UNIVERSIDAD DE LA REPÚBLICA

FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN

TRABAJO FINAL PARA OBTENER EL TÍTULO DE

ESPECIALIZACIÓN GESTIÓN FINANCIERA EN INSTITUCIONES PÚBLICAS

Ley N° 18.331 de Protección de Datos Personales de Uruguay: Análisis dogmático, evolución normativa y desafíos institucionales.

por

Cra. Constanza Durán

Cra. Mariana Laura López

Cra. Geraldinna Sayabedra

TUTOR: Dra. Natalia Veloso

COORDINADOR: Profa. Gabriela Pintos

Montevideo

URUGUAY

2024

Página de Aprobación

El tribunal docente integrado por los abajo firmantes aprueba el Trabajo Final:

Título

Ley N° 18.331 de Protección de Datos Personales de Uruguay: Análisis dogmático, evolución normativa y desafíos institucionales.

Autor/es

Cra. Constanza Durán

Cra. Mariana Laura López

Cra. Geraldinna Sayabedra

Tutor

Dra. Natalia Veloso

Posgrado

Gestión Financiera en Instituciones Públicas

Puntaje ……

Tribunal

Profesor…… (nombre y firma).

Profesor…… (nombre y firma).

Profesor…… (nombre y firma).

FECHA.....

AGRADECIMIENTOS

A lo largo de este camino de aprendizaje, son muchas las personas que han sido fundamentales para que este trabajo de investigación pueda realizarse.

En primer lugar debemos agradecer a nuestra tutora, Dra. Natalia Veloso por su guía, dedicación, compromiso y por compartir su experiencia que enriquecieron enormemente el desarrollo de esta investigación. Sin ella nada de esto hubiera sido posible.

No debemos dejar de agradecer también a nuestro entorno laboral, por brindarnos el espacio, colaboración, contención y la comprensión necesaria para poder equilibrar nuestras responsabilidades laborales con los requerimientos académicos de este proceso.

Agradecemos igualmente a nuestros familiares y amigos quienes han sido un sostén emocional y nos han brindado su respaldo incondicional a lo largo de este viaje.

Agradecer también al programa de posgrados, tanto a los profesores, como a todo el personal administrativo del Centro de Posgrados de la Facultad de Ciencias Económicas y Administración, por darnos la oportunidad de ser parte de esta formación académica de alto nivel, bajo un ambiente de aprendizaje estimulante y lleno de compromiso y esfuerzo. Así como también a todos nuestros compañeros de generación, quienes hicieron de este camino una experiencia aún más enriquecedora.

Por último, pero no menos importante, agradecer a cada uno de ustedes que se han interesado en nuestro trabajo y han dedicado su tiempo a leerlo.

RESUMEN

La protección de los datos personales se ha convertido en un reto jurídico y social preponderante a nivel global. Con el auge de las tecnologías de la información y las comunicaciones, nuestras interacciones han sufrido cambios significativos, elevando la privacidad a un derecho fundamental. En este marco, Uruguay ha tomado medidas significativas para proteger la información personal de sus ciudadanos.

A tales efectos, en el año 2008, Uruguay promulgó la Ley N° 18.331, donde se establece un marco legal para la protección de datos personales, reconociéndose el derecho a la protección de datos como inherente a cada persona, en consonancia con el artículo 72 de la Constitución de la República Oriental del Uruguay. Esta ley regula aspectos como la recolección, tratamiento, almacenamiento y la transferencia de datos, otorgando también derechos como el acceso, rectificación, inclusión y eliminación de la información personal a través de la acción de habeas data.

El presente trabajo tiene como propósito principal realizar un análisis dogmático de la ley, evaluando su evolución, aplicación e implementación en la sociedad uruguaya. Además, se revisarán las resoluciones más relevantes emitidas por la Unidad Reguladora y de Control de Datos Personales (entidad responsable de supervisar el cumplimiento de la normativa y asegurar la protección de los datos personales), así como el contexto histórico y las influencias internacionales que impulsaron la creación de esta legislación, destacando sus fortalezas y desafíos desde un enfoque normativo, institucional y comparado.

Palabras claves:

Ley N° 18.331, protección de datos personales, datos sensibles, tratamiento de datos, Unidad Reguladora y de Control de Datos Personales.

Tabla de contenido

ABREVIATURAS Y SIGLAS

ADN - Ácido desoxirribonucleico.

AGESIC - Agencia de Gobierno Electrónico y la Sociedad de la Información y del Conocimiento.

Derechos ARCO – Derecho de Acceso, Rectificación, Cancelación u Oposición.

CERTuy - Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay.

CI - Cédula de Identidad.

DNPI - Dirección Nacional de la Propiedad Industrial.

DPO – Delegado de Protección de Datos.

EEE - Espacio Económico Europeo.

EE.UU. – Estados Unidos.

LFPDPPP - Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México).

LGPD - Ley General de Protección Datos (Lei Geral de Proteção de Dados Pessoais) (Brasil).

LPDP - Ley de Protección de Datos Personales.

LGPDPPSO - Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (México).

LPVP – Ley Protección de la Vida Privada (Chile).

PDPA - Ley de Protección de Datos Personales Argentina (Argentina).

RGPD - Reglamento General de Protección de Datos de la Unión Europea.

STF - Supremo Tribunal Federal (Brasil).

TCA - Tribunal de lo Contencioso Administrativo.

UI – Unidad Indexada.

URCDP - Unidad Reguladora y de Control de Datos Personales.

UE – Unión Europea.

URSEC - Unidad Reguladora de Servicios de Comunicaciones.

VIH - Virus de Inmunodeficiencia Humana.

1. INTRODUCCIÓN

En la actualidad, la protección de datos personales se ha convertido en uno de los desafíos más importantes de las organizaciones y de la sociedad toda. El crecimiento exponencial de los últimos 20 años en lo que refiere a la generación, recopilación y procesamiento de información se identifican como aspectos claves y preocupantes de la cotidianidad de las sociedades. Este crecimiento se vio impulsado por un mundo cada vez más digitalizado, en donde la globalidad es el eje principal de las nuevas generaciones y tanto el consumo masivo como las redes sociales son la moneda corriente del día a día de la población. Todo esto a su vez viene acompañado de la existencia de constantes amenazas en los derechos de las personas, que van desde el uso no autorizado por terceros de información personal, ya sea para publicidad, marketing, negocios, entre otros, como filtraciones de datos o acceso no autorizado de la información personal por parte de organizaciones y particulares.

En esta era digital que estamos viviendo, la protección de los datos personales se ha convertido en un tema central tanto a nivel nacional como internacional. El constante avance tecnológico y el uso masivo de la información llevan a la necesidad de establecer normativas que regulen el tratamiento de los datos personales, garantizando los derechos fundamentales de las personas y promoviendo un uso responsable de la información almacenada por diferentes entidades.

Frente a esta situación, los organismos legisladores han puesto especial foco en implementar leyes, regulaciones y reglamentos, con el fin de promover y garantizar el derecho fundamental de la protección de datos de los individuos.

Es así que, el 11 de agosto de 2008, y envuelto en un contexto social y económico de crecimiento tecnológico, el Poder Legislativo de Uruguay promulga la Ley N° 18.331 de Protección de Datos Personales, estableciendo así, un marco normativo para la recolección, almacenamiento y tratamiento de datos personales, con el fin de asegurar a toda la población estándares mínimos en la privacidad de sus datos y garantizando el derecho inherente a la calidad del ser humano de ser protegido en el tratamiento de los datos personales.

Inspirada en estándares internacionales como ser el Reglamento General de Protección de Datos de la Unión Europea (RGPD), o en legislaciones de países regionales, como ser el caso de la República Argentina, Uruguay comenzó a recorrer el camino de la protección de datos, promulgando la citada ley y creando la Unidad Reguladora y de Control de Datos Personales (URCDP) como organismo regulador en la materia. Esta legislación busca equilibrar el derecho a la privacidad con el desarrollo tecnológico y la necesidad de acceso a la

información, estableciendo principios, obligaciones y mecanismos de control para las entidades que manejan datos personales.

Este análisis no sólo es relevante para comprender el alcance y efectividad de la normativa, sino que la importancia radica en la creciente necesidad de preservar la privacidad de todos nosotros, especialmente en la era digital en que estamos inmersos y de la que formamos parte cotidianamente, ya sea utilizando la última tecnología en inteligencia artificial o simplemente visualizando el estado del tiempo para el día siguiente en el celular. Los avances constantes y permanentes motivan la necesidad de evaluar si la normativa vigente en Uruguay responde adecuadamente a los desafíos actuales. Comprender cómo se aplica esta ley y cómo afecta a la población es clave para proponer mejoras y garantizar un equilibrio entre la innovación tecnológica y la protección de los derechos fundamentales.

1.1 OBJETIVOS DEL TRABAJO

1.1.1 Objetivo general

Este estudio tiene como objetivo realizar un análisis dogmático de la Ley N° 18.331 de Protección de Datos Personales en Uruguay, examinar su evolución y aplicación, con el fin de intentar comprender cómo fue adoptada en la sociedad uruguaya, así como comprender los estándares que propone para la correcta recolección, uso, resguardo y transferencia de información personal.

Este análisis permitirá dar una idea de la efectividad de la ley en la protección de derechos ciudadanos a través del análisis de diferentes dictámenes y resoluciones del tema a los que pudimos acceder, así como también establecer el ajuste de la legislatura uruguaya con los diferentes estándares internacionales que regulan este tema.

1.1.2 Objetivos específicos

- Describir el marco legal aplicable en Uruguay respecto a la protección de datos personales.
- Analizar la aplicación de la ley en la sociedad uruguaya, identificando su implementación en distintos ámbitos.
- Examinar el contexto histórico, nacional e internacional, que propulsó la creación de la ley.
- Analizar el rol que ejerce la URCDP en lo que respecta a la supervisión, regulación y aplicación de la normativa vigente.

- Realizar una comparación del marco normativo nacional con el contexto internacional y sus reglamentaciones.

1.2. FUNDAMENTACIÓN

El tratamiento de los datos personales es un tema central en la era digital. En este sentido Peschard Mariscal (2011, p.22) advierte:

> Las redes sociales en Internet han devenido herramientas de comunicación multifuncionales, que nos permiten entrar en contacto con personas de todo el mundo y compartir experiencias de muy variado tipo en esta nueva aldea global: permiten obtener, almacenar y transmitir un sin número de datos, documentos, fotografías, videos, música, -entre otros-, y el acceso a éstos es tan sencillo con simplemente un clic.[1]

El presente estudio es relevante dado el creciente uso de sistemas informáticos para gestionar la información de la sociedad, los cuales pueden ser vulnerados, violentando un derecho inherente a la persona como es la protección de datos personales, por lo que es responsabilidad de cada organismo, empresa o el Estado velar por la correcta protección y uso adecuado de la información que se mantiene. Existe una relación directamente proporcional entre el aumento de datos manejados por las organizaciones y la aparición de nuevos y complejos desafíos en cuanto a seguridad, confidencialidad y disponibilidad de datos, siendo éstos los pilares principales para garantizar la privacidad, los derechos y las libertades de los individuos. Como plantea Chantal Bernier (2011, p.16):

> El reconocimiento a las dimensiones internacionales de la protección de los datos personales en la era digital, la importancia de los desafíos a la protección de los datos personales de los más jóvenes en internet y la urgencia de elaborar marcos normativos que puedan orientar a los Estados y a las empresas en sus esfuerzos para responder a esos desafíos, es, hoy en día, objeto de múltiples debates, conferencias y seminarios en todo el mundo.[2]

Sin dudas Uruguay no se ve exento del contexto global, donde las nuevas tecnologías juegan un rol cada vez más importante y los datos personales son el recurso más valioso y sensible en el mercado, donde es imprescindible contar con un marco normativo claro, que establezca principios, obligaciones y mecanismos de control para la protección de datos personales. Por este motivo, en el año 2008 y siendo de los primeros países de Latinoamérica en tomar consciencia de la necesidad de acción en el tema (el primero fue Argentina en los años 2000) el Estado Uruguayo promulga la Ley N° 18.331 de Protección de Datos Personales, la cual junto con su normativa complementaria, regulan el tratamiento de la información personal, con

el objetivo de resguardar la privacidad y los derechos de los uruguayos. Esta ley no sólo impone obligaciones a quienes procesan datos, sino que también otorga derechos a los ciudadanos para el control de su información, brindándoles la posibilidad de rectificar, actualizar, incluir o suprimir sus datos.

