte.: *"Nadie puede obligar a otro a hacer alguna cosa, o restringir su libertad, sin estar legalmente autorizado para ello".*

El Artículo 36 *"Del derecho a la inviolabilidad del patrimonio documental y la comunicación privada"* de la Constitución Nacional, aporta elementos importantes al marco de protección de datos personales:

> *Artículo 36. Del derecho a la inviolabilidad del patrimonio documental y 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 o lo precripto anteriormente carecen de valor en juicio. En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado.*

En primer lugar, garantiza la protección de los datos personales, al proscribir la violación del patrimonio documental y la comunicación privada de las personas. El acceso a información y datos que integren el patrimonio documental, propiedad de una persona, sea cual fuere el formato en que se encuentren, sólo puede permitirse mediante orden judicial amparada en la ley.

Por otra parte, es interesante destacar que este artículo establece una limitación de *finalidad y proporcionalidad*[37] en el tratamiento de datos personales, al disponer que este acceso será *"siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades". También subraya la proporcionalidad necesaria y minimización del acceso, expresando que "en todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado".*

Es dable señalar lo dispuesto en el artículo 30 *in fine,* que establece una protección especial de la intimidad personal ante el uso de las señales de comunicación electromagnética:

> *Artículo 30. De las señales de comunicación electromagnética.*
> *[...]*
> *Las autoridades asegurarán que estos elementos no sean utilizados para vulnerar la intimidad personal o familiar y los demás derechos establecidos en esta Constitución."*

37 La finalidad como concepto en materia de protección de datos, tiene que ver con que todo tratamiento de datos personales debe limitarse al cumplimiento de una finalidad previamente establecida, que además debe ser en todos los casos, legítima: *"El requisito de legitimidad en las finalidades para las cuales se tratan los datos personales es una norma fundamental, profundamente arraigada en valores democráticos básicos y en el estado de derecho. En principio, la recopilación de datos personales debería ser limitada y realizarse con el conocimiento o el consentimiento de la persona. No deberían recopilarse datos sobre personas excepto en las situaciones y con los métodos permitidos o autorizados por ley y (por lo general) deberían darse a conocer a las personas afectadas en el momento en que se recopilen. Los Estados Miembros deberían, por lo tanto, incluir en sus legislaciones nacionales disposiciones específicas sobre las finalidades legítimas del Tratamiento de Datos Personales"* (Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, Organización de los Estados Americanos).
La proporcionalidad, por su parte, prescribe que una vez determinada esta finalidad legítima, los datos personales serán objeto de un tratamiento acorde a la misma, bajo criterios de pertinencia, necesidad y minimización: *"Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior. [...] …el requisito de que los datos sean "pertinentes" significa que deberían guardar una relación razonable con las finalidades para las cuales hayan sido recopilados y se tenga la intención de usarlos. [...] …deberían hacer un esfuerzo razonable para cerciorarse de que los Datos Personales que manejen correspondan al mínimo requerido para la finalidad expresa"* (Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, Organización de los Estados Americanos).

La Constitución Nacional consagra el Hábeas Data como garantía constitucional, para toda persona ciudadana que requiera el acceso a la información y datos sobre sí misma o sus bienes. Esta garantía dispone la tutela jurisdiccional inherente al derecho a la protección de datos personales, con el máximo rango normativo:

> *Artículo 135. Del Hábeas Data. Toda persona podrá acceder a la información y a los datos que sobre sí 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. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.*

La proyección del derecho a la protección de datos personales sobre otros derechos fundamentales

Desde la vertiente tutelar al derecho al libre acceso a la información y libertad de expresión, como expresiones del derecho a la protección de datos personales, la Constitución Nacional estatuye:

> *Artículo 28. Del derecho a informarse. Se reconoce el derecho de las personas a recibir información veraz, responsable y ecuánime. Las fuentes públicas de información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo. 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.*

El artículo 28 se encuentra reglamentado a través de la Ley N° 5282/14 "De libre acceso a la información pública"[38], que tiene por objeto garantizar el ejercicio del derecho a la información pública[39], a la cual se define como aquella producida, obtenida, bajo control o en poder de las fuentes públicas[40]. A su vez, conforme a la ley, las fuentes públicas son todos los organismos públicos que integran los poderes del Estado.

Esta legislación tutela el libre acceso de toda la ciudadanía a la información pública, dotando de los mecanismos legales en instancia administrativa y jurisdiccional[41], para que este derecho sea efectivamente observado y cumplido.

---

38 «Ley N° 5282/14 "De libre acceso a la información pública"» (2014), https://informacionpublica.paraguay.gov.py/public/ley_5282.pdf.

39 Ídem, *"Artículo 1.- Objeto. La presente ley reglamenta el artículo 28 de la Constitución Nacional, a fin de 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. Ninguna disposición de esta ley podrá ser entendida o utilizarse para negar, menoscabar o limitar la libertad de expresión, la libertad de prensa o la libertad de ejercicio del periodismo".*

40 *"Artículo 2.- Definiciones. 2. Información pública: 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".*

41 La vía procesal fue determinada por Acordada de la Corte Suprema de Justicia N°1005/2014, por la cual se dispone que para el caso de denegación expresa o tácita de una solicitud de acceso a la información, la acción judicial se tramite según las reglas para el juicio de amparo; y para el caso de cualquier otro incumplimiento de una repartición pública con relación a las obligaciones previstas en la Ley 5282/14, la acción judicial se tramite por las reglas del procedimiento sumario.

La protección de datos personales no es referida de forma expresa, pero asoma su presencia bajo la salvedad excluyente expresada en el concepto de información pública del artículo 2, inciso 2, : *"...salvo que se encuentre establecida como secreta o de carácter reservado por las leyes",* así como lo dispuesto en el artículo 22 que define la información pública reservada como *"...aquella que ha sido o sea calificada o determinada como tal en forma expresa por la ley".*

No obstante, la realidad ha sido que las fuentes públicas se han encontrado con un escenario difuso, indeterminado y altamente controvertido, en cuanto se trató de la denegación de acceso a información pública, por contener datos personales que se estimaron —en ciertos casos— como indisponibles para su divulgación[42].

La garantía del derecho de acceso a la información pública, por medio de su reglamentación en la Ley N° 5282/14, hace aún más necesario el dictado de un marco adecuado de protección de datos personales, que delimite su alcance y ofrezca principios y criterios interpretativos que permitan una adecuada ponderación del alcance de cada uno de estos derechos, en determinadas situaciones de tensión entre éstos.

La protección que hoy existe al derecho al libre acceso a la información pública confirma la necesidad de una debida tutela jurídica por parte del Estado en materia de protección de datos personales, ya que solo de esta forma se brindará una adecuada protección de los mismos, siendo imperativo equilibrar el ordenamiento jurídico hacia ambos extremos.

En cuanto al derecho a la libertad de expresión y de prensa, la Constitución ratifica este derecho en el artículo 26, refiriendo a la posibilidad de *"generar, procesar o difundir información"* como parte del mismo:

> *Artículo 26. De la libertad de expresión y de prensa. Se garantizan la libre expresión y la libertad de prensa, así como la difusión del pensamiento y de la opinión, sin censura alguna, sin más limitaciones que las dispuestas en esta Constitución; en consecuencia, no se dictará ninguna ley que las imposibilite o las restrinja. No habrá delitos de prensa, sino delitos comunes cometidos por medio de la prensa. Toda persona tiene derecho a generar, procesar o difundir información, como igualmente a la utilización de cualquier instrumento lícito y apto para tales fines.*

La protección de datos personales debe convivir en armonía con el derecho al libre acceso a la información y la libertad de expresión; ambas dimensiones de derechos fundamentales se encuentran en un pie de igualdad y deben, por tanto, gozar de equivalente protección, evitando que la vigencia y efectividad de uno, signifique la supresión o menoscabo del otro.