1.3. ALCANCE

El alcance de este trabajo se centra en el análisis de la Ley N° 18.331 de Protección de Datos Personales en Uruguay, considerando aspectos desde su promulgación hasta la actualidad, haciendo especial énfasis en su evolución, aplicación y las repercusiones acontecidas por la entrada en vigor de la normativa en el contexto nacional, en el entendido de que éste último ítem se abordará con el análisis empírico de resoluciones, sentencias y decretos expedidos por la jurisprudencia uruguaya correspondiente.

Se incluirá un análisis del marco histórico y legal que engloba la legislación, incluyendo un análisis exhaustivo de los artículos clave de la ley, los principios que la rigen y el rol de la URCDP en su función de asesor, regulador y supervisor del cumplimiento adecuado de la ley.

Se efectuarán comparaciones con legislaciones internacionales, para realizar un análisis del entorno global y como Uruguay se posiciona entre los países de la región con respecto a la materia.

Se pone en manifiesto que este estudio no abordará aspectos técnicos de ciberseguridad ni el desarrollo específico de infraestructuras tecnológicas para el almacenamiento o resguardo de información, sino que se centrará únicamente en el análisis normativo y su aplicación.

1.4. METODOLOGÍA DE TRABAJO

El presente trabajo se llevará a cabo basándose en un enfoque cualitativo y descriptivo, enfocado en un análisis dogmático de la normativa vigente respecto a los datos personales en Uruguay. La metodología se centra en el análisis de los textos normativos vigentes y su significado, acompañado de un análisis empírico, que tomará en cuenta la aplicación de esa normativa a la sociedad uruguaya.

Se utilizarán como fuentes de información la legislación nacional vigente, documentos oficiales relacionados con la protección de datos personales, jurisprudencia, normativas internacionales, estudios previos sobre la materia, textos públicos de autores referentes y resoluciones de los órganos de control.

La metodología utilizada incluirá una revisión documental y normativa, con el cometido de evaluar la documentación legal existente en el orden jurídico uruguayo que respalda la normativa vigente.

2. MARCO LEGAL Y NORMATIVO

En un mundo donde la información personal se ha convertido en un activo de alto valor, la regulación sobre su tratamiento y protección se ha vuelto un pilar fundamental para garantizar los derechos de los ciudadanos. Uruguay ha sido pionero en América Latina en el desarrollo de un marco legal sólido en materia de protección de datos personales, estableciendo estándares que han sido reconocidos a nivel internacional.

Con el objetivo de proteger el derecho inherente de identificación, la legislación uruguaya ha presentado particular interés en promulgar leyes y decretos, enfocados en proteger la intimidad y los derechos de los ciudadanos del uso indebido o incorrecto, que se pueden llegar a realizar con nuestros datos. Es así como en 2008 se promulgó la Ley N° 18.331, denominada “Ley de Protección de Datos Personales” (LPDP), marcando un antes y un después en la regulación de la información personal en el país. Esta normativa establece los principios fundamentales para el tratamiento de datos personales, con el objetivo de garantizar el derecho a la privacidad de los ciudadanos.

2.1 DECRETOS Y ACTUALIZACIONES A LA LEY

Con el compromiso del Estado uruguayo de mantener un marco legal robusto y actualizado, la legislatura ha modificado e introducido artículos y reglamentaciones a lo largo de los años en la materia. Tal como especifica Augusto Durán Martínez (2011), “la ley siguió aquí las más modernas tendencias que se han impuesto en el mundo”[3] para poder posicionarse en la materia.

La Ley N° 18.331 se encuentra regulada por el Decreto N° 414/009 de 31 de agosto de 2009, en donde entre otras cosas se establecen disposiciones específicas para la aplicación de ésta. Entre las disposiciones más trascendentes se presentan:

- Ámbito de aplicación territorial: la ley será aplicada cuando el responsable de la base de datos o el tratamiento de los datos esté establecido en territorio uruguayo o utilice medios situados en el país para el tratamiento de datos, salvo que dichos medios se utilicen exclusivamente con fines de tránsito.

- Consentimiento del titular: especificando que se requiere el consentimiento expreso del titular de los datos para su tratamiento, los cuales pueden ser obtenidos a través de distintos medios.

- Principio de finalidad: los datos personales deben ser utilizados únicamente para las finalidades específicas para las cuales fueron recolectados y deben ser eliminados cuando dejen de ser necesarios.

El derecho a la protección de datos personales es reconocido en varios instrumentos internacionales, como ser, el artículo 8° de la Carta de los Derechos Fundamentales de la Unión Europea y el “Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su protocolo adicional". Este Convenio del año 1981 sirvió de instrumento para que en 2013 Uruguay se posicione como el primer país no europeo en adherirse al Convenio y su Protocolo Adicional, mediante la Ley N° 19.030 de 27 de diciembre de 2012. Este tratado internacional, actualizado en 2018 y conocido como 108+ (único instrumento vinculante internacional en la materia), que actualmente está integrado por más de 50 países en todo el mundo, fue ratificado por Uruguay en 2021 ante la Secretaría General del Consejo de Europa tras presentarse la aprobación en el Parlamento Nacional por la Ley N° 19.948 de 16 de abril de 2021, reforzando el compromiso del país con la protección de datos personales a nivel internacional y posicionándose como el primer país de América Latina en ratificar el protocolo.

La ley sufrió una modificación en sus artículos 14°, 15°, 16° y 17°, referidos a los derechos que le otorga la LPDP a los individuos. Dicha modificación fue dada por la Ley N° 18.719 de 27 de diciembre de 2010, en la que se modifican algunos incisos de los artículos anteriormente comentados, dándole una mejor interpretación a los artículos originales y brindándoles de un mayor peso y relevancia para la sociedad.

Del mismo modo, la Ley N° 18.331 presentó una actualización bajo la Ley N° 19.670 de 15 de octubre de 2018, en donde se modificaron algunos artículos como ser la sustitución del artículo 12 original, en el cual se reforzó el principio de responsabilidad, estableciendo que tanto el responsable como el encargado de la base de datos presentan responsabilidad en el caso de alguna violación a las disposiciones de la ley. En esta actualización se introduce el principio de responsabilidad, deberes de confidencialidad y se ampliaron las facultades de la URCDP. La Ley N° 19.670 fue reglamentada por el Decreto N° 64/020 de 17 de febrero de 2020, el cual regula los artículos 37 a 40, estableciendo nuevas implicancias y ajustando los procedimientos de denuncias y sanciones. Estos cambios significan la inclusión de cuatro artículos que llevan consigo importantes modificaciones a la norma de protección de datos personales en Uruguay, éstos son:

- **Aplicación del ámbito de aplicación de la ley de datos personales:** anteriormente se aplicaba la ley solamente al tratamiento de datos cuando el responsable o encargado de la base de datos estuviera establecido y operara dentro del territorio uruguayo, o si la infraestructura estuviera ubicada dentro de nuestro país. Con este cambio, el alcance se extiende incluso fuera de las fronteras nacionales cuando los datos estén vinculados a servicios o bienes dirigidos a residentes uruguayos.
- **Nuevas obligaciones para responsables y encargados de bases de datos:** con esta nueva normativa el responsable de datos en caso de detectar una vulneración de seguridad deberá notificar la situación de inmediato, junto con todas aquellas medidas que hayan sido implementadas para subsanar el inconveniente y reducir el impacto del mismo. La vulneración deberá ser comunicada tanto al titular de los datos como a la URCDP, quien será el encargado de comunicarse con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy) para coordinar los pasos siguientes (Anexo 1).
- **Modificaciones al "principio de responsabilidad":** la redacción original de este principio se encontraba dada por el artículo 12 de la ley, sin embargo con la modificación en el artículo 39 de la Ley N° 19.670 se estableció que tanto el responsable como el encargado de una base de datos, serán solidariamente responsables en caso de incumplimiento en disposiciones legales. Agregando también que se exigen medidas técnicas y organizativas para garantizar la seguridad de la información de los datos.
- **Creación de la figura del "delegado de protección de datos":** Mediante esta nueva ley surge la figura del "delegado de protección de datos" y se dispone que tanto entidades públicas como privadas deberán contar con tal figura. Tendrá la responsabilidad de asesorar en la creación, implementación y ejecución de políticas de protección de datos, supervisar el buen cumplimiento conforme a la normativa vigente e impulsar medidas para alinearse con la legislación nacional y los estándares internacionales.

Mediante el Decreto N° 64/020 se derogan los artículos 7° y 8° del Decreto N° 414/009, los cuales presentaban las implicancias de las medidas de seguridad de las bases de datos y las vulneraciones de seguridad que se podían presentar.

En la Ley N° 19.924 de 18 de diciembre de 2020 - Presupuesto Nacional en su artículo 3° y 86° se incluyeron y regularon los datos biométricos, agregando el literal Ñ al artículo 4° en donde especifica cómo será su tratamiento.

Finalmente, con la Ley N° 20.075 de 20 de octubre de 2022 se ampliaron las obligaciones de los responsables y encargados del tratamiento de datos personales, especialmente en lo que refiere al derecho de información y regulación del tratamiento automatizado de los datos. Estas reformas permiten posicionar a Uruguay como un país con regulación avanzada en materia de protección de datos, alineándose con los estándares internacionales, por ejemplo, del Convenio 108 del Consejo de Europa.

Los principales cambios en el artículo 13° fueron: ampliación del derecho de información, incluyendo la notificación sobre el derecho de actualización de datos y el derecho a impugnar valoración de personas automatizadas. Se establece que deberán ser comunicadas la existencia de transferencias internacionales, y se exige informar previamente sobre los criterios y procedimientos de evaluación cuando un tratamiento automatizado pueda afectar significativamente al titular.

Para complementar con la legislación, la URCDP ha dictado resoluciones de modo complementarias en la materia, con el espíritu de tratar temas que tal vez no fueron directamente plasmados en la legislatura. Es así que por ejemplo en la Resolución N° 23/021 de 08 de junio de 2021 y la Resolución N° 41/021 de 08 de setiembre de 2021, en donde se trata el tema de países u organizaciones consideradas adecuadas para transferencias internacionales de datos, y aquellos territorios no adecuados. En el Dictamen N° 1/014 de 04 de febrero de 2014 de la URCDP se estableció que se consideran como públicas o accesibles al público, las fuentes o documentos, conforme a las modificaciones introducidas por la Ley N° 18.996 de 07 de noviembre de 2012 en su artículo 9 bis.

Existen otros casos en los que se modifica algún artículo en específico, pero se dejará constancia a lo largo del análisis.

3. CONTEXTO NACIONAL E INTERNACIONAL

3.1 ORIGEN Y DESARROLLO DEL DERECHO A LA PROTECCIÓN DE DATOS

El derecho a la protección de datos personales tiene raíces históricas profundas que se originan en la Constitución de Weimar de 1919, la cual fue la primera constitución democrática de Alemania tras la caída del Imperio Alemán, en donde a través de su artículo 129 se reconocía, por primera vez en la historia, el derecho de los funcionarios públicos a acceder y corregir su expediente personal. Esta referencia inicial estableció un precedente en el reconocimiento de la necesidad de que los individuos controlen la información registrada sobre ellos (González Fuster, 2014)[4].

Con el paso del tiempo y junto con la expansión del procesamiento automatizado de datos, en la segunda mitad del siglo XX surgen las primeras leyes específicas en la materia. La pionera fue la ley de protección de datos del estado de Hesse, Alemania, en 1970, cuyo objetivo fue garantizar que los datos de individuos que fueran procesados no fueran violados de su derecho a la autodeterminación informativa de la ley alemana. Más tarde, en 1977, Alemania aprobó "Ley Federal de Protección de Datos", consolidando estos principios a nivel nacional y regulando la protección de datos y la privacidad en el territorio alemán, esta ley ha sido actualizada para adaptarse al RGPD y se encuentra en vigencia actualmente.

Así como el derecho a la intimidad se encuentra vinculado a la creación pretoriana de los tribunales de los Estados Unidos de América (EE.UU.), la doctrina y la jurisprudencia germanas han elaborado el concepto del "derecho a la autodeterminación informática" (Masciotra, 2019)[5]. El derecho a la intimidad ha sido definido por Matilde Zavala (1982) como "un derecho que protege la reserva espiritual de la vida privada del hombre, asegurando su libre desenvolvimiento en lo personal, en sus expresiones y en sus afectos"[6].

Lo que se conoce como "autodeterminación informativa", clave en la doctrina alemana, fue un término consagrado por el Tribunal Constitucional Federal en su célebre sentencia de 1983 sobre el Censo Federal en la que se afirmó que el control sobre la propia información constituye un derecho fundamental. En la actualidad, este concepto se asemeja a lo que hoy denominamos habeas data.