No existirá una verdadera libertad de expresión y de prensa, en la medida en que su ejercicio no pueda reputarse íntegramente respetuoso de la privacidad e intimidad de las personas, por falta de claridad de los límites entre éstos derechos.

---

42 En el fallo de la Corte Suprema de Justicia, recaído en la causa *"Acción de inconstitucionalidad en los autos caratulados: Amparo constitucional L. F., J. C. c. Contraloría General de la República (Ac. y Sent. N° 111)"*, se plantea la tensión entre el concepto de información pública de las Declaraciones Juradas de funcionarios públicos, y la protección de la privacidad y datos personales de los titulares de estas declaraciones, debiendo mediar para su divulgación, un pedido de un órgano jurisdiccional competente (Ley N° 5033/13). La postura adoptada por la C.S.J. no fue unánime, y en el voto de la Dra. Boungermini se exhiben importantes y valiosos argumentos a favor de la protección de datos personales en el derecho positivo nacional y supranacional, y la ponderación que necesariamente debe realizarse en cada caso, considerando que *"ambos son derechos humanos, sino que tiene que ser ponderada caso por caso, atendiendo a los ya conocidos criterios de finalidad, razonabilidad y proporcionalidad, que son esenciales a la hora de juzgar derechos fundamentales de rango constitucional."*

Ley N° 6534 "De protección de Datos Personales Crediticios"

La anterior legislación que regía sobre la materia de protección de datos personales - Ley N° 1682/2001 "Que reglamenta la información de carácter privado"[43]y sus modificatorias-, lo hacía desde la limitada perspectiva de reglamentar la información de "carácter privado". Apenas se conceptualizaban los datos sensibles (artículo 4), se legitimaba el tratamiento de datos o características personales, para fines científicos, estadísticos, encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualice las personas o entidades investigadas (artículo 3), así como el tratamiento de datos personales para uso estrictamente privado (artículo 1). Por último, se disponía sobre el derecho al libre acceso a la información (artículo 2).

Derogando esta ley, se publica en 2020 la actual Ley N° 6534 "De protección de Datos Personales Crediticios"[44], que tiene por objeto garantizar la protección de datos crediticios de toda persona. Con esta ley podría notarse una leve evolución positiva en materia de protección de datos personales, en tanto se incorporan principios básicos, desde una perspectiva más amplia de derechos fundamentales, como lo expresa el Artículo 1 *"...con el fin de preservar los derechos fundamentales, la intimidad, la autodeterminación informativa, la libertad, la seguridad y el trato justo de las personas, de conformidad con lo establecido en la Constitución Nacional, la presente Ley y los Tratados suscritos y ratificados por la República del Paraguay"*[45].

En esta línea, la ley define conceptos clave[46] que, hasta su publicación, no habían aparecido consagrados en una ley especial: dato personal, tratamiento, Titular, Responsable del tratamiento, Encargado del tratamiento, Consentimiento; además de conceptos específicos sobre el objeto de la ley, como información crediticia, sus fuentes y sociedad de información crediticia. Además, se incorporan ciertos principios que resultan preliminares a todo tratamiento de datos personales que se pretenda realizar: derecho a la autodeterminación informativa (artículo 5), derecho al consentimiento informado y la ilicitud del tratamiento y cesión no consentida de datos personales (artículo 6), el principio de exactitud o calidad de la información (artículo 7), la consagración de los derechos disponibles para el titular de los datos como acceso, rectificación, cancelación y oposición, para los cuales el responsable debe hacer disponible un procedimiento y medios sencillos, expeditos, accesibles y gratuitos (artículo 8), derecho a la seguridad de los datos (artículo 10), entre otros.

Sin embargo, tal como se ha apuntado en las investigaciones anteriores realizadas[47], en materia de protección de datos personales *"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."*[48]

---

43 «Ley No 1682/2001 "Que reglamenta la información de carácter privado"» (2001), https://www.bacn.gov.py/archivos/1760/20130923115653.pdf.

44 Ley 6534/2020 "De protección de Datos Personales Crediticios".

45 Ídem, Artículo 1: *"Objeto. La presente Ley tiene por objeto garantizar la protección de datos crediticios de toda persona, cualquiera sea su nacionalidad, residencia o domicilio. También se busca regular la actividad de recolección y el acceso a datos de información crediticia, así como la constitución, organización, funcionamiento, derechos, obligaciones y extinción de las personas jurídicas que se dediquen a la obtención y provisión de información crediticia, con el fin de preservar los derechos fundamentales, la intimidad, la autodeterminación informativa, la libertad, la seguridad y el trato justo de las personas, de conformidad con lo establecido en la Constitución Nacional, la presente Ley y los Tratados suscritos y ratificados por la República del Paraguay".*

46 Ídem, Artículo 3.- Definiciones.

47 Acuña, Fulchi, y Sequera, «La Protección de Datos Personales en Bases de Datos Públicas en Paraguay - Un estudio exploratorio».

48 Ídem. P. 15.

De esta forma, el marco legal vigente sobre derechos, deberes y obligaciones en materia de protección de datos personales, además del marco constitucional, en su ámbito formal se constituye hoy por la referida Ley N° 6534/20, reglamentada a su vez por Resoluciones de las Autoridades de Aplicación: Banco Central del Paraguay, por Resolución N°03/2023 del Directorio[49]; y la Secretaría de Defensa al Consumidor y al Usuario (SEDECO), por Resolución SDCU 1502 del 26 de septiembre de 2022[50].

Desde este bloque normativo, resulta evidente que la protección o tutela actualmente disponible para el derecho de protección a los datos personales, está lejos de ofrecer un marco integral acorde a los estándares internacionalmente establecidos para garantizar un nivel adecuado de protección.

Esto último, en primer lugar porque el alcance de la legislación y su normativa reglamentaria, se enfoca en los derechos personales de naturaleza "crediticia" y como consecuencia, todo el esquema de reclamación y posible ejercicio de los derechos de protección de datos personales: Derechos de Acceso, Rectificación, Oposición, Supresión y Portabilidad de los datos personales del titular, así como la determinación de obligaciones que recaen sobre los responsables del tratamiento, prohibiciones, e incluso, las sanciones aplicables, se limitan —conforme a los Capítulos II y III de la Ley— a los datos personales de naturaleza crediticia exclusivamente. Toda vulneración al derecho de protección de datos personales que no revista naturaleza crediticia, no cuenta con un régimen de mecanismos y procedimientos para hacer valer este derecho y suscitar la protección adecuada del Estado[51].

Otra consecuencia que se desprende del limitado alcance de la ley, es que el marco normativo vigente no atiende adecuadamente a la necesidad de contar con una autoridad de control independiente e imparcial en sus potestades, cuyas decisiones únicamente puedan ser recurribles por el control judicial, ajenas de toda influencia externa, con facultades de supervisión e investigación en materia de protección de datos personales, y dotada de recursos humanos y materiales suficientes para su cometido[52].

En este sentido, la ley establece dos autoridades de aplicación distintas, cuyas potestades deben ser ejercidas conforme al ámbito de competencia que legalmente les corresponde. (y El ámbito de competencias que les corresponde de acuerdo a su marco legal de creación[53], precede esta atribución

---

49 Banco Central del Paraguay, «Resolución N°03/2023 del Directorio, REGLAMENTO DE BURÓS DE INFORMACIÓN CREDITICIA (BIC) Y PROTECCIÓN DE LA INFORMACIÓN PERSONAL CREDITICIA EN EL MARCO DE LA LEY N° 6534/2020 DE PROTECCIÓN DE DATOS PERSONALES CREDITICIOS», 2023.

50 Secretaría de Defensa al Consumidor y al Usuario (SEDECO), «Resolución SDCU No 1.502, del 26 de septiembre de 2022, «POR LA CUAL SE REGLAMENTA LOS ARTÍCULOS 6o, 9° y 20° DE LA LEY N° 6.534_2020« .pdf», 2022.

51 Cfr. Red Iberoamericana de Protección de Datos (RIPD), «Estándares de Protección de Datos de los Estados Iberoamericanos»., Considerando 25: *"...régimen que garantice a los titulares una serie de mecanismos y procedimientos para presentar sus reclamaciones ante la autoridad de control cuando consideren vulnerado su derecho a la protección de datos personales, así como para ser indemnizados cuando hubieren sufrido daños y perjuicios como consecuencia de una violación de su derecho".*

52 Ídem, Considerando 24.

53 El ámbito natural de competencia del Banco Central del Paraguay, conforme a lo establecido en la Ley N°6104 "Que modifica y amplía la Ley N° 489/95 "ORGÁNICA DEL BANCO CENTRAL DEL PARAGUAY", artículo 3°.- Objetivos, establece: *"Son objetivos fundamentales del Banco Central del Paraguay preservar y velar por la estabilidad del valor de la moneda y promover la eficacia, integridad y estabilidad del sistema financiero".*
Por su parte, en cuanto a la SEDECO, la Ley N° 4974 "DE LA SECRETARÍA DE DEFENSA DEL CONSUMIDOR Y EL USUARIO", establece lo siguiente en el artículo 2°.-Ámbito de Competencia: *"La Secretaría de Defensa del Consumidor y el Usuario (SEDECO) actuará como Autoridad de Aplicación en el ámbito Nacional de la Ley de Defensa del Consumidor y el Usuario y de las demás Leyes y reglamentos que rigen la materia…"* y en el Artículo 5°.-Objetivos: *"La Secretaría de Defensa del Consumidor y el Usuario (SEDECO), tiene por objeto: a. Velar por el cumplimiento de las disposiciones de la presente Ley y demás normas que rijan y tengan relación en materia de protección al consumidor y el usuario; b. Difundir los derechos y deberes como también realizar acciones de información y educación al consumidor; c. Promover la formalización del mercado, evitando la desprotección del consumidor y el usuario."*

especial en la materia, y acota sustancialmente el alcance que puedan ejercer en materia de protección de datos personales. Sumado a ello, el propio ámbito de alcance de protección que establece la ley se limita a los datos personales de naturaleza *crediticia*.

Por otra parte, las decisiones que adopten estas Autoridades en ejercicio de estas competencias, no agotan la instancia administrativa, ni están, por lo tanto, exentas de revisión en instancia administrativa.

Otro aspecto que denota la insuficiencia del marco legal vigente, es la ausencia de regulación sobre medidas proactivas a cargo de los responsables, que a su vez sean impulsadas y promovidas por la autoridad de aplicación. Estas medidas son esenciales en el sistema de protección de datos personales, ya que atribuyen la responsabilidad de rendición de cuentas y de toma de acciones de forma activa y preventiva, tanto al sector público como a las empresas y demás actores del sector privado. Entre ellas se encuentran la adopción de esquemas de autorregulación vinculante o sistemas de certificación en la materia, designación de un oficial de protección de datos personales, elaboración de evaluaciones de impacto, privacidad por defecto y por diseño[54].

No puede dejar de mencionarse asimismo, la omisión en la legislación vigente respecto a la dimensión de protección y regulación del "libre flujo de información", específicamente en cuanto a las transferencias internacionales de datos personales, aspecto que demanda un adecuado y suficiente abordaje, que siente las bases para que su realización no obstaculice el comercio, la innovación, el intercambio de datos, el desarrollo; sino que lo promueva, preservando la integridad del tratamiento apropiado de los datos personales.

En ese orden, puede comprobarse todavía la situación advertida en los trabajos de investigación anteriores, de que *"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"*[55].

Proyecto de Ley de Protección de Datos Personales en el Congreso

En el año 2021 ha sido presentado el proyecto de "Ley de Protección de Datos Personales en Paraguay"[56], que aún se encuentra siguiendo el correspondiente proceso legislativo, como respuesta a la necesidad de un adecuado marco legal integral de protección de datos personales, invocando a tal efecto sólidos argumentos demostrados en la exposición de motivos que lo integra.

Este proyecto de ley surge como resultado del trabajo de múltiples partes interesadas, bajo el impulso de la Coalición de Datos Personales[57], así como el apoyo de la entonces vigente Comisión de Ciencia y Tecnología de la Cámara de Diputados. Como se menciona en la exposición de motivos, *"la mesa de trabajo siguió los principios de la gobernanza de Internet, siendo abierto, colaborativo, voluntario, inclusivo y transparente, con la participación de múltiples partes interesadas. Se realizaron webinars de socialización y discusión con expertos regionales y de la Unión Europea sobre datos personales, para debatir el*

54 Red Iberoamericana de Protección de Datos (RIPD), «Estándares de Protección de Datos de los Estados Iberoamericanos»., Considerando 23.

55 Acuña, Fulchi, y Sequera, «La Protección de Datos Personales en Bases de Datos Públicas en Paraguay - Un estudio exploratorio».

56 «Proyecto de Ley de Protección de Datos Personales en Paraguay».

57 Formada durante el cuarto Foro de Gobernanza de Internet del Paraguay - IGFPY, en el año 2017. Sitio web disponible en: https://www.datospersonales.org.py

anteproyecto de ley y compartir experiencias de los diferentes actores. Además, se recibieron comentarios y contribuciones de la sociedad civil organizada, la comunidad empresarial, representantes del gobierno, del sector técnico y académico y ciudadanos interesados en el tema"[58].

El proyecto de ley apunta a establecer definitivamente un conjunto de normas reguladoras del derecho a la protección de datos personales, que revistan carácter obligatorio tanto para el sector privado como el público, y conformen un cuerpo coherente y sistemático, dotado de una Autoridad de Control con competencias suficientes y adecuadas para supervisar y controlar su implementación, un régimen sancionatorio y procedimientos para su aplicación.

Las carencias señaladas en el marco legal vigente en materia de protección de datos personales, son debidamente atendidas en la propuesta legislativa, que se extiende de forma integral sobre la protección de datos personales, abarcando cada uno de los principios consensuados a nivel internacional[59], incorporando las dimensiones que propician el libre flujo de información, aspectos de seguridad, mecanismos de autorregulación; autoridad de aplicación con competencias suficientes de supervisión e investigación, independencia de criterio y sujeta a suficiente control judicial.

Los desafíos para su aplicación no son menores, por lo que a conciencia de ello y con la debida cautela, se establece un periodo de 24 (veinticuatro) meses a partir de su sanción, para su efectiva entrada en vigor, a fin de que todos los sectores involucrados incorporen estas disposiciones al tratamiento de datos que realicen.

Desde la Coalición de Datos Personales, se ha realizado una loable tarea de armonización de este marco legal propuesto a nivel internacional, para adecuarlo a la realidad local y a las configuraciones legales que rigen en nuestro territorio.

Si bien no puede negarse la extensión y aparente complejidad de la propuesta legislativa, no debe perderse de vista la importancia de la sanción de la ley sin mayores remisiones reglamentarias que aquellas estrictamente necesarias, puesto que la experiencia de países más avanzados en la aplicación de esta ley ha demostrado que este derecho fundamental exige un marco de protección de rango legal, suficientemente robusto y coherente, que aborde con amplitud los desafíos de protección, el acceso a derechos que garantizan esta protección, conciliando su vigencia con la innovación tecnológica y los desafíos de la sociedad de la información y la economía digital, cruciales en el desarrollo económico.