A nivel europeo, el derecho a la protección de datos se consolidó formalmente con la entrada en vigor de la Carta de Derechos Fundamentales de la Unión Europea en el año 2000, en ella se recogen todos los derechos civiles, políticos, jurídicos, sociales y económicos de los habitantes. En su artículo 8 se reconoció expresamente y separado del derecho a la privacidad (artículo 7) el derecho de la protección de datos personales. Esta Carta, junto con otras normativas, como ser el Convenio 108 del Consejo de Europa (1981), y la Directiva 95/46/CE de 24 de octubre de 1995, que durante años fue la principal norma europea en la materia, fueron los cimientos para la construcción de la normativa internacional posterior.

En materia de protección de datos personales, 2015 puede ser recordado como el año en el que se produjo un momento álgido en el escenario internacional, particularmente entre la Unión Europea y los EE.UU., lo que puntualiza la necesidad de contar con estándares comunes de protección entre países (Maqueo, Moreno, & Recio, 2016)[7].

La "revolución normativa" llegó en 2016 con la aprobación del RGPD o Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, el cual en sus artículos intentó modernizar y unificar la legislación europea existente. Entre sus principales cometidos se encuentran:

- El principio de “responsabilidad proactiva” o *accountability.*
- El alcance extraterritorial de la norma, en el cual se declara que el reglamento será aplicable incluso a empresas situadas fuera de la Unión Europa que tratasen datos de ciudadanos europeos.
- Se introducen nuevos derechos y conceptos, como ser el derecho al olvido y el derecho a la portabilidad de datos (Voigt & von dem Bussche, 2017)[8].
- Impulsó la obligación de designar Delegados de Protección de Datos (DPO) en algunas organizaciones
- Exigió más reglamentaciones conforme al consentimiento informado y la transparencia en el tratamiento de datos personales.

El modelo europeo ejerció una influencia significativa en América Latina, además de Uruguay, Argentina, Brasil y México impulsaron reformas inspiradas en los principios del RGPD, aunque adaptadas a sus contextos locales (URCDP, 2020)[9].

Brasil, por su parte, aprobó en 2018 la *Lei Geral de Proteção de Dados Pessoais* (LGPD, Ley Nº 13.709), siguiendo en gran medida los lineamientos del RGPD europeo, aunque con particularidades propias como un enfoque más sectorizado y gradual en su implementación.

Otros países, como México, Chile y Panamá, también avanzaron en sus reformas, mostrando un claro proceso de "europeización" de las normas de privacidad en la región, aunque ninguno implementó el RGPD de forma textual.

3.2 CONTEXTO EN URUGUAY

3.2.1 Avance en la digitalización

A comienzos de la década de los 2000, Uruguay se vio envuelto en un proceso de digitalización, promovido tanto por proyectos públicos como privados y por un entorno global que lo favorecía. El acceso y facilidad a Internet, junto con el aumento de los comercios electrónicos, promovieron la creación de bases de datos más avanzadas en distintos sectores.

La aparición de programas como "Ceibal" en 2007, fomentados por el gobierno en su intento de modernización, también aumentó la familiaridad de la población con las tecnologías digitales, brindando un acceso más asequible de la tecnología e incrementando en consecuencia los volúmenes de datos personales generados y almacenados.

3.2.2 Crisis económica

La crisis económica de principios de los 2000 en la que se vio envuelta la sociedad del Río de la Plata, originada principalmente por la caída financiera en Argentina, impactó de manera adversa en Uruguay y en su sociedad, especialmente en lo que respecta a confianza con las

instituciones bancarias y financieras. Como observa Baridon (2009), “la desconfianza ciudadana no solo afectó al sistema económico, sino que también generó una mayor preocupación sobre la protección de la información personal, particularmente los datos financieros sensibles”[10].

Este panorama de inseguridad y desconfianza resaltó la ausencia de una normativa apropiada y específica para la gestión de datos personales, impulsando prácticas de uso indebido o no autorizado de bases de datos y los datos que pertenezcan a ellas.

3.2.3 Gobierno Electrónico

Uruguay, desde principios de la segunda mitad del siglo XXI, apostó al desarrollo del gobierno electrónico a través de la estrategia de “e-Gobierno”, proceso que comenzó por la creación de la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC), quien lideró el desarrollo de las nuevas estrategias. Si bien esta modernización trajo numerosos beneficios en términos de eficiencia y acceso a los servicios públicos, también planteó nuevos desafíos respecto a la protección de los datos ciudadanos.

Se hizo evidente la necesidad de establecer un marco normativo que garantizara no solo la operatividad de los sistemas electrónicos, sino también la privacidad y seguridad de la información recabada por el Estado.

3.2.4 Influencia de normativas Internacionales

Con la Directiva 95/46/CE de 24 de octubre de 1995 de la Unión Europea como referencia, Uruguay buscó alinear su legislación a los estándares internacionales, con el objetivo de obtener el reconocimiento de “país adecuado” por parte de la UE, que le permitiría facilitar las transferencias internacionales de datos, aspecto que se presenta como eje principal en la expansión del comercio y los servicios digitales.

De hecho, en 2012, Uruguay fue reconocido oficialmente por la Comisión Europea como un país con un nivel de protección de datos personales adecuado, siendo uno de los primeros en la región.

3.2.5 Incidentes relacionados con el uso indebido de datos personales

Antes de la promulgación de la Ley N.º 18.331, los casos de uso indebido de datos personales eran bastante frecuentes en la sociedad. Según Tosi Zás (2010), prácticas como la venta de bases de datos, el envío de correos electrónicos no solicitados y la utilización de información sin consentimiento eran moneda corriente, en parte debido a la falta de regulación específica y de conciencia pública sobre los derechos asociados a la privacidad[11].

Estas situaciones pusieron en evidencia la urgencia de contar con un marco jurídico sólido que protegiera efectivamente los derechos de los titulares de los datos.

4. CONCEPTO Y CARACTERÍSTICAS

En Uruguay, se entiende que el derecho a la protección de los datos personales es un derecho fundamental inherente a la persona humana y por tanto, incluido en el artículo 72 de la Constitución de la República. Desde la base constitucional, y con el fin de reglamentar este derecho humano irrevocable, el poder legislativo promulgó la Ley N° 18.331, en donde se especifican cuáles son los tipos de datos que se considerarán personales, se declaran los derechos y obligaciones ante los mismos, el ámbito de aplicación de las regulaciones y los lineamientos para su tratamiento dentro de la sociedad uruguaya. Con la aprobación de la ley el Estado uruguayo buscó equilibrar el avance tecnológico y la necesidad de preservar la privacidad y autonomía de los individuos, en el entendido de que ésta información reviste un alto nivel de sensibilidad y viene acompañada de potenciales problemas por su mala utilización.

Para comprender qué implica la protección de datos personales, primero es necesario definir qué se entiende por dato personal. En este sentido, en el artículo 4° de la Ley N° 18.331 se define como: “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables”. En otras palabras, dato personal refiere a toda aquella información (numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo) relacionada a personas físicas o jurídicas. José Luis Piñar Mañas (2004) agrega que “el derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales”[12]. Como ejemplos encontramos nombre o apellido (datos que individualizan a la persona e identifica a las familias de origen), dirección física, Número de Cédula de Identidad (CI) o número de pasaporte, huella digital e incluso queda considerado dentro de esta categoría el Ácido desoxirribonucleico (ADN).

El concepto de dato personal se encuentra directamente relacionado con el avance de las nuevas tecnologías, la digitalización de la información y el progreso de los derechos humanos con respecto a la privacidad. La noción de dato personal fue tomando un papel relevante en el mundo a medida que gobiernos y empresas comenzaron a recopilar cada vez más información sobre las personas con distintos fines, ya sean administrativos o comerciales. Sin embargo, no fue hasta mediados del siglo XX cuando comenzaron las primeras inquietudes con respecto a la necesidad de que dichos datos tuvieran un mínimo grado de seguridad con el fin de preservar la privacidad de las personas. Antonio Pérez Luño (2006) plantea que la era digital “ha contribuido a redimensionar la nueva imagen del hombre en cuanto sujeto de

derechos. Las nuevas condiciones de ejercicio de los derechos humanos han determinado una nueva forma de ser ciudadano en el Estado de derecho de las sociedades tecnológicas"[13].

Las primeras regulaciones a los datos personales surgen en la década del 70' en distintos países de Europa, donde se promulgaron leyes relacionadas a esta temática, y plantearon los pilares que luego se utilizarían en el resto de países del mundo con respecto a la materia y la privacidad. Una década después, el 28 de enero de 1981 (fecha que actualmente se conmemora el día mundial de la protección de datos personales), se firma el Convenio 108 del Consejo de Europa, siendo el primer instrumento de carácter multinacional y jurídicamente vinculante relativo a la protección de datos personales. Fuente: Parlamento Europeo.

5. ÁMBITO DE APLICACIÓN DE LA LEY

La ley establece en sus primeros artículos los criterios que determinan su aplicabilidad en el territorio, definiendo el alcance de la normativa en función del tipo de tratamiento de datos, los sujetos involucrados y el ámbito territorial para su ejecución.

El ámbito de aplicación de la ley se encuentra dado por el artículo 2° y se especifica que lo allí redactado se extiende a todos los habitantes de la República Oriental del Uruguay por ser un derecho humano considerado inherente a la persona, y a todas las bases de datos ubicadas en el territorio uruguayo, incluyendo también aquellos responsables que operen fuera de Uruguay y que procesen datos de uruguayos.
También por el artículo 2° se especifica que no solo será aplicable a personas físicas sino que aplicará por extensión a las personas jurídicas en lo que corresponda y con un análisis de cada caso. En ambos casos según el artículo 1° del Decreto 414/009 se aplica "directa o indirectamente, a través de cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiera a ellas".

Territorialmente el Decreto N° 414/009 reglamentó en su artículo 3° que la ley aplicará para todo tratamiento realizado en la República Oriental del Uruguay. Para radicados en el exterior se aplica si las actividades de tratamiento están relacionadas con oferta de bienes o servicios dirigidos a habitantes de Uruguay, si en el tratamiento se utilizan medios situados en Uruguay o si el contrato así lo dispone.

5.1 APLICACIÓN OBJETIVA

El artículo 3 se establece que la ley aplicará a cualquier tipo de tratamiento de datos personales, tanto del sector público como privado, independientemente de la tecnología y forma en la que se haya obtenido la información, incluyendo toda modalidad de uso posterior, como puede ser la recolección, almacenamiento, transferencia o cualquier otro tipo de

operación que se realice con respecto a los datos personales. Esto implica que se tomarán del mismo modo tanto los registros físicos en papel, como los sistemas más avanzados en términos tecnológicos.

Existen excepciones establecidos en la ley donde no se aplica el régimen, estos están establecidos en el artículo 3° inciso 2 de la ley y en el artículo 2° de del Decreto N° 414/009 de y son:

A) Bases de datos mantenidas por personas en el ejercicio de actividades exclusivamente personales o domésticas, como por ejemplo las agendas personales.

B) Bases de datos con finalidad de la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

C) Bases de datos creadas y reguladas por leyes especiales.

6. LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES

La normativa uruguaya recoge en un conjunto de principios generales que rigen la protección de datos personales. Estos principios determinan la forma, contenido y condiciones para el tratamiento de los datos, garantizando su legalidad, transparencia y seguridad. En particular, se establecen los responsables, encargados y titulares de cumplir las obligaciones impuestas, quienes facilitan el ejercicio de los derechos; y también orientan a la URCDP en como de valorar los comportamientos en el cumplimiento de las disposiciones legales y reglamentarias. Los principios están detallados en el artículo 5°, y se especifican en los artículos 6° a 12° de la Ley N° 18.831.

6.1 LEGALIDAD

El principio de legalidad, definido en el artículo 6°, establece que las bases de datos en las que se incluyan datos personales, así como todos los datos que sean recopilados, almacenados y que fueran a tener un tratamiento posterior serán de carácter legítimo si dichas bases se encuentran debidamente inscriptas en el registro oficial, y cumplen con las disposiciones de la ley y los reglamentos que se dicten al respecto.
Así mismo, en el segundo inciso del artículo 6°, se prohíbe expresamente la creación y mantenimiento de bases de datos que tengan propósitos ilícitos, es decir, que tengan como objetivo la violación de derechos humanos o acciones contrarias a la ley o moral pública.

Será obligatorio registrar todas las bases de datos que almacenen información de carácter personal, sin importar si se encuentran gestionadas en soportes digitales (servidores digital o nube), manuales (papel físico) o mixtas. La obligación recae siempre que los datos que allí se

presenten permitan identificar o hacer identificables a las personas, como por ejemplo, las bases de datos de videovigilancia de organizaciones públicas o privadas. A modo de ejemplo, se comentan a continuación algunos casos.