58 Ver en: https://silpy.congreso.gov.py/web/expediente/123459

59 Cfr. Principios en Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas, adoptada por el Comité Jurídico Interamericano (CJI) de la Organización de Estados Americanos (OEA), 2015. Disponible en: https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_Guia_Legilsativa_CJI.pdf

ENTREVISTAS Y HALLAZGOS

Como parte del proceso de recolección de datos realizado en el marco de la presente investigación, se llevaron a cabo entrevistas con personal calificado de empresas de cada uno de los tres rubros elegidos: fintech, recursos humanos y bienes raíces.

Las empresas entrevistadas pertenecen al ámbito privado y, en distintos grados y para diversas aplicaciones, manejan o tratan datos personales. Las preguntas de investigación que fueron realizadas[60] han permitido reflejar una perspectiva sobre el grado de comprensión y cumplimiento de los Principios sobre protección de datos personales, así como los desafíos de cara al cumplimiento de éstos, incorporados en el proyecto de ley ya mencionado.

Como resultado de estas conversaciones, se ha estudiado y procesado la información recopilada, que se pasa a exponer en la siguiente tabla, ordenando de acuerdo a cada uno de los Principios de protección de datos personales establecidos en el proyecto de ley (que coinciden con los estándares internacionales reconocidos), las respuestas obtenidas y analizadas, a modo de extraer deducciones a partir de las mismas. Para aquellos casos en los que nos fue posible extraer de la entrevista una cita textual, se coloca una síntesis de lo expuesto por parte de la persona autora.

Por último, y a modo de diferenciar la aplicación actual de los principios *vis-a-vis* las percepciones de las personas entrevistadas en la implementación futura de la ley, se hace un análisis separado de la tabla con los principios.

60 Formulario de preguntas disponible en el Anexo I.

PRINCIPIOS	FINTECH	RRHH	BIENES RAÍCES
Principio de Licitud del tratamiento: Para que el tratamiento sea lícito, los datos personales deben ser tratados conforme a alguna de las bases jurídicas previstas en la ley[61]: Consentimiento de Titular; Contrato o trámites preliminares, a solicitud de éste; Intereses legítimos del Responsable, siempre que sobre dichos intereses no prevalezcan los derechos y libertades fundamentales; La licitud del tratamiento, además de tener que realizarse sobre alguna de estas bases legales, depende del cumplimiento de todos los principios y demás disposiciones del marco legal de protección de datos personales.	*"...tenemos todo un contrato que tiene términos y condiciones larguísimos, te puedo enviar… en dónde está todo lo que se contempla para ese tipo de cosas.."* Si bien el entrevistado dice que en los Términos y Condiciones se establece la base legal para el tratamiento de datos personales, al leerlos no se evidencia ninguna mención acerca de las condiciones de legalidad de este tratamiento. No existiendo otro documento dentro de la relación con los titulares de datos, asimilable a un contrato, esta base legal quedaría descartada. Tampoco se declaró en la entrevista obtener ningún tipo de consentimiento de parte de los Titulares. Por último, podría considerarse la posibilidad de argumentar un interés legítimo en el tratamiento de datos por parte de la empresa, en tanto los datos obtenidos son necesarios para la realización del procesamiento del pago deseado por el Titular. Sin embargo, en tal caso deben acreditarse los requisitos para su adecuada configuración, entre ellos y principalmente, un análisis previo de necesidad, proporcionalidad y legitimidad.	*"No. Yo confirmo que no está en la postulación no aparece (consentimiento)"* *"En el formulario de postulación no hay una explicación de qué datos se van a recoger y para qué..."* De las posibles bases legales para el tratamiento, no resultaría aplicable invocar el consentimiento del Titular, según lo confirma el entrevistado. Tampoco existe un Contrato con el Titular de los datos en la etapa de recolección, según nos relata la persona entrevistada. Existe una Política de Privacidad en la página web, que contiene disposiciones claras sobre el tratamiento de los datos personales que hace la empresa. Sin embargo, esta política no forma parte de la interacción con el Titular de Datos y por tanto, no se configura como un Contrato, no habiendo acuerdo de voluntades. Podría considerarse la posibilidad de argumentar un interés legítimo en el tratamiento de datos por parte de la empresa, en tanto los datos obtenidos son necesarios para la realización del procesamiento de la solicitud de empleo realizada por el Titular. Sin embargo, en tal caso, deberán acreditarse los requisitos para su adecuada configuración, entre ellos y principalmente, un análisis previo de necesidad, proporcionalidad y legitimidad.	*"No, realmente no (tenemos consentimiento expreso). Sí (tenemos) una vez que se desembolsa el crédito recién, en el contrato está esto que me mencionas…"* *"No sé si el interés de la persona en acceder al crédito, en la gestión de su crédito es a lo que se podría considerar como un consentimiento…"* La empresa entrevistada trata datos de carácter crediticio, por lo tanto solo un consentimiento expreso configuraría una base legal para el tratamiento, de acuerdo a la legislación vigente en protección de datos crediticios (Ley 6534, art. 6). Tal consentimiento no es obtenido, conforme lo relatan las personas entrevistadas. Tampoco indican la existencia de un contrato previo al tratamiento, que pudiera configurarse como base legal para el tratamiento de datos personales. Podría considerarse la posibilidad de argumentar un interés legítimo en el tratamiento de datos por parte de la empresa, en tanto los datos obtenidos son necesarios para el procesamiento del crédito deseado por el Titular, tal como la persona entrevistada incluso manifiesta. Sin embargo, en tal caso deberán acreditarse los requisitos para su adecuada configuración, entre ellos y principalmente, un análisis previo de necesidad, proporcionalidad y legitimidad.

61 Considerando el grupo de entrevistados, se listan las bases jurídicas que resultarían aplicables a su condición. Se omite mencionar las demás bases legales establecidas, en tanto no les resultarían aplicables: cumplimiento de una obligación legal o reglamentaria; Poderes del Estado, en ejercicio de sus funciones propias; Datos que figuren en fuentes de acceso público; Para procedimientos judiciales, administrativos o arbitrales.

Principio de exactitud de datos: Los datos personales serán veraces, exactos, completos y actualizados. Los responsables y encargados del tratamiento deben adoptar todas las medidas razonables para corregir errores, modificar los datos que resulten ser falsos, inexactos, desactualizados o incompletos y garantizar la certeza y veracidad de la información objeto de tratamiento.	*"Si el comercio (adherido) actualiza, sí, si no, no…"* De acuerdo al entrevistado, las categorías de los datos de Titulares que son recolectados, son definidas por los comercios que contratan el servicio de la empresa. La exactitud de los datos recolectados no consiste en un interés de la empresa entrevistada, que presta servicios transaccionales meramente. Todo aspecto relativo a la veracidad, exactitud o actualización de los datos recolectados y almacenados, queda bajo control de los comercios, según lo que manifiestan. Si hubiera una inconsistencia en los datos, existe la posibilidad de que el Titular solicite la actualización al comercio. De la operativa relatada, surge que existen datos que sí son recolectados únicamente para la prestación del servicio de la empresa entrevistada (pago), por lo que como responsables de éstos datos, deberían adoptar las medidas para cumplir con este principio. Aún actuando como encargado, le corresponden iguales responsabilidades.	*"El postulante también puede ir actualizando en cualquier momento."* Los datos recolectados quedan a vista de sus Titulares en todo momento, en tanto éstos pueden acceder al sistema en el cual están almacenados, de acuerdo a lo que manifiesta el entrevistado. De esta forma, los Titulares tienen pleno acceso a sus datos, para modificar, actualizar, corregir. El interés de la empresa radica fundamentalmente en que los datos sean lo más veraces, exactos, completos y actualizados, por lo que se busca proactivamente que el Titular propicie y ofrezca esta exactitud.	Los datos son corregidos y actualizados según lo que el Titular le indique a la empresa. Estas correcciones o actualizaciones que realizan de los datos, apuntan directamente a los intereses de la empresa, en cuanto al perfil crediticio que construyen de los clientes y la posibilidad de prestar sus servicios. Se denota, por los testimonios recolectados en la entrevista, que existe cierta proactividad por parte de la empresa en buscar, actualizar y tener exactitud en los datos de su interés, para así viabilizar la prestación de servicios.

Principio de Finalidad: Los datos personales deben ser recogidos y procesados con fines determinados, explícitos, legítimos y de duración limitada, y no serán tratados, posteriormente, de manera incompatible o distinta con dichos fines.	*"Se va a guardar en mi sistema, pero qué deciden ellos pedir depende de cada comercio."* Los datos recolectados no son utilizados para ninguna otra finalidad que no sea la transacción para la cual el Titular provee los datos, de acuerdo a lo relatado. No hay una duración determinada para el almacenamiento, que se efectúa por tiempo indefinido. Según lo que manifiesta la persona entrevistada, la definición de las categorías de datos a recolectar para cada transacción, la realiza el comercio adherido, que utiliza los servicios de la empresa. Por tanto, no hay un análisis y limitación de la finalidad por parte de la empresa entrevistada.	*"No averiguamos más ni un otro dato extra, sino exclusivamente el desempeño de la persona si tuvo algún antecedente negativo y luego llamamos a recursos humanos para corroborar…"* Los datos son tratados únicamente para la finalidad para la cual fueron recolectados, de acuerdo a lo manifestado. No hay una duración determinada para el almacenamiento, que se realiza por tiempo indefinido.	*"Nosotros nos quedamos simplemente en lo que la persona necesita…. un dato más, no le solicitamos."* Los datos son tratados únicamente para la finalidad para la cual fueron recolectados, de acuerdo a lo manifestado. No hay una duración determinada para el almacenamiento, que se realiza por tiempo indefinido.
Principio de Minimización: El responsable y el encargado tratarán únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento. Asimismo, los datos deberán someterse a revisión periódica para determinar si continúan cumpliendo la finalidad.	De lo relatado, surge que no habría un control de cumplimiento de este principio. El comercio decide según su criterio qué categorías de datos recolectar, y la empresa simplemente almacena los datos que ésta indica; luego, la empresa utiliza únicamente aquellos datos que necesita para procesar la transacción. Siendo indeterminada la duración del almacenamiento, no se verifica un control de la finalidad *a posteriori.*	Se deja ver que sí existe un control sobre los criterios que componen este principio, ya que se recolectan únicamente aquellos datos que la empresa considera necesarios para prestar sus servicios a las personas usuarias y clientes. Sin embargo, se resalta también en la entrevista, la pérdida de control sobre la finalidad y la necesidad, sobre el uso de los datos que realizan los clientes de la empresa (terceros) a los cuales ésta transfiere datos de los titulares (perfiles elaborados).	Se deja ver que sí existe un control sobre los criterios que componen este principio, ya que se recolectan únicamente aquellos datos que la empresa considera necesarios para prestar sus servicios a los Titulares interesados. Siendo indeterminada la duración del almacenamiento, no se verifica un control de la finalidad *a posteriori.*

Principio de Lealtad: No podrán recabarse datos personales por medios o métodos fraudulentos, engañosos, desleales o ilícitos, lo que implica que: No se recaben datos personales con dolo, mala fe o negligencia No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado. Se informen todas las finalidades del tratamiento.	Los datos son recolectados en el marco de la relación comercial entre cliente y comercio. De lo relatado, no se explicita al Titular de datos en ningún momento, qué tratamiento se dará a los datos ni la duración de su almacenamiento. Sin embargo, se denota de la entrevista que no hay un exceso o deslealtad respecto a la recolección y tratamiento que se realiza de los datos, que se limita a la finalidad que el Titular puede razonablemente presumir cuando entrega sus datos (procesamiento de pago).	*"La analista tiene como parte de su speech mencionarle que los datos le compartimos al cliente"* *"No dejamos escrito en ningún documento ni en ninguna plataforma si es que la persona dio información falsa o tuvo malas referencias…"* Según la persona entrevistada, verbalmente se le informa al Titular qué tratamiento se le dará a sus datos y en la práctica no se excede este uso informado. Se denota que no hay un exceso o deslealtad respecto a la recolección y tratamiento que se realiza de los datos, que se limita a la finalidad que el Titular puede razonablemente presumir cuando entrega sus datos (búsqueda de empleo). Se resalta la pérdida de control sobre el uso de los datos que realizan los clientes de la empresa (terceros) a los cuales ésta transfiere datos de los titulares (perfiles elaborados).	Si bien no se explicita en ningún momento qué tratamiento se le dará a los datos ni la duración de su almacenamiento, se denota que no hay un exceso o deslealtad respecto a la recolección y tratamiento que se realiza de los datos, que se limita a la finalidad que el Titular puede razonablemente presumir cuando entrega sus datos (procesamiento de crédito).
Principio de transparencia: El responsable informará al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. Esta información será fácilmente accesible, en lenguaje claro y sencillo.	De la operativa de tratamiento relatada por la persona entrevistada, se verifica que no existe cumplimiento de este principio. No hay ningún tipo de comunicación expresa y completa por parte de la empresa (o comercio adherido) sobre el tratamiento que se dará a los datos personales entregados por el Titular.	Existe una política de privacidad en la página web en la cual se detalla cuidadosamente el tratamiento que se realizará de los datos por parte de la empresa. Sin embargo, al momento de la utilización del servicio por los Titulares, no se comprueba que éstos hayan leído y comprendido éste documento, y por tanto, se corrobore el cumplimiento de este principio. También manifiestan que existe una comunicación verbal por parte de la empresa, sobre el tratamiento que se dará a los datos, pero recién una vez avanzado el proceso a instancias de la entrevista.	De la operativa de tratamiento relatada por la persona entrevistada, se verifica que no existe cumplimiento de este principio. No hay ningún tipo de comunicación expresa y completa por parte de la empresa (o comercio adherido) sobre el tratamiento que se dará a los datos personales entregados por el Titular.

Principio de conservación: No podrán conservarse o mantenerse los datos durante más tiempo del necesario para los fines del tratamiento. El Responsable del tratamiento deberá establecer los plazos para la supresión y/o revisión periódica.	Según lo expresado por la persona entrevistada, el almacenamiento de los datos es por tiempo indefinido. No hay un proceso de supresión y/o revisión periódica.	Según lo expresado por la persona entrevistada, el almacenamiento de los datos es por tiempo indefinido. No hay un proceso de supresión y/o revisión periódica.	Según lo expresado por la persona entrevistada, el almacenamiento de los datos es por tiempo indefinido. No hay un proceso de supresión y/o revisión periódica.
Principio de responsabilidad proactiva: El responsable y encargado del tratamiento debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente Ley, y que le permitan demostrar a la Autoridad de Control su efectiva implementación.	De la operativa de tratamiento relatada por el entrevistado, se verifica que no existe cumplimiento de este principio.	De la operativa de tratamiento relatada por el entrevistado, se verifica que no existe cumplimiento de este principio.	De la operativa de tratamiento relatada por el entrevistado, se verifica que no existe cumplimiento de este principio.
Principio de Seguridad: En el tratamiento de datos personales se deberán adoptar medidas técnicas y organizativas que garanticen la seguridad de los datos y que tendrán como finalidad evitar la alteración, pérdida, tratamiento o acceso no autorizado.	De acuerdo a lo relatado, el acceso a los datos recolectados y almacenados, está restringido únicamente a quienes se encuentren autorizados por los comercios adheridos a los servicios de la empresa, a través de perfiles con niveles de accesos diferenciados. Se registran todos los accesos realizados. Cada acceso se limita a los datos relacionados a los servicios prestados a cada comercio exclusivamente. No hay medidas adicionales a éstas, sobre el cumplimiento de este principio.	Según lo relatado, la información recolectada y almacenada es accedida únicamente por analistas de búsqueda, que pertenecen a la empresa. No se reporta la implementación de medidas adicionales para garantizar la seguridad.	*"...no hay nadie que vele por la seguridad más que cada persona de la de sus archivos, que no se modifiquen"* Los datos recolectados son almacenados de forma abierta a todo el personal de la empresa, sin control de accesos de ningún tipo. Incluso carecen de control para la descarga de información, que se almacena de forma compartida por todos. No se reporta la implementación de medidas como las exigidas en este principio.