Dictamen N° 5/019 de 23 de abril de 2019 de la URCDP: A modo ilustrativo encontramos la consulta planteada por la Unidad Reguladora de Servicios de Comunicaciones (URSEC) que refiere a la legalidad de que un operador de televisión para abonados instale cámaras en la vía pública y transmita en vivo las 24 horas a través de su canal local. Considerando que la colocación de cámaras por particulares en la vía pública tiene los límites establecidos por la LPDP, específicamente la actuación de los responsables de las bases de datos debe ajustarse a los principios de su art. 5° (Legalidad, Veracidad, Finalidad, Previo consentimiento informado, Seguridad de los datos, Reserva y Responsabilidad), y en particular a lo dispuesto en los arts. 6º y 7º. El Consejo Ejecutivo de la URCDP dictamina que la colocación de cámaras en la vía pública solo resulta legítima si se da cumplimiento a los principios rectores en materia de protección de datos personales. Con especial énfasis en que si las cámaras están orientadas a lugares privados y permiten la identificación de las personas, deberá obtenerse su consentimiento previo, expreso e informado e inscribirse la base de datos, además de cumplir el resto de las obligaciones referidas en la Ley Nº 18.331.

Resolución N° 32/024 de 10 de setiembre de 2024 de la URCDP: El caso refiere a una denuncia entre particulares, donde se detalla que la denunciada dio aviso que iba a colocar una cámara de video vigilancia en el complejo habitacional donde vive. La denunciante manifestó que en tanto no violara su privacidad podía proceder a la instalación. Resultando que se instaló la cámara enfocando a la entrada del block de viviendas, violando no solo la privacidad de la denunciante sino la de todas las personas que allí residen, recalcando además que la cámara graba imágenes y voz. Como primera medida la URCDP notificó en diferentes ocasiones a la denunciada, requiriéndole el cumplimiento de diversas medidas contempladas en la normativa vigente y haciendo hincapié en la Resolución N° 58/021 de 21 de diciembre de 2021 de dicha unidad, pero no recibió respuesta. Teniendo en consideración la falta de colaboración de la denunciada ante la URCDP siendo esto una conducta pasible de sanción según lo previsto en el artículo 34° de la Ley N° 18.331 y que omitió el cumplimiento de obligaciones formales previstas en el artículo 6°. Como resultado la URCDP resolvió sancionar a la denunciada con apercibimiento por incumplir lo dispuesto en el artículo 34 de la Ley N° 18.331 e intimarla a que realice la inscripción de la base de datos de video vigilancia como lo establece el art. 6° de la LPDP y el cumplimiento de todas las medidas indicadas en la Resolución N° 58/021, en un plazo de 15 días hábiles o proceder a el retiro de la cámara correspondiente.

6.2 VERACIDAD

El principio de veracidad se encuentra definido en el artículo 7° de la ley y tiene como trasfondo garantizar la exactitud, integridad y actualización de toda aquella información que es recopilada. En este sentido la ley específica que los datos personales que se recaben para su tratamiento deben ser veraces, adecuados, ecuánimes, exactos, no deben ser excesivos con respecto a la finalidad para la que se obtuvieron, haciendo especial hincapié en que ésta regulación no aplica solamente al momento de su recolección, sino que también deben ser actualizados, corregirlos, complementarlos, sustituirlos e incluso suprimirlos cuando sea necesario, para evitar información errónea o desactualizada en relación a los individuos. Este principio tiene intrínseco que los datos reflejen la realidad de sus titulares, protegiendo sus derechos, y evitando que información incorrecta, incompleta, falsa o engañosa, pueda afectar a los individuos y su privacidad.

Este principio agrega también que los datos no pueden obtenerse por medios fraudulentos, desleales, abusivos, extorsivos o de forma contraria a las disposiciones de la normativa. Y si así sucediera, esta información no podría utilizarse conforme a la normativa y de modo lícito.

Finalmente, el artículo 7° establece que los datos personales deben ser eliminados cuando hayan caducado su propósito por el cual fueron recolectados de acuerdo con lo previsto en la ley. Este inciso apunta a reducir riesgos de malversación, uso indebido o no autorizado de la información de terceros.

Dictamen N°4/021 de 23 de marzo de 2021 de la URCDP: Este dictamen responde a una consulta realizada por la Dirección Nacional de la Propiedad Industrial (DNPI) ante la URCDP sobre la posibilidad de que terceros accedan a datos de su registro para servicios de algoritmos de búsqueda. La URCDP señala que, aunque la DNPI puede contratar estos servicios, debe garantizar que los datos proporcionados sean veraces y se utilicen conforme a la finalidad para la cual fueron recolectados, respetando el principio de veracidad establecido en el artículo N° 7 de la Ley N° 18.331. Y en el caso que dicho tercero conserve esa información con una finalidad distinta a la que impulsó su recolección, deberá notificar a los titulares de los datos de lo acontecido, y como consecuencia dicho tercero adquirirá el carácter de responsable del tratamiento de los datos personales, debiendo dar cumplimiento con todas las obligaciones previstas en la Ley N° 18.331, por no aplicarse la excepción prevista en el artículo 3° de la antedicha ley.

6.3 FINALIDAD

De este principio, detallado en el artículo 8° de la ley, se extrae que los datos personales deben ser recopilados con un propósito específico, legítimo y determinado con anterioridad a

su recolección. El objetivo final que motiva la recolección de los datos personales debe tener como punto de partida un destino predefinido con anterioridad a su recolección y su utilización no puede ser otra que no sea éste.
En caso de que la finalidad sea distinta o incompatible con los fundamentos para su obtención, el responsable de los datos debe recabar el consentimiento explícito del individuo dueño de los datos, sin este consentimiento no pueden utilizarse.
Este principio busca preservar la privacidad y transparencia en el uso de datos personales, evitando su uso posterior incorrecto por parte de los recolectores de información y generando la obligación a éstos de comunicar eficaz y oportunamente la necesidad de almacenar los datos solicitados.

Al igual que en el artículo anterior, el principio de finalidad establece que no pueden ser utilizados los datos recolectados una vez que hayan dejado de ser necesarios para los cuales fueron obtenidos, indicando que deben ser eliminados en estos casos. Sin embargo, en el segundo inciso del artículo 8°, la legislación específica casos en los que aunque se haya finalizado la necesidad o pertinencia del manejo de datos, éstos pueden seguir siendo utilizados, en el entendido que existen algunas casuísticas que deben ser consideradas como excepciones, las cuales serán establecidas por la ley. Estas excepciones plantean que ciertos datos pueden ser conservados por su valor histórico, estadístico o científico, siempre y cuando la obtención, uso y resguardo se realicen conforme a la legislación vigente y se haya autorizado la necesidad o pertinencia de este accionar.

Para finalizar, en el último inciso del artículo, se define que no podrán ser comunicados datos entre distintas bases, sin que se recabe el consentimiento informado del titular de los datos o que medie una ley que así lo disponga.

Dictamen N°12/021 de 29 de junio de 2021 de la URCDP: Este dictamen analiza el uso de la información contenida en la historia clínica laboral destacando que, según el principio de finalidad establecido en el artículo N° 8 de la Ley N° 18.331, la información contenida en estas historias debe utilizarse exclusivamente para controlar enfermedades que puedan afectar la relación laboral. Asimismo, se subraya que los datos personales no pueden emplearse para fines distintos o incompatibles con aquellos que motivaron su recolección y recalca la importancia de respetar la finalidad original para la cual se recopilan los datos personales, evitando su uso para propósitos no relacionados o incompatibles con dicha finalidad.

6.4 PREVIO CONSENTIMIENTO INFORMADO

Es un principio fundamental para la protección de datos personales, y es la base para preservar la privacidad y respetar los derechos de los individuos, se encuentra descripto en el

artículo 9° de la ley, en donde se explica que el consentimiento debe ser libre, expreso, documentado e informado por parte de los titulares de datos.

El responsable de la base de datos (o de su recolección) debe recabar de forma libre, previa a la recolección y de manera informada, el consentimiento de los titulares de datos sobre el motivo de la recolección de la información. El consentimiento debe ser explícito y de forma inequívoca, explicando la finalidad para la cual serán destinados los datos y el tipo de actividad en la cual se desarrolla el responsable de la base de datos, evitando dobles interpretaciones o vacíos legales. Si no se obtiene el consentimiento bajo estas características, se entiende que éste será nulo y no podrá utilizarse.

El artículo 6° del Decreto N° 414/009 especifica que los modos en los que se puede recabar los consentimientos varían según la necesidad y el tipo de datos, pero que se debe priorizar que los medios sean sencillos, claros y gratuitos, para garantizarle al titular de los datos opciones fáciles y accesibles para el consentimiento o no del tratamiento de sus datos. Pueden ser obtenidos mediante grabaciones, formularios, aceptación en sitios web, entre otros. Para los casos de sitios web Pablo Schiavi (2013) puntualiza que “el consentimiento que presta el usuario es válido en el momento en que decide aceptar la política de privacidad y condiciones de uso de la plataforma que constan en el formulario de registro” (p. 21)[14].

El artículo 6° continúa explicando que el consentimiento se entiende dado cuando se permita al titular la elección entre dos opciones claramente identificadas que no se encuentren pre marcadas a favor o en contra. La Ley N° 18.331 establece excepciones a este principio en su artículo 9°, indicando que no será necesario el previo consentimiento en los siguientes casos:

• Cuando los datos son tomados de fuentes públicas de información, como registros o publicaciones en medios de comunicación masiva. La Ley N° 18.331 define en forma taxativa las fuentes públicas de información en el artículo 9° bis.

• Cuando se usen para el ejercicio de funciones de los poderes del Estado o una obligación legal.

• Cuando se trate de listados cuyos datos se limiten a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento para personas físicas. Para personas jurídicas, razón social, nombre fantasía, domicilio, registro único de contribuyentes, teléfono e identidad de las personas a cargo de la misma.

• Cuando provienen de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

• Cuando se haga por una persona física con un fin exclusivo personal, individual o doméstico.

El responsable de la base de datos debe recabar y guardar la prueba del consentimiento, en cualquier medio. Se especifica que la prueba del resguardo de esta información puede ser requerida por la URCDP en cualquier momento y en cualquier circunstancia que así lo amerite. En Anexo 2 se agrega un ejemplo de formulario para recabar el consentimiento de un individuo.

Resolución N° 35/020 de 09 de junio de 2020 de la URCDP: Esta resolución aborda la implementación de sistemas de rastreo de contactos por intermedio de aplicaciones móviles en el contexto de la emergencia sanitaria por COVID-19. La URCDP pone de manifiesto que el monitoreo a gran escala de los contactos de las personas no posee una base legal que lo habilite, sino que se fundamenta en el consentimiento informado en forma previa y expresa de los titulares de los datos según lo establecido en el artículo 9° de la Ley N° 18.331, pudiendo ser recabado a través de medios electrónicos y a su vez prever la eventualidad de revocar su consentimiento para el uso del rastreo de contacto, aún sin tener que eliminar la aplicación. El tratamiento de dichos datos podrá llevarse a cabo únicamente durante el período de vigencia de la emergencia sanitaria, en el contexto de una política de mitigación de la pandemia, y bajo el estricto control y responsabilidad de la autoridad sanitaria competente.

6.5 SEGURIDAD DE LOS DATOS

Según el artículo 10° de la Ley N° 18.331 “las medidas tendrán que evitar la adulteración, pérdida, consulta o el tratamiento no autorizado y detectar desviaciones de información, ya sea por riesgos provenientes de la acción humana o del medio técnico utilizado “.

Por este principio se exige que quienes sean los responsables de la base de datos deberán tomar medidas que garanticen la seguridad y confidencialidad de los datos, ya sean medidas de índole técnicas u organizativas, cumpliendo con los estándares adecuados en seguridad de la información. Se debe prever también todos los riesgos asociados que se pueden presentar, garantizando así un buen funcionamiento del sistema de prevención de la seguridad de la información con respecto a la base de datos y los fundamentos que lo acompañan, como ser la confidencialidad, integridad y disponibilidad de la información, minimizando la posibilidad de filtraciones o acceso no permitido a actores que intenten vulnerar las bases de datos de algún modo.

Según la norma los datos deben ser almacenados de forma que permitan el ejercicio del derecho de acceso de su titular cuando éste lo requiera, es decir que debe estar resguardada de modo tal que su acceso sea ágil y oportuno cuando el titular de los datos así lo desee.

Finalmente, en el último inciso del artículo 10° especifica que queda prohibido registrar datos personales en bases de datos que no tengan condiciones técnicas de integridad y seguridad.