Principio de Confidencialidad: Los responsables y encargados del tratamiento de datos de carácter personal, así como toda persona que intervenga en cualquier fase de este estarán sujetas al deber de confidencialidad, obligación que subsistirá aun después de finalizar sus relaciones con el titular.	No se reporta la implementación de medidas que garanticen el cumplimiento de este principio, según lo relatado.	No se reporta la implementación de medidas que garanticen el cumplimiento de este principio, según lo relatado.	No se reporta la implementación de medidas que garanticen el cumplimiento de este principio, según lo relatado.
Derechos al Acceso, Rectificación, Oposición, Supresión y Portabilidad de los datos personales del Titular: El responsable deberá establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular de datos ejercer sus derechos.	De acuerdo a lo relatado, no existen procedimientos ofrecidos al Titular para el ejercicio de estos derechos. Sin embargo, consideran factible el acceso, la rectificación y supresión, en caso de que el Titular lo solicite al comercio o a la empresa.	"Si nos pide por llamada, por correo, por A o B motivo, lo eliminamos y ya está" De acuerdo a lo relatado, no existen procedimientos ofrecidos al Titular para el ejercicio de estos derechos. Sin embargo, consideran factible y fácil el acceso, la rectificación y supresión, en caso de que el Titular lo solicite.	De acuerdo a lo relatado, no existen procedimientos ofrecidos al Titular para el ejercicio de estos derechos.
Consentimiento: Es toda manifestación de voluntad libre, previa,expresa, específica, informada e inequívoca por la que una persona física acepta y autoriza, ya sea mediante una declaración o una clara acción afirmativa realizada por escrito o por medios electrónicos, así como por cualquier forma equivalente que la tecnología permita, el tratamiento de los datos personales que le conciernen.	No hay un consentimiento otorgado por el Titular, que reúna las condiciones exigidas.	No hay un consentimiento otorgado por el Titular, que reúna las condiciones exigidas.	No hay un consentimiento otorgado por el Titular, que reúna las condiciones exigidas.

Tabla elaborada por la persona autora con base en las entrevistas.

FINTECH	RRHH	BIENES RAÍCES
"...cuando no haya una correlación entre la multa por infringir un protocolo o una ley, y el beneficio que sacas, nunca va a funcionar…"	"...no vamos a poder avanzar si no tenemos el consentimiento recibido de parte de las personas que van a estar siendo parte de nuestros procesos… [...] …si no tenemos la autorización, el consentimiento de nuestros postulantes, no podemos presentar sus datos. Va a ser también mucho más delicado eso y el cliente tiene que entender [...] …Entonces si vos, para pedirle ya su cédula y empezar a analizar su perfil necesitas que te firme un consentimiento, eso para mí va a ser perjudicial, desde mi punto de vista…"	"...la gente piensa que para darte su cédula ya le vas a sacar un préstamo. Imagínate si le pedís que te firme un consentimiento, o sea, para ellos eso va a ser, vos le vas a endeudar y no le vas a dar nada, le vas a estafar, le vas a robar [...] …De que va a impactar en la economía, va a impactar en la economía, si es que no se hace una muy muy buena comunicación, una explicación del porqué, de qué esto es seguro, que es para el beneficio de ellos, no para utilizar sus datos y endeudarle sin su consentimiento."

Tabla elaborada por la persona autora con base en las entrevistas.

Desafíos para aplicar la futura ley de Protección de Datos Personales

Las citas transcritas, tomadas de las entrevistas realizadas en la presente investigación, son ilustrativas de cuáles son los desafíos identificados por éstas personas, en miras a la entrada en vigencia de una Ley de Protección de Datos Personales.

Podemos concluir de las expresiones señaladas, que evidencian en primer lugar la imperiosa necesidad de avanzar en materia de concienciación y sensibilización sobre el derecho a la protección de datos personales, a la ciudadanía en general.

La naturaleza de éste derecho y su ámbito de protección, la necesidad de que las personas se identifiquen como adjudicatarias de éste derecho, entendiendo cuáles son los valores que se hallan comprometidos en esta protección, desde su misma dignidad, libertad, intimidad, seguridad, y demás; son algunos aspectos que demandan un profuso trabajo de concientización, orientación, educación y difusión. Asimismo, es necesario que las personas puedan comprender cuál es la protección mínima exigible a los responsables del tratamiento de sus datos personales, y cuáles son los medios de los que dispone para suscitar esta protección, a través del Estado, ante su vulneración o riesgo.

Por otra parte, es evidente que ante una futura implementación, será necesario un importante trabajo de concientización sobre las garantías que la aplicación de una ley de protección de datos personales trae a empresas. Esto debido a que es posible argumentar, por los testimonios recolectados, que representantes de las empresas perciben como consecuencia directa de la implementación de la ley, una serie de perjuicios sobre la manera en la cuál interactúan con sus clientes, y no al contrario, de que esta ley en realidad les permitirá ofrecer un mayor grado de seguridad a los mismos e incluso tener acceso a nuevas oportunidades de negocios en el extranjero, mayor competitividad en otras jurisdicciones con altos estándares en materia de protección de datos personales.

Otro desafío que se deja ver, es el de lograr que el cumplimiento de la ley y las consecuencias por su incumplimiento puedan ser equitativamente exigibles y aplicables a todos los actores responsables. El *enforcement*, la efectiva aplicación de la ley, es una dimensión de la protección que no debe descuidarse especialmente en sus primeras fases de implementación, ya que sienta las bases para que la protección proactiva, preventiva y el *compliance* de parte de los responsables del tratamiento de datos personales vaya en aumento, generando contención y evitando que se produzcan situaciones de vulneración, cuyas consecuencias nunca son del todo reparables.

CONCLUSIONES

El escenario ilustrado como resultado del procesamiento de los hallazgos, plantea indudablemente importantes desafíos para la efectividad de un marco de protección de datos personales. Esto demandará grandes esfuerzos para crear conciencia sobre la importancia de este derecho, tanto en los Titulares como en los responsables y encargados, así como en la sociedad toda.

El concepto de tratamiento de datos personales es sumamente amplio y abarcativo. Probablemente, y aún sin ser enteramente conscientes, la mayoría de las personas trata datos personales de forma corriente, bien sea para el giro de negocios o prestación de servicios, u otras acciones.

Sin embargo, existen preconceptos o ideas desacertadas asociadas al tratamiento de datos personales, que diluyen la responsabilidad requerida para asegurar la integridad de los mismos y la legitimidad del tratamiento realizado, visibilizadas a través de los testimonios que demuestran la falta de comprensión de nociones elementales en la materia, como los principios, la necesidad de una base jurídica para el tratamiento, el consentimiento, los roles y responsabilidades de quienes participen en el tratamiento.

Respecto a la licitud del tratamiento, se evidencia que aquellas empresas que no obtienen un consentimiento ni formalizan un Contrato, podrían invocar un interés legítimo, considerando la naturaleza y la situación del tratamiento que realizan. Sin embargo, para ello será necesario que transiten con diligencia cada uno de los requerimientos exigidos para su adecuada configuración, como el análisis previo de razonabilidad y proporcionalidad.

Por otra parte, los testimonios evidencian la falta de entendimiento sobre la definición de conceptos de responsable o encargado, especialmente en situaciones en las que son varios los actores involucrados en el tratamiento de datos, dentro de una cadena de servicios para concretar una misma operación. Ante este tipo de situaciones, la competencia o la atribución de definir los fines y medios del tratamiento, es la que determinará quién ostenta la calidad de responsable o encargado del tratamiento de datos personales. Sin embargo, se verifica que esta distinción es minimizada, entendiéndose sencillamente que quién recolecta los datos ante el Titular en primera instancia, es el único responsable del tratamiento.

Es importante comprender que las obligaciones de protección de datos personales persisten a lo largo de toda la cadena de tratamiento del que sean objeto los datos, variando únicamente según se trate de un responsable o encargado. Pero en ningún caso puede darse un tratamiento de datos personales, sin existir un responsable de cumplir los principios y demás disposiciones que garantizan la debida protección.

Por otra parte, se evidencia también que, si bien en ocasiones se cumplen las acciones indicadas en los principios de protección de datos personales, como por ejemplo el principio de exactitud, este cumplimiento se hace únicamente en la medida de los intereses comerciales de la empresa, que se preocupa por la exactitud y actualización de los datos a efectos de poder prestar sus servicios. No se comprenden estas acciones en su dimensión de protección de los datos personales, como un derecho de los Titulares y una obligación de los responsables. Tal protección implicaría adoptar medidas técnicas y organizativas, de forma proactiva, ejecutando acciones aún si esto significase un esfuerzo adicional respecto a las actividades principales del responsable, e incluso, aunque no tengan relación directa con la finalidad específica del tratamiento.

Los principios de minimización, finalidad y conservación, que son enteramente consecuentes entre sí, no son visualizados ni tenidos en cuenta en el marco de los servicios prestados por las empresas. La conservación de datos por tiempo indeterminado en todas las entrevistas, demuestra esta omisión respecto a la necesidad de que el tratamiento se realice siempre en cumplimiento a una finalidad específica. Así, tampoco se verificó el cumplimiento del principio de transparencia, en tanto esta finalidad y demás condiciones, no son puestas a conocimiento previo e informado del Titular.

En definitiva, el tratamiento de datos personales podría decirse que se realiza sin sujetarse a ningún tipo de reglas, sino en la medida de los intereses de las partes y en último caso, guiados por la buena fe.

No se visualiza ni comprende a la protección de los datos personales como un derecho fundamental de los Titulares de estos datos, ni como una obligación ineludible para los responsables del tratamiento. De esta manera, la investigación vuelve a reflotar, una vez más, la necesidad de que Paraguay cuente con una ley integral de protección de datos personales. Es urgente destrabar el tratamiento del proyecto de ley de protección de datos personales en la Cámara de Diputados, con miras a generar un debate basado en la evidencia, que haga foco en los vacíos y prácticas indeseables como aquellas expuestas en la presente investigación, brindando una respuesta a estos escenarios de desprotección y sentando las bases de una digitalización responsable por parte de actores privados y públicos.

BIBLIOGRAFÍA

1. Acuña, Jazmín, Luis Alonzo Fulchi, y Maricarmen Sequera. «La Protección de Datos Personales en Bases de Datos Públicas en Paraguay - Un estudio exploratorio». Paraguay: TEDIC, 2017. https://www.tedic.org/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay/.

2. Asamblea General de las Naciones Unidas. «Declaración Universal de Derechos Humanos», 1948. https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf.

3. Banco Central del Paraguay. «Resolución N°03/2023 del Directorio, REGLAMENTO DE BURÓS DE INFORMACIÓN CREDITICIA (BIC) Y PROTECCIÓN DE LA INFORMACIÓN PERSONAL CREDITICIA EN EL MARCO DE LA LEY N° 6534/2020 DE PROTECCIÓN DE DATOS PERSONALES CREDITICIOS», 2023.

4. BASTERRA, Marcela. Protección de Datos Personales. 2018.a ed. Buenos Aires: Editora AR, s. f.

5. BIANCHI, Alberto. Control de Constitucionalidad. 1992.a ed. Vol. I. Buenos Aires: Ábaco, s. f.

6. Coalición de Datos Personales Py. «Comunicado de la Coalición de Datos Personales en respuesta a las publicaciones y declaraciones hechas en medios periodísticos sobre el proyecto de ley de protección de datos personales». Accedido 11 de abril de 2024. https://www.datospersonales.org.py/comunicado-de-la-coalicion-de-datos-personales-en-respuesta-a-las-publicaciones-y-declaraciones-hechas-en-medios-periodisticos-sobre-el-proyecto-de-ley-de-proteccion-de-datos-personales/.

7. «Urgen tratamiento de proyecto que protege datos personales». Accedido 11 de abril de 2024. https://www.datospersonales.org.py/urgen-tratamiento-de-proyecto-que-protege-datos-personales/.

8. Comité Jurídico Interamericano, Organización de Estados Americanos (OEA). «INFORME DEL COMITÉ JURÍDICO INTERAMERICANO - PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES». Río de Janeiro, Brasil, 2015. https://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf.

9. Consejo de Europa. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, Pub. L. No. Acuerdo Internacional (1985). https://www.boe.es/eli/es/ai/1981/01/28/(1).

10. Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos. «Principios actualizados sobre la privacidad y la protección de datos personales / [Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos]», 2022.

11. Fulchi, Luis Alonzo, y Maricarmen Sequera. «La protección de datos personales en el sector privado de Paraguay - Un estudio exploratorio». Paraguay: TEDIC, 2018.

12. Ley 6534/2020 “De protección de Datos Personales Crediticios” (s. f.).

13. Ley N° 5282/14 “De libre acceso a la información pública” (2014). https://informacionpublica.paraguay.gov.py/public/ley_5282.pdf.

14. Ley No 1682/2001 “Que reglamenta la información de carácter privado” (2001). https://www.bacn.gov.py/archivos/1760/20130923115653.pdf.

15. OCDE. «Declaration on Government Access to Personal Data Held by Private Sector Entities». OECD Legal Documents. Accedido 22 de abril de 2024. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

16. OCDE. Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información, 2021.

17. OECD. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales Resumen. OECD, 2002. https://doi.org/10.1787/9789264196391-en.

18. Parlamento Europeo y del Consejo. «REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016 - relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos)». Diario Oficial de la Unión Europea, 2016.

19. Principios Rectores Sobre las Empresas y los Derechos Humanos: Puesta en Práctica del marco de las Naciones Unidas para “proteger, Respetar y Remediar”. United Nations, 2011. https://doi.org/10.18356/3b7fe68b-es.

20. «Proyecto de Ley de Protección de Datos Personales en Paraguay». Accedido 11 de abril de 2024. https://silpy.congreso.gov.py/web/expediente/123459.

21. «¿Quiénes somos? – Coalición de Datos Personales Py». Accedido 11 de abril de 2024. https://www.datospersonales.org.py/quienes-somos/.

22. Red Iberoamericana de Protección de Datos (RIPD). «Estándares de Protección de Datos de los Estados Iberoamericanos», 2017. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

23. Romero Silvera, Graciela. «Interés público y protección de datos personales con especial referencia a los Derechos Humanos». 2010, 2010. https://www.redipd.org/sites/default/files/2020-01/Graciela_Romero.pdf.

24. Schmidt-Assmann, Eberhard. La Teoría General del Dercecho Administrativo como Sistema. Madrid: Instituto Nacional de Administración Pública Marcial Pons, 2003.

25. Secretaría de Defensa al Consumidor y al Usuario (SEDECO). «Resolución SDCU No 1.502, del 26 de septiembre de 2022, «POR LA CUAL SE REGLAMENTA LOS ARTÍCULOS 6o, 9° y 20° DE LA LEY N° 6.534_2020« .pdf», 2022.

26. TEDIC. «Inician las Mesas de Trabajo para una Ley Integral de Datos Personales». TEDIC (blog), 20 de febrero de 2020. https://www.tedic.org/inician-las-mesas-de-trabajo-para-una-ley-integral-de-datos-personales/.