Resolución N° 59/020 de 8 de diciembre de 2020 de la URCDP: Esta resolución dirime respecto a una posible vulneración de seguridad que permitió el acceso no autorizado a datos personales administrados por la empresa UES S.A. que incluye información de tarjetas de crédito, nombres y domicilios de sus clientes. Estableciendo la obligatoriedad de los responsables de bases de datos de adoptar medidas necesarias para garantizar la seguridad y confidencialidad de los datos personales, según lo establecido en el artículo 10 de la Ley N° 18.331. Además, el Decreto N° 64/020, reglamentario de la Ley N° 19.670, dispone que, al constatarse una vulneración de seguridad que afecte la protección de datos personales, los responsables deben iniciar procedimientos para minimizar el impacto dentro de las primeras 24 horas y comunicarlo a la URCDP en un plazo máximo de 72 horas. Como resultado de la vulneración detectada la URCDP sancionó a la empresa con una multa de 12.001 Unidades Indexadas (UI) por incumplimiento a los artículos 10 y 17 de la Ley N° 18.331, la exhortó a efectuar una evaluación de impacto en protección de datos personales dentro del plazo establecido por el Decreto N° 64/020 y la intimó a culminar la inscripción de bases de datos en un plazo de 30 días hábiles, bajo apercibimiento.

6.6 RESERVA

Las personas (cualquiera fuera su naturaleza jurídica) que obtengan legítimamente información contenida en una base de datos, serán obligadas a utilizar dicha información en forma confidencial y exclusivamente para el tratamiento habitual de los mismos y con los fines relacionados a su actividad o función. El artículo 11° de la ley, prohíbe expresamente la difusión o divulgación de la información obtenida a terceros no autorizados, estando sujetas a una estricta confidencialidad para con los datos.

El artículo 11° también agrega que cualquiera sea el vínculo con el acceso a las bases de datos, los individuos que incurran en infracciones comentadas en el párrafo anterior hacen incurrir en el delito de secreto profesional previsto en el artículo 302 del Código Penal Ley N° 9.155 de 04 de diciembre de 1933. Cabe destacar que los funcionarios públicos tienen implícita la reserva en su relación funcional así como los dependientes en su relación laboral.

Esta responsabilidad se mantendrá vigente incluso luego de terminada la relación con el responsable de datos.

Resolución N° 52/021 de 07 de diciembre de 2021 de la URCDP: En esta resolución se manifiesta que entre los días 5 y 7 de diciembre de 2020, los denunciantes recibieron llamadas a sus teléfonos celulares donde se les practicó una encuesta, la que al parecer era de opinión

pública, pero en el transcurso de esta se transformó en una encuesta específica sobre la actividad lechera y su sistema político.

6.7 RESPONSABILIDAD PROACTIVA

El artículo 12 de la Ley N° 18.331, modificado por el artículo 39 de la Ley N° 19.670, regula el principio de responsabilidad. En su versión original el responsable era "responsable" de las infracciones a la normativa de protección de datos personales que pudieran suceder, con carácter general. La modificación evoluciona el concepto hacia el de una responsabilidad proactiva, en donde responsables y encargados de tratamiento deben ir más allá del cumplimiento de la ley, y adoptar medidas en que demuestren dicho cumplimiento.

Estas medidas deberán documentarse a efectos de demostrar, en caso de ser requerido por la URCDP, el cumplimiento efectivo de las normas en la materia. Obligación que no corresponde sólo a los responsables, sino que, en determinados casos, también a los encargados. Los responsables y encargados deben adoptar medidas que aseguren y demuestren el cumplimiento de la normativa de protección de datos personales. (URCDP, 2019)[15].

En Uruguay el Decreto N° 64/020 regula los casos en los que se debe realizar una evaluación de impacto en forma obligatoria (art. 6°), el concepto de privacidad por diseño (artículo 8°) y por defecto (Artículo 9°).

La URCDP podrá complementar estos aspectos, como hizo con la inclusión de los datos biométricos y su tratamiento que requerían una evaluación de impacto previa (Resolución N° 30/020 de 12 de mayo de 2020 de la URCDP).

Una buena política de protección de base de datos incluye la gestión de los accesos a la base de datos con fuertes contraseñas, mecanismos lógicos, control de usuarios privilegiados, enmascaramiento de la información y doble factores de autenticación lo que permite generar un entorno más seguro y confiable. Recomendado también la adopción del marco de ciberseguridad de AGESIC.

Dictamen N° 3/022 de 15 de marzo de 2022 de la URCDP: Este dictamen responde a una consulta realzada a la unidad respecto a si el género de una persona (hombre, mujer, hombre trans, mujer trans, no binario). A lo que la URCDP contesta que si bien el género no está incluido en la enumeración de datos sensibles prevista en el literal E) de ese mismo artículo pero se reconoce que puede referir a personas en situaciones vulnerables. Por ello, se recomienda que el responsable del tratamiento de estos datos realice una evaluación de impacto en la protección de datos personales antes de su tratamiento, conforme al artículo 6° literal d) del Decreto N° 64/020.

7. DERECHOS EN LA PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales no solo refiere a las obligaciones para quienes gestionan las bases de datos, sino que también brinda derechos a las personas (físicas y jurídicas) para controlar y hacer valer la protección de su información privada. Durán Martínez (2012) agrega que "puede definirse el derecho a la protección de datos personales 'como la facultad o el poder que tienen las personas para actuar per se y para exigir la actuación del Estado...'" (p. 11)[16]. Es así como la ley explicita en los artículos 13° a 17° principios que garantizan los derechos de los individuos alcanzados por la ley, los cuales en resumidas cuentas son derechos que permiten conocer, controlar y limitar el uso de sus datos privados.

- El derecho de acceso - artículo 14°: Este es uno de los principales derechos que le otorga la LPDP a los individuos, ya que le permite conocer qué información sobre ellos se encuentra almacenada en las distintas bases, ya sean de origen públicos o privados.

El acceso a la información debe procurar ser gratuito y los interesados sólo podrán realizar la solicitud en períodos no menores a seis meses; este período deberá ser cumplido salvo que exista un interés legítimo que justifique una solicitud en un plazo menor al estipulado.

En el inciso 2° del artículo 14° donde se aborda la temática de datos de titulares fallecidos, sufrió una modificación dada por la Ley N° 18.719 en su artículo 152°, especificando que en el caso que involucre datos de fallecidos, el derecho de acceso a la información podrá ser ejercido por cualquiera de los sucesores universales estipulados por la ley, que acrediten su condición de tal, bajo los estándares establecidos.

Para ejercer este derecho conforme a lo estipulado en el artículo 14° de la Ley N° 18.331, la URCDP implementó un formulario específico (Anexo 3), el cual se encuentra disponible en su página web para todo el público. El interesado de ejercer el derecho de acceso a la información debe completar y presentar este formulario ante el responsable de la base de datos, ya sea un organismo u empresa; una vez entregado comenzará a aplicar el plazo de 5 días hábiles para la respuesta por parte de los responsables de la base de datos en cuestión.

Este derecho se encuentra altamente vinculado con la Ley N° 18.381 "Derecho de Acceso a la Información Pública" de 17 de octubre de 2008, la cual garantiza el derecho de todas las personas a acceder a la información que se encuentre en poder del Estado y otros organismos públicos. Dentro de sus cometidos promueve la transparencia de la gestión pública y busca incentivar la participación ciudadana. En concordancia con el artículo 14° de la LPDP, la ley de acceso a la información pública establece que la información debe ser de acceso libre (salvo excepciones justificadas) y gratuita, estableciendo plazos para la entrega de esta.

La “Ley de Acceso a la Información Pública” es un tema de gran interés y se encuentra estrechamente relacionado con el objeto de este trabajo, sin embargo, dada su extensión y complejidad, no se profundizará en los detalles de este. En cuanto al procedimiento administrativo especial en materia de acceso a la información pública, se regulan expresamente la solicitud de acceso y sus requisitos (artículo 13), los límites (artículo 14), los plazos (artículo 15), la competencia para decidir (artículo 16), el acceso (artículo 17) y el silencio positivo (artículo 18), según lo señalado por Schiavi (2015)[17].

Un ejemplo de vulneración de este derecho se encuentra en la **Sentencia Nº 273/2010 del Tribunal de lo Contencioso Administrativo (TCA) del 1° de Setiembre de 2010**. En este caso, empresas que comercializaban semillas de maíz transgénico presentaron una acción de habeas data para impedir que se exhibieran registros que contenían información sobre sus operaciones comerciales. El TCA resolvió que dicha información no era de carácter reservado ni confidencial y que debía estar accesible al público, especialmente en materia ambiental, respaldando así el derecho de acceso a la información. Este fallo destaca la importancia del derecho de acceso a la información y cómo su vulneración puede ser objeto de acciones legales para garantizar su cumplimiento.

- El derecho de rectificación, actualización, inclusión o supresión - artículo 15° de la ley: Este derecho busca garantizar que la información almacenada en bases de datos sea precisa y que refleje la realidad, concluyendo en que los dueños de los datos no presenten dudas sobre la información que se posee de ellos.

Como se dispone en el artículo 15° de la Ley N°18.331, cualquier persona física o jurídica, puede solicitar ante el responsable de una base de datos u organización la eliminación o corrección de sus datos personales en el caso de que la información detallada presente errores, omisiones o datos falsos.

- ***Derecho de rectificación:*** detallado en el artículo 10° del Decreto 414/009, tiene como objetivo que el titular de los datos pueda solicitar que se modifiquen todos los datos que le pertenecen y que a su parecer resulten inexactos o incompletos, garantizando la exactitud y veracidad de la información personal de los titulares. (Anexo 4)

Sentencia Definitiva Nº 1410/2023 de 21 de diciembre de 2023 dictada por la Suprema Corte de Justicia. En el presente caso, un abogado solicitó la desindexación de información vinculada a su persona que devolvía un motor de búsqueda, la cual consideraba desactualizada y perjudicial para su honor e integridad. La Corte desestimó su recurso de casación, destacando la importancia de seguir los procedimientos específicos establecidos en la Ley N° 18.331 para la rectificación o eliminación de datos personales.

- ***Derecho de actualización:*** este derecho, explicado en el artículo 11° del Decreto 414/009, brinda a los propietarios de datos personales la posibilidad de solicitar que su información sea actualizada, rectificada o renovada cuando la misma se haya vuelto obsoleta, anticuada o incorrecta en el momento en el que se vaya a ejercer el derecho. Este derecho toma especial relevancia en casos en los que los datos pueden variar con el tiempo, como pueden ser las direcciones particulares, el estado civil, situaciones laborales, sin ser ésta una lista taxativa de los casos en los que se puede solicitar el ejercicio del derecho.

Resolución N° 33/020 de 2 de junio de 2020 de la URCDP: En esta resolución, una persona recibió llamadas de una cooperativa de ahorro y crédito a consecuencia de que una conocida suya proporcionó su número de teléfono al solicitar un préstamo. A pesar de que la afectada solicitó la eliminación de sus datos de contacto completando formulario a esos efectos, continuó recibiendo comunicaciones, lo que llevó a la URCDP a sancionar a la entidad responsable y a su encargado de tratamiento por no actualizar y suprimir correctamente los datos personales de la denunciante.

- ***Derecho de inclusión:*** explicado en el artículo 12° del Decreto 414/009, plantea que el titular puede solicitar que lo incorporen en una base de datos cuando demuestre con fundamento un interés legítimo para pertenecer a ella. El titular del dato personal puede solicitar ser incluido en una base de datos si por ejemplo se le demuestra que le trae aparejado un beneficio.

- ***Derecho de supresión:*** el titular tiene derecho a que se eliminen los datos cuya utilización por terceros resulte ilegítima, o que sean inadecuados o excesivos. La supresión no procederá cuando los datos personales deban ser conservados por razones históricas, estadísticas o científicas y de acuerdo con la legislación aplicable o en las relaciones contractuales entre el responsable y el titular, que justificaron el tratamiento de los datos.
El titular del dato personal puede pedir en cualquier momento que le supriman sus datos de una base de datos cuando no sea necesario su tratamiento, o si fue incorporado por error, o sin su consentimiento. El responsable debe documentar ante el titular que ha cumplido con lo solicitado.

Un ejemplo de denuncia presentada con respecto al derecho de supresión es la ***Resolución N° 07/020 de la URCDP del 18 de febrero de 2020***, en donde se presenta una denuncia contra Brisanier SA (Rappi Uruguay) por un incumplimiento del derecho de supresión, donde la denunciante presentó una solicitud de supresión de sus datos sin haber obtenido una respuesta en el término legal (5 días hábiles) por la empresa. En la resolución se observó a Brisanier S.A por el incumplimiento y se lo intimó a inscribir sus bases de datos en un plazo de 30 días hábiles.

Al igual que el derecho al acceso de la información, los derechos de rectificación, actualización, inclusión y supresión pueden ser ejercidos de manera gratuita, en períodos no menores a 6 meses y ante el responsable, a quien le regirá un plazo máximo para responder de 5 días hábiles desde la solicitud por parte del titular de los datos, por los medios que se hayan indicado, respondiendo si corresponde o no la solicitud, de una manera de fácil legibilidad e inteligible, sin utilizar claves o códigos. En caso de falta de respuesta o incumplimiento de los plazos por parte del dueño de las bases, el titular de los datos será habilitado para ejercer la acción de habeas data, concepto el cual será profundizado en un apartado específico dentro de este trabajo.

Es importante aclarar que mientras se lleva a cabo la verificación, corrección, inclusión o eliminación de los datos personales, los responsables de las bases de datos o de su tratamiento deberán indicar que la información se encuentra en un proceso de verificación por distintos motivos en aquellos casos en que concomitantemente se realice una solicitud de información de esos datos por un tercero.

En cuanto a los elementos necesarios para la solicitud, el Decreto 414/009 en su artículo 9° especifica que los derechos previstos en el artículo 15° en la ley podrán ser ejercidos por:

- El titular o cualquiera de sus representantes.
- De forma conjunta o independiente.
- Debe estar exento de formalidades y en forma totalmente gratuita.
- Mediante comunicación dirigida al responsable de la base de datos o tratamiento deberá contar con: la identificación del titular, el motivo de ejercer el derecho, domicilio (tanto real como constituido), fecha y firma del solicitante y documentos acreditativos de la solicitud que sean pertinentes y complementarios.

- ***El derecho a la impugnación de las valoraciones personales - Artículo 16°:*** este derecho pretende garantizar a las personas la protección de ser sometidas a decisiones que puedan afectar de manera significativa su vida, subsistencia o desarrollo, cuando éstas sean basadas únicamente en el tratamiento automatizado de datos y cuyo objetivo final sea evaluar determinados aspectos de su personalidad, rendimiento laboral, crediticio, de su conducta en diferentes ámbitos o de su confiabilidad. En otras palabras, este derecho pretende evitar que una persona, cualquiera sea su naturaleza, sea juzgada o categorizada únicamente por algoritmos o sistemas automatizados, sin una intervención humana apropiada que respalde su accionar.

En caso de que un individuo se vea afectado por alguna de estas circunstancias, podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, fundamentados exclusivamente por un tratamiento de datos personales que ofrezca una definición de sus características o personalidad. En caso de que realice estas acciones, el interesado podrá obtener información del responsable de la base de datos en cuestión, sobre los criterios que se tomaron en cuenta para dicha valoración, así como también al programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto.

- Derechos referentes a la comunicación de datos - Artículo 17° de la ley 18.331 y el artículo 14° del Decreto 414/009: Este derecho establece que los datos personales pueden ser intercambiados con terceros siempre y cuando la transferencia esté relacionada con un interés legítimo tanto del emisor como del destinatario. Para que la transferencia sea válida deben contar en una primera instancia, con el consentimiento expreso del titular de los datos a transferir, y se le debe informar de manera clara, sencilla y precisa la finalidad por la cual se está ejerciendo dicha transferencia, cuál será el destinatario de los datos transferidos y cuál es la actividad que éste desarrolla. En caso de que no se pueda identificar al destinatario, se deben brindar los elementos necesarios para poder hacerlo.

El previo consentimiento puede no aplicar en los casos que así lo disponga una ley de interés general. En los supuestos del artículo 9° de la ley (principio del previo consentimiento informado), cuando se haya aplicado algún procedimiento de disociación de información, siendo los titulares no reconocibles en el simple estudio de la información o cuando se trate de datos directamente vinculados a la salud y la comunicación sea imperativa por razones sanitarias, de emergencia o por razones epidemiológicas. Éste último caso de no aplicabilidad debe estar acompañado de mecanismos de disociación de los datos de las personas en los casos que por su sensibilidad lo requiera, estos criterios pueden encontrarse en la Resolución N° 68/017 de 26 de abril de 2017 de la URCDP.

En caso de que se presente alguna filtración, descuido, fuga o cualquier mal tratamiento de los datos transferidos, tanto el emisor como el receptor serán solidariamente responsables ante el titular de los datos y el órgano regulador.

La ***Resolución N° 23/021*** invalida las transferencias de datos personales a EE.UU. que se basaban en el marco del Privacy Shield. La URCDP determinó que dicho marco no proporcionaba un nivel de protección adecuado según los estándares uruguayos, afectando así la legalidad de ciertas comunicaciones de datos hacia ese país.

Así mismo, la ***Resolución N° 41/021 de la URCDP*** proporciona una guía con recomendaciones sobre el contenido mínimo de las cláusulas contractuales apropiadas para

la transferencia internacional de datos a países que no ofrecen niveles de protección adecuados. Esta guía busca asegurar que las comunicaciones de datos internacionales se realicen de manera segura y conforme a la normativa vigente.

8. DERECHO AL OLVIDO

El avance de las tecnologías ha transformado la manera en que se guarda, almacena y se accede a la información. Sin ir más lejos, todo lo que se publica en redes sociales como Instagram, Facebook o “X” en una primera instancia se clasifica como público, salvo que se realicen restricciones de privacidad, siendo de fácil acceso en motores de búsqueda como Google, Bing, Yahoo, entre otros. Toda esta información podría afectar de distintos modos a los individuos aún años después de haber sido publicada.

En este contexto, surge el denominado “derecho al olvido”, concepto que pretende ser una herramienta esencial en la protección de la privacidad y la reputación de las personas en el entorno digital actual. El derecho al olvido es una figura jurídica que permite a las personas solicitar la eliminación o desvinculación de información personal que ya no sea relevante o actualizada, especialmente en motores de búsqueda y plataformas en línea. Pablo Schiavi (2017) define el derecho al olvido como “derecho de toda persona, de todo titular de datos, a que determinada información personal que la hace identificable … no permanezca en forma permanente y de manera indefinida en internet las 24 horas del día y los 365 días del año”[18], es decir, que se intenta que toda información que identifica a las personas no permanezca accesible de manera indefinida en internet, sin la necesidad de borrar u ocultar información, sino que restringiendo su acceso a terceros.

El derecho al olvido se fundamenta en la idea de que los individuos no deben mantenerse constantemente vinculados a información pasada que no tiene importancia en el presente, especialmente cuando dicha información puede afectar negativamente su vida personal o laboral. Este derecho busca encontrar un equilibrio entre la protección de la privacidad y la libertad de expresión y el derecho a la información, siendo muy estrecha la línea entre el derecho al olvido y el incumplimiento de éstos, siendo esencial equilibrar la protección de la privacidad con el interés público en acceder a información histórica o relevante.

El origen del término está ligado al caso "Google Spain vs. AEPD" en la Unión Europea, el cual sentó precedentes en la aplicación del RGPD, al establecer que los motores de búsqueda serían los responsables del tratamiento de los datos personales, y que por tal motivo pueden ser obligados a eliminar lo que allí se encuentre en caso de que sea inadecuado, irrelevante o excesivo en relación con los fines para los que se procesó.

En los países que integran el sistema interamericano de derechos humanos (bloque al que pertenece Uruguay) no existe consagración normativa del llamado “derecho a olvidar”, por lo que, ante los recientes reclamos de olvido, la situación se vuelve aún más compleja (Rotondo, Delpiazzo, Mezzadri & Ruanova, 2023)[19]. En países como Argentina y Colombia se ha abordado el derecho al olvido en sus sistemas jurídicos, incluyéndose en los denominados “Derechos ARCO” y promulgando leyes directamente relacionadas a la temática. En general, la tendencia en América Latina ha sido defender la libertad de expresión garantizada por el sistema legal continental, lo que ha generado debates sobre la implementación del derecho al olvido y su posible colisión con otros derechos fundamentales, como en el caso de Brasil, en donde el Supremo Tribunal Federal (STF) de este país, determinó que el derecho al olvido es incompatible con la Constitución Federal de Brasil, considerando que el derecho al olvido restringiría de manera excesiva la libertad de expresión.

El concepto del derecho al olvido ha sido extensamente debatido y utilizado en varios países a nivel mundial, a pesar de ello, su reconocimiento y aplicación en Uruguay no es explícito, ya que no existe una regulación específica sobre el derecho al olvido. Se podría interpretar que el derecho al olvido se encontrara incluido en la Ley N° 18.331, sin embargo, como se detalló en el capítulo previo de este trabajo, esta normativa otorga derechos como el acceso, rectificación, actualización, inclusión y supresión de datos personales, sin hacer referencia explícita al derecho al olvido, generado un vacío legal que obliga a los jueces a interpretar su aplicación caso a caso. Se intentó su incorporación en la llamada “Ley de Urgente Consideración” (actual Ley N° 19.889 de 09 de julio de 2020), pero finalmente no se avanzó con el texto proyectado por posibles vulneraciones al derecho de libertad de expresión y de acceso a la información, que también son considerados fundamentales (Acosta, 2023)[20].

Si bien no existe la definición en una ley, la URCDP como órgano regulador en la materia se ha pronunciado al respecto, es así como en su Informe N° 305/019 de 13 de setiembre de 2019, ha definido al derecho al olvido como el derecho a "impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa" tomando como fuente lo expuesto por la Agencia Española de Protección de Datos.

Para ejemplificar una aplicación del derecho al olvido en nuestro país podemos citar la ***Sentencia Definitiva N° 193/2022 de Tribunal de Apelaciones Civil de 6° Turno*** de 3 de octubre de 2022, en donde el Tribunal de Apelaciones realizó una sentencia por primera vez en materia al derecho del olvido en Uruguay, condenando a Google Argentina SRL y a Google LLC. a la desindexación de ciertos contenidos en sus búsquedas, reconociendo al derecho al olvido, aunque no estuviera regulado por una normativa.

9. REGÍMENES ESPECIALES DE TRATAMIENTO DE DATOS

Si bien la Ley N° 18.331 de Protección de Datos Personales establece el marco general para el tratamiento de los datos personales, no todos se consideran con el mismo nivel de regulación. Es así que algunos de los detallados a continuación presentan un especial énfasis para la legislación, en el entendido que incluyen un mayor grado de sensibilidad y su mala utilización puede generar efectos jurídicos negativos sobre las personas. Por tal motivo, en el capítulo 4 de la ley denominado "Datos especialmente protegidos", se detallan a través de los artículos 18 a 23 aquellos regímenes especiales que se encuentran especialmente protegidos, siendo éstos:

• **Artículo 18 - Datos sensibles:** la ley define los datos sensibles como aquellos que revelen el origen racial u étnico, las preferencias políticas, las convicciones religiosas o morales, la afiliación sindical y las informaciones referentes a la salud o la vida sexual. La particularidad de este tipo de datos es tal que se especifica en la redacción del artículo que ninguna persona puede ser obligada a proporcionarlos, y solo pueden ser recolectados con el consentimiento expreso y escrito del titular, y tan solo en el caso de que medien razones de interés general autorizadas por la ley, o cuando el organismo o institución tenga autorización para realizar la acción.

• **Artículo 18-BIS - Datos biométricos:** Este artículo fue agregado por la Ley N° 19.924 de Presupuesto Nacional, en su artículo 87, el Poder Ejecutivo remitió al Parlamento el Proyecto de ley correspondiente al presupuesto introduciendo modificaciones en la Ley N° 18.331 en el entendido de que los datos biométricos debían presentar un especial régimen de regulación dentro de la legislación, por su nivel de singularidad y sensibilidad. Como antecedente se contaba con la Resolución N° 30/020 de la URCDP, en la que se resolvió que todo responsable que efectuara tratamiento de datos biométricos, debería efectuar una evaluación de impacto a la protección de datos personales, en condiciones y plazos establecidos. Estos datos se encuentran incluidos dentro de la clasificación de Datos Sensibles, dado que permiten la identificación de los individuos a partir de características físicas, fisiológicas o de comportamiento.

En los últimos años, el uso de tecnologías basadas en información biométrica para identificar o autenticar a las personas se ha vuelto común en la vida diaria, incluyendo huellas dactilares, rasgos faciales, voces, entre otros. Y es fundamental contar con una evaluación de impacto que tenga como objetivo principal identificar los riesgos a los que los datos personales pueden estar expuestos durante su tratamiento, con el fin de implementar controles que los minimicen o eliminen. Su finalidad última es garantizar el cumplimiento de la LPDP y demostrar dicho

cumplimiento. En este sentido, las organizaciones que gestionen datos biométricos deberán reforzar las medidas de protección de datos.