ANEXO

Guión de entrevista

A. Exploración del tratamiento de datos personales

¿Considera que en el marco de los servicios y actividades realizadas por la empresa, son recolectados datos personales?

En tal caso, ¿qué tratamiento se le da a estos datos personales?

¿Qué "base legal" se considera para esta recolección y tratamiento?
Algunas de las bases legales consideradas legítimas para el tratamiento de datos, serían:

- Consentimiento del Titular de los datos;
- Ejecución de un contrato con el Titular de los datos;
- Obligación legal del responsable (empresa que recolecta y trata);
- Para proteger intereses vitales del interesado;
- En cumplimiento a una misión de interés público o ejercicio de poderes públicos (sólo aplica al Estado);
- Satisfacción de interés legítimo del responsable.
- En caso de basarse en el consentimiento del Titular de los datos, ¿cómo evaluarías los siguientes requisitos del consentimiento?:
- Capacidad de demostrar que existe este consentimiento;
- La solicitud de consentimiento al Titular de los datos personales es distinguible, inteligible, de fácil acceso, en lenguaje claro y sencillo;
- El consentimiento otorgado por parte del TItular es revocable, de la misma forma en que se da;
- No supedita la ejecución del contrato, al otorgamiento del consentimiento de datos que no son necesarios para su ejecución, por parte del Titular.

B. Principios de protección de datos personales

¿Se notifica e informa al Titular de datos sobre la recolección y tratamiento que se realiza de sus datos personales? ¿de qué forma se realiza esta información? (principio de transparencia, de lealtad)

¿Está identificada y delimitada la finalidad de la recolección de estos datos? (principio de finalidad, de transparencia)

Esta finalidad, ¿incide en la cantidad de datos recolectada? ¿Existe un plazo determinado de conservación de los mismos? (principio de minimización, de conservación)

¿Considerarías que todos los datos recolectados, son necesarios (indispensables) para realizar las acciones autorizadas (o no) por el Titular de los datos, por parte de la empresa? (principio de minimización)

¿Se utilizan esos datos para otros propósitos que no sean los fines originales (fines de archivo, estudios científicos, otros) (principio de lealtad, finalidad)

¿Se difunden, comparten o publican los datos recolectados, más allá de los fines originales de la recolección? (principio de lealtad, finalidad)

¿Se actualizan estos datos? ¿Cómo? (principio de exactitud)

¿Se modifican estos datos en caso de ser erróneos? ¿Cómo? (se rectifican, suprimen) (principio de exactitud)

¿Se eliminan estos datos en algún momento? ¿Luego de cierto tiempo? ¿Con qué razones?; en caso de que no se eliminen, ¿por qué? (principio de conservación)

¿Existen normativas, protocolos de uso y manejo de las bases de datos dentro de la empresa? (principio de seguridad)

¿Qué riesgos a la seguridad de las bases de datos identifica? (jurídicos, tecnológicos, humanos) (principio de seguridad)

¿Recuerdas algún incidente en el que se haya visto 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?

¿Existe algún tipo de transferencia de datos personales por parte de la empresa? En ese caso, ¿Las transferencias son nacionales y/o internacionales?

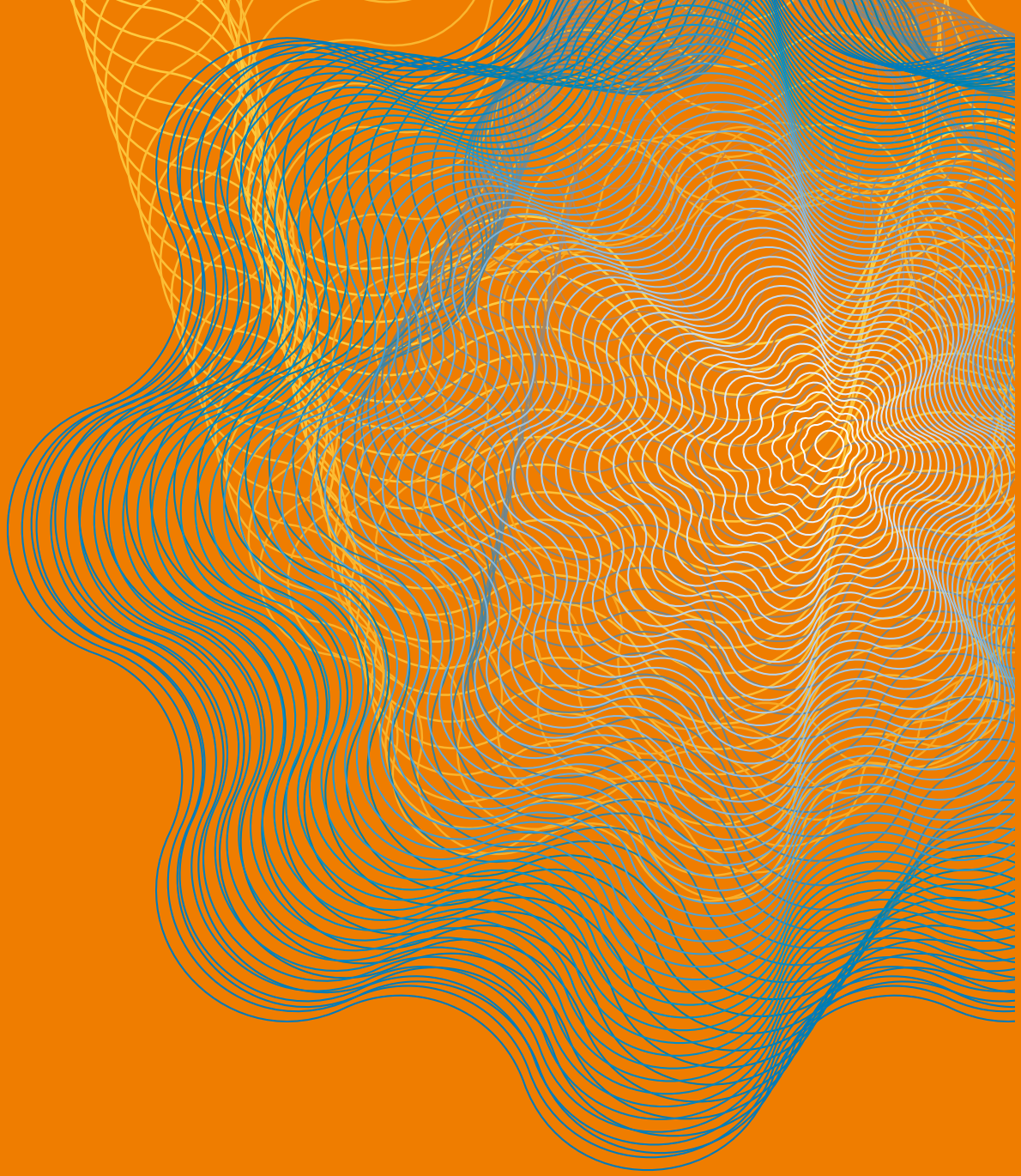
¿Existe un área específica dentro de la empresa encargada del tratamiento de datos personales, que centralice las gestiones relativas a estos?

C. Futura entrada en vigencia y aplicación de la Ley de Protección de Datos Personales

Teniendo en cuenta las preguntas anteriores, que refieren a los Principios de Protección de Datos Personales que estarían establecidos en el proyecto de Ley, ¿cómo considerás que les resultaría la entrada en vigencia y aplicación de la ley?

¿Considerás que en un periodo de 24 meses podrán incorporar los ajustes necesarios, con [poco / medio / mucho] apoyo de parte de la Autoridad de Aplicación de la ley?

Cuál considerás que sería el mayor desafío para tu empresa o rubro, en la aplicación de la ley?



Tecnología
& Derechos
Humanos