• **Artículo 19 - Datos relativos a la Salud:** Los centros de salud, tanto públicos como privados, así como los profesionales del ámbito sanitario, están autorizados a recopilar y procesar información personal relacionada con la salud física o mental de los pacientes que los consulten o que hayan estado bajo su tratamiento. Este tratamiento debe realizarse en cumplimiento de las normas específicas aplicables, respetando el secreto profesional y las disposiciones establecidas en la ley.

La recopilación de los datos confluye en la historia clínica del paciente la que incluye información íntima sobre enfermedades, tratamientos, adicciones, datos genéticos, entre otros aspectos sensibles como raza, vida sexual o creencias religiosas. Estos datos son esenciales para la atención médica y el bienestar del paciente, por lo que su veracidad es crucial. Los datos deben ser obtenidos directamente del paciente, salvo en situaciones de emergencia, y siempre con consentimiento informado, previo, libre y por escrito. El paciente debe ser informado de cualquier incidencia relacionada con el uso de sus datos, excepto en casos de urgencia o riesgo grave. La historia clínica puede ser solicitada por el paciente, su familia o sus sucesores en caso de fallecimiento, además debe mantenerse de forma confidencial, accesible solo para el personal autorizado y garantizar la seguridad de los datos, tanto escritos como electrónicos. Cualquier tratamiento de datos por terceros debe estar regido por cláusulas contractuales que aseguren la protección de la información. Además en la Ley N° 19.286 de 25 de setiembre de 2014 se regula el secreto médico profesional el cual debe respetarse en los certificados médicos con carácter de documento público y evitar que el médico tratante revele públicamente la patología concreta que aqueje a un paciente, así como las conductas diagnósticas y terapéuticas adoptadas.

Para citar un ejemplo, estas consideraciones cobran especial relevancia cuando se trata de la confidencialidad de información relativa a una persona infectada de Virus de Inmunodeficiencia Humana (VIH), toda vez que la revelación de esta información puede afectar de manera dramática su vida privada y familiar, laboral y social, exponiéndola al oprobio y el ostracismo (TEDH, Z. v. Finland, párrs. 111–112; I. v. Finland, Sentencia de 17 de octubre de 2008, párr. 35)[21].

• **Artículo 20 - Datos relativos a las telecomunicaciones:** Los proveedores de redes públicas o servicios de telecomunicaciones deben garantizar la protección de los datos personales en el ejercicio de su actividad, en cumplimiento de la normativa vigente. Asimismo, están obligados a implementar medidas técnicas y de gestión adecuadas para asegurar la seguridad en la operación de sus redes y la prestación de sus servicios, cumpliendo con los

estándares de protección de datos exigidos por la normativa complementaria. En caso de que se detecte un riesgo significativo de violación de la seguridad en las redes de comunicación electrónica o de la red pública de comunicaciones electrónicas, el operador responsable deberá notificar a los usuarios sobre la amenaza y las medidas que adoptará para mitigar.

En el mismo artículo se detalla que lo dispuesto en la ley se aplica sin perjuicio de las regulaciones específicas en materia de telecomunicaciones relacionadas con la seguridad pública y la defensa nacional que puedan presentarse.

• **Artículo 21 – Bases de datos con fines de publicidad:** Este artículo plantea que está permitido el tratamiento de información destinada a la elaboración de perfiles con objetivos comerciales para aquellos casos en los que la recopilación sea para la gestión de bases de datos con fines publicitarios o de mercadeo. Se incluyen dentro de esta lista las direcciones, distribución de documentos, actividades promocionales, prospección comercial, ventas y otras prácticas similares. Asimismo, se pueden analizar hábitos de consumo siempre que la información provenga de documentos de acceso público, haya sido proporcionada por los propios titulares o recopilada con su consentimiento.

En estos casos, los titulares de los datos tienen el derecho de acceder a su información sin costo alguno, y pueden solicitar en cualquier momento la eliminación o el bloqueo de sus datos en las bases de datos mencionadas en este artículo.

Cabe destacar que este artículo, en específico su inciso 1°, sufrió modificaciones por la Ley N° 18.719 en su artículo 152. Allí se modificó la denominación de actividades que menciona para la recolección de datos, incluyendo “prospección comercial” entre éstas. A simple vista se podría tomar como un simple cambio de redacción dentro del artículo, sin embargo, esta acción permite la ampliación del alcance del tratamiento de los datos, no limitando solo a los clientes actuales, sino también incluyendo a todos aquellos potenciales clientes.

• **Artículo 22 - Datos relativos a la actividad comercial o crediticia:** Este artículo autoriza expresamente el tratamiento de datos de las personas en lo que refiere a su solvencia patrimonial o crediticia, en aquellos casos donde se informe la capacidad de pago, la conducta comercial o posibilidad de concretar negocios en general. Esto incluye información sobre el cumplimiento o no de obligaciones comerciales o crediticias que presente el cliente, siempre y cuando ésta provenga de fuentes de acceso público, del acreedor o de situaciones previstas en la ley. En el caso de personas jurídicas, el artículo manifiesta que se permite el tratamiento de toda la información permitida por la normativa vigente.

Los datos personales relativos a las obligaciones comerciales de personas físicas solo podrán registrarse por un máximo de cinco años desde su incorporación en las bases de datos. Si la

deuda continúa pendiente al finalizar dicho período, el acreedor puede solicitar su renovación por otros cinco años, pero solo una vez y dentro de los 30 días previos al vencimiento original. Las obligaciones canceladas o extinguidas se mantendrán en el registro por un período máximo de cinco años, con la indicación expresa de su cancelación, sin posibilidad de renovación.

Los responsables de bases de datos deben procesar la información de manera objetiva, sin realizar interpretaciones subjetivas.

Cuando se cancela una obligación registrada, el acreedor tiene un máximo de cinco días hábiles para notificar al responsable de la base de datos, quien deberá actualizar la información en un plazo máximo de tres días hábiles.

Al igual que en el caso del artículo anterior, el artículo 22 sufrió modificaciones en la Ley N° 18.719 en su inciso 1°, cambio que busca una mayor precisión al momento de hablar de los datos, no sólo limitando a datos personales, y busca restringir su aplicación especificando que el objetivo final del artículo es evaluar la solvencia crediticia de los individuos.

• **Datos relacionados con el ámbito laboral:** En el ámbito laboral, el uso y tratamiento de los datos personales se encuentra restringido al marco del contrato de trabajo, siendo este el fundamento para la recopilación de la información necesaria para el cumplimiento de las funciones laborales. Las disposiciones en esta materia deben complementarse con las normativas laborales aplicables a sectores específicos de actividad, así como con las regulaciones relativas a la prevención de accidentes de trabajo y a la seguridad y salud laboral. Es pertinente, además, señalar que la documentación destinada a la protección y control del trabajo, conforme a la reglamentación pertinente, se considera adecuada a los términos de la Ley N° 18.331, en consonancia con lo dispuesto en el artículo 84 de la Ley N° 19.355 de 19 de diciembre de 2015, tal como fue modificada por el artículo 91 de la Ley N° 19.438 de 14 de octubre de 2016.

• **Artículo 23 – Datos transferidos internacionalmente:** Queda prohibida la transferencia de datos personales, cualquiera sea su naturaleza, a aquellos países que no revistan los niveles de protección adecuados, esta clasificación será realizada bajo los estándares del Derecho Internacional o Regional.

Quedan eximidos de esta prohibición los casos en los que la información sea englobada en alguno de estos casos:

- Cooperación judicial internacional, cuando esté estipulado en un tratado o convención y atendiendo las circunstancias del caso.

- Intercambio de datos de carácter médico, cuando sea por razones de salud o higiene públicas.

- Transferencias bancarias o bursátiles.

- Acuerdos en el marco de tratados internacionales en los que nuestro país forme parte.

- Cooperación internacional entre organismos de inteligencia en materia de lucha contra el crimen organizado, terrorismo y/o narcotráfico.

- El interesado haya dado su consentimiento inequívocamente.

- Que la transferencia sea necesaria para la ejecución de un contrato entre el responsable del tratamiento y el interesado, o para la ejecución de medidas adoptadas por el interesado

- Que la transferencia sea imprescindible para la formalización o ejecución de un contrato, ya sea vigente o a realizarse en el futuro, en beneficio del titular de los datos, entre el responsable del tratamiento y un tercero.

- Que la transferencia resulte esencial o que lo exija la ley para proteger un interés público relevante, o para el reconocimiento, ejercicio o defensa de un derecho dentro de un proceso judicial.

- Que la transferencia sea necesaria para la salvaguardia del interés vital del interesado.

- Que la transferencia provenga de un registro que, conforme a las disposiciones legales o reglamentarias, esté destinado a proporcionar información al público y esté abierta a la consulta por parte de éste, o a aquellas personas que presenten un interés legítimo, siempre y cuando se cumplan las condiciones establecidas por la ley para su consulta.

A pesar de lo expuesto anteriormente, la URCDP está facultada para permitir una transferencia de datos personales a un país que no cuente con la protección adecuada, siempre y cuando el responsable del tratamiento de datos asegure fehacientemente que tiene medidas suficientes para resguardar la privacidad, los derechos fundamentales, y el ejercicio de estos. Estas garantías pueden derivar o estar respaldadas por cláusulas contractuales apropiadas.

Otros regímenes especiales que revisten especial tratamiento:

Tratamiento de datos de menores: El criterio general es la necesidad de recabar el consentimiento de sus padres o tutores antes del tratamiento de los datos de menores. Los responsables deben cuidar la utilización de este tipo de datos personales, debiendo considerar la finalidad y las medidas de seguridad como elementos esenciales previo a su

análisis. El Decreto N° 64/020, en su artículo 6°, establece que el tratamiento de datos de menores requiere una evaluación de impacto previa (URCDP).

Tratamiento de datos de videovigilancia: El uso de videovigilancia implica la captación de imágenes y sonido, considerados datos personales protegidos por la normativa vigente. La URCDP ha analizado esta temática en distintas ocasiones, estableciendo en el Dictamen N° 10/010 de 16 de abril de 2010 que la videovigilancia abarca la grabación, transmisión, conservación y almacenamiento de imágenes y, en algunos casos, sonidos, mediante la utilización de videocámaras u otro medio análogo. Dado que la grabación de imágenes constituye información personal, su tratamiento debe cumplir con la normativa de protección de datos. Es fundamental definir qué puede ser videovigilado, de qué forma y bajo qué principios, además de determinar si los registros deben conservarse. La videovigilancia tiene como principales objetivos la protección de personas y bienes, el mantenimiento del orden público y la prevención de delitos, entre otros intereses legítimos. Asimismo, la normativa exige la presencia de logos de videovigilancia, establecidos en la Resolución N° 989/010 de 30 de julio de 2010. Por su parte, la Resolución N° 58/021, regula el uso de cámaras en distintos ámbitos, incluyendo seguridad personal, espacios públicos, entidades bancarias, lugares de trabajo, complejos habitacionales, edificios públicos, vehículos, instituciones educativas y drones.

10. INSCRIPCIÓN EN EL REGISTRO DE BASES DE DATOS PERSONALES

Toda base de datos, ya sea de origen público o privado, deberá ser inscripta en el registro de bases de datos que lleva a cabo la URCDP, creado por el artículo 1° del Decreto N° 664/008 de 22 de diciembre de 2008, de acuerdo a los criterios que se establezcan en la ley y en las resoluciones posteriores por parte del regulador de conformidad a las facultades legales conferidas a éste.

Ningún usuario, dueño de base de datos o responsable de la misma, podrá poseer datos personales que difieran de la cualidad declarada en el registro. Si se constata que se incumplió en algún aspecto de lo declarado o se presenta alguna irregularidad en el uso de las bases de datos, se dará lugar a las sanciones administrativas que se encuentran reguladas en la ley.

El artículo 15° del Decreto N° 414/009 establece que deberán inscribirse en el registro de la URCDP:

A. Personas físicas que generen, alteren o eliminen bases de datos con información personal, siempre que su uso no sea estrictamente personal o doméstico.

B. Personas jurídicas tanto privadas como públicas, ya sean estatales o no, que creen, modifiquen o supriman bases de datos con información personal, con excepción a las previstas en la ley.

C. Los códigos de conducta de práctica profesional, en donde se establezcan las normas para el tratamiento de datos personales.

D. Autorizaciones que presente en relación a las transferencias internacionales de datos personales.

Se detalla también en el artículo 15° de la ley, que para realizar la inscripción será necesario que el responsable de la base de datos a registrar debe declarar una serie de datos de carácter obligatorio, entre los que se encuentran:

- Identificación de la base de datos
- Responsable de la base de datos a registrar.
- Naturaleza de los datos que va a almacenar la base de datos a inscribir.
- Procedimientos de obtención y tratamiento posterior de datos.
- Medidas que garanticen la salvaguarda en materia de seguridad de los datos.
- Descripción técnica de la base de datos.
- Protección de datos personales y ejercicio de los derechos en la materia.
- Destino final de los datos personales y toda aquella persona física o jurídica a las que puedan ser transmitidos cualquiera sea el medio de transmisión.
- Tiempo estimado de conservación de los datos por parte del dueño de las bases.
- Métodos en los que los titulares de los datos podrían llegar a acceder a los datos referidos a su persona en caso de ser necesario. Así como también especificación de los procedimientos que pueden llevar a cabo los titulares de datos en relación a la rectificación o actualización de la información cuando proceda.
- Número de acreedores que revistan la calidad de persona física y que hayan alcanzado el plazo de cinco años establecido en el artículo 22° de la ley (datos relativos a la actividad comercial o crediticia)
- Número de cancelaciones por cumplimiento de la obligación de pago (en caso de corresponder), también bajo las directrices del artículo 22° de la ley. Este literal se incluyó en la Ley N° 18.719, no estando presente en la redacción original de la ley.

El artículo 16° del Decreto N° 414/009, a través de su modificación por el Decreto N° 30/014 de 11 de febrero de 2014, agrega a la lista del Artículo 15° de la ley, que se deberá también proporcionar información sobre el domicilio constituido de la persona, organización o grupo que será la responsable de la base de datos, con el cometido de que en caso necesario se puedan realizar las comunicaciones y/o notificaciones que se necesiten.
Será obligación del responsable de las bases de datos mantener actualizados los datos que se inscriben en el registro de base de datos, comunicando trimestralmente si existen modificaciones o actualizaciones.

Hoy en día la inscripción de las bases de datos se realiza a través del sistema de registro en línea, el cual se encuentra disponible en el sitio web de la URCDP.
Desde 2016, los responsables del registro de las bases de datos cuentan con esta herramienta digitalizada, que facilita el envío y formalización del registro. Esta herramienta a lo largo de los años se ha ido perfeccionando para hacer cada vez más ágil el proceso de registro, logrando que actualmente solo contando con un usuario “Gub.uy” de identificación electrónica, en cualquiera de sus modalidades, se le permite al responsable de las bases de datos el acceso al sistema para la carga de los datos que allí se le requieren.
El trámite es sin costo y el ingreso es individual por persona física. La información que allí se releva es información sobre qué tipo de datos son recolectados, por qué se recolectan, cuantas personas son alcanzadas, si se hace comunicación de datos o transferencias de datos al exterior, así como las medidas de seguridad lógicas y físicas adoptadas para asegurar la confidencialidad de los datos, tal como se estipula en la ley.

El plazo de inscripción de las bases de datos está reglamentado por el artículo 17° del Decreto 414/009, en el cual se dispone que toda base de datos que presenten carácter personal y estuvieran en funcionamiento al momento de la creación del decreto, contaban con 90 días corridos desde la publicación en el Diario Oficial para regularizar la inscripción, éste inciso se creó para darles a los responsables que ya se encontraban operando en ese momento un plazo razonable para regularizar su situación para con el regulador. Sin perjuicio de esto, también se establece que toda base de datos que fuera creada luego de la aprobación del decreto y que presenten carácter personal, deberán ser inscriptas en un plazo máximo de 90 días contados a partir del inicio de sus actividades.
La fecha de inscripción de la base de datos será dada por la resolución de la URCDP que aprueba la misma y deberá ser exhibida por parte de los responsables de bases de datos, en un lugar que presente clara visibilidad y acceso a los usuarios, junto con el número de resolución que dio a lugar la inscripción.

Para contextualizar, la cantidad de trámites que recibe la URCDP aumenta anualmente, accediendo a los datos abiertos de la URCDP pudimos observar que en 2024 se registraron un total de 376 bases de datos, correspondientes a 185 responsables distintos (8 personas físicas, 18 organismos públicos y 159 personas jurídicas), y que entre ellas predomina la inscripción de bases de datos de videovigilancia (Fuente: URCDP)[22].

11. ÓRGANO REGULADOR

Un pilar clave para el cumplimiento de la normativa vigente es la figura de un órgano regulador con la potestad de velar por el correcto cumplimiento de la Ley N° 18.331, así como de controlar, regular y sancionar en caso de incumplimiento. Por esta razón, la legislación uruguaya ha puesto especial énfasis en definir a través de los artículos 31° a 36° de la ley la composición, cometidos y atribuciones del órgano que cumplirá con estas características, estableciendo su rol dentro del marco normativo uruguayo.

La autoridad de control de los datos personales definida por ley es la URCDP, ésta se crea en el Artículo 31° de la Ley N° 18.331, en el cual se "define como un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)". Cuenta con autonomía técnica, no así presupuestal, dependiendo de AGESIC en este sentido. Sus principales competencias son custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios, con el cometido de garantizar la protección efectiva de los datos personales de los ciudadanos uruguayos, asegurando que su tratamiento sea legítimo, transparente y acorde con la legislación vigente.

La máxima autoridad es el Consejo Ejecutivo, el cual está conformado por un equipo de trabajo interdisciplinario, compuesto por integrantes de distintas ramas, como ser expertos en derecho, tecnología y privacidad. El consejo se conforma por tres miembros, el director ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo elegidos conforme a sus antecedentes personales, profesionales y de conocimiento en la materia. El Consejo Ejecutivo está asistido por un Consejo Consultivo, que está integrado por cinco miembros, un representante del Poder Legislativo, un representante del Poder Judicial, un representante del área académica, un representante del Ministerio Público y un representante del sector privado.

Como órgano de control debe realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones que la ley así disponga. Sus principales tareas se encuentran reguladas en el artículo 34° de la Ley N° 18.331, entre las cuales se destaca la asistencia y asesoramiento a las personas, la potestad de dictar normas y reglamentaciones,

realizar un censo de las bases de datos, controlar la observancia del régimen legal, solicitar información a entidades públicas y privadas, emitir opinión toda vez que sea requerido, asesorar al Poder Ejecutivo en proyectos de ley relacionados con la materia e informar a las personas sobre la existencia de bases de datos, finalidad e identidad de sus responsables.

Dentro de sus potestades también se encuentra la posibilidad de aplicar sanciones, las cuales pueden ser: observación, apercibimiento, multa de hasta 500.000 unidades indexadas, suspensión de la base de datos por hasta 5 días y clausura de la base de datos. Para este último caso requiera control judicial previo. La ***Resolución N° 105/015 de 23 de diciembre de 2015*** del consejo ejecutivo de la URCDP determina las infracciones plausibles de sanción y su categorización. Las sanciones se categorizan en muy leve, leve, grave o muy grave. Para su determinación toma en cuenta aspectos como gravedad, reiteración o reincidencia de la infracción y los antecedentes del infractor.

Para aplicar dichas sanciones, en una primera instancia la URCDP recibe los reclamos y denuncias de los individuos. A través de los años, y ligado con el mayor conocimiento por parte de las personas sobre la protección de datos personales, la URCDP ha visto incrementado su número de denuncias y reclamos recibidos. Es así que para 2023 la URCDP recibió 141 denuncias, 48 más que para 2019 (Fuente: URCDP)[23]. Para 2020 la mesa de ayuda de la URCDP, quien realiza la atención de consultas formuladas por distintos canales, recibió más de 1600 consultas, de las cuales culminaron en la creación de expedientes para su análisis posterior 32 consultas, 101 en denuncias y 8 solicitudes de informe (Fuente: Memoria Anual 2020 de la URCDP)[24].

Desde sus comienzos, la Unidad ha desarrollado importantes tareas de capacitación y sensibilización dirigidas a diferentes sectores de la sociedad incluyendo a las personas, empresas y organismos del Estado. Se encuentra disponible actualmente un curso sobre protección de datos personales en Uruguay (que tiene como objetivo dar a conocer los conceptos básicos sobre la regulación del derecho a la protección de datos personales en nuestro país), disponible en la plataforma educativa de AGESIC. Además ha hecho énfasis en la capacitación de niños, adolescentes y sus familias a través de campañas dirigidas a las escuelas públicas y privadas del país bajo la nomenclatura "Tus datos valen. Cuídalos" que fue de 2013 a 2018. Adicional al trabajo comentado anteriormente, de forma aperiódica la URCDP publica la “Revista uruguaya de Protección de datos personales”, en la cual se incluye información actual en la materia, entrevistas y actualizaciones pertinentes.
Otras labores de la URCDP en cumplimiento de su cometido son:

- El 28 de enero la URCDP se suma a la celebración del Día Internacional de la Protección de Datos Personales, y destaca la importancia de que las personas

conozcan sus derechos, obligaciones y los mecanismos para cuidar sus datos personales.

- Cumple con lo establecido en la Ley N° 18.381 en sus artículos 5° y 7° en lo que respecta a acceso a información pública como organismo estatal.
- Con el motivo de promover la protección de datos personales y posicionar a nuestro país como ejemplo a nivel mundial, la URCDP ha enfocado sus esfuerzos en desarrollar la cooperación internacional. Es así como ha establecido convenios de cooperación en materia de protección de datos personales con diversos países, siendo uno de los ejemplos la participación en la Red Iberoamericana de Protección de Datos, así como también del Comité Organizador de la Conferencia Internacional de Protección de Datos.

12. HABEAS DATA

Uruguay no contaba con una ley específica en materia de protección de datos personales previo a la promulgación de la Ley N° 18.331, esto provocaba que las garantías relacionadas a la privacidad de los individuos se encontraran dispersas en distintas normas de carácter más general, como ser en la Constitución de la República o en algunas disposiciones dentro del Código Civil, las cuales apuntaban más concretamente a la protección de la intimidad de las personas y no al pleno derecho de la protección de sus datos identificatorios, no existiendo un procedimiento definido que habilitaba a las personas reclamar o iniciar acciones respecto al tratamiento indebido o inapropiado de sus datos. Años antes de la promulgación de la Ley Nº 18.331 en la legislatura uruguaya se presentó la Ley Nº 17.838 de 24 de setiembre de 2004 (actualmente derogada), la cual introdujo el habeas data como una acción especial dentro del sistema procesal uruguayo, siendo un antecedente inmediato al actual habeas data. Esta normativa permitió, por primera vez en el país, que los ciudadanos pudieran solicitar judicialmente el acceso, la rectificación o la supresión de datos personales. Si bien constituyó un avance inicial, su regulación era considerada insuficiente y limitada en cuanto a los alcances sustantivos y procedimentales, Guerra Pérez (2005, p.147) señala que “esta ley no alcanzaba a la protección de todos los datos personales porque el uso que de ellos pueda realizarse en cualquier circunstancia, sino que está limitada a la protección de datos personales cuyo tratamiento tenga un destino comercial […]”[25]. Es así como el régimen uruguayo comenzó a notar la necesidad de adecuar el régimen actual a estándares internacionales, como los establecidos en el Convenio 108 del Consejo de Europa, impulsando la posterior sanción de la Ley Nº 18.331, que superó las deficiencias anteriores y estableció un sistema integral de protección de datos.

El habeas data se encuentra estipulado en los artículos 37° a 45° de la Ley N° 18.331; es un instrumento jurídico que permite a las personas conocer, actualizar, rectificar y, en ciertos casos, suprimir la información personal que se encuentren almacenados en distintas bases de datos, sean estas públicas o privadas. En la doctrina nacional, Sánchez Carnelli precisa que:

> "el habeas data comprende dos aspectos: es un medio para conocer la información o los datos existentes y es un medio para poder rectificarlos a los efectos de restablecer la verdad. Siendo entonces una garantía del derecho al honor del individuo como medio para poder asegurarse que no existirán informaciones falsas y no se le afectará con las mismas"[26].

Esta acción responde a la necesidad de preservar la dignidad humana y proteger la autonomía personal frente al tratamiento indiscriminado o incorrecto de información. Gaiero Guadagna y Soba Bracesco señalan que "se trata de un procedimiento sumario, autónomo, definitivo, no residual, de tutela diferenciada para ciertos derechos de raigambre constitucional previstos por la norma, ubicado fuera del Código General del Proceso (extra código), contencioso y de conocimiento."[27]

El artículo 38 y 39 de la ley introduce la acción de habeas data, estableciendo que cualquier persona podrá acudir ante el Poder Judicial para ejercer los derechos de acceso, inclusión, rectificación, actualización o supresión de datos personales que consten en distintas bases de datos. Anterior a presentarse al Poder Judicial, el titular de los datos (su representante o sucesores universales en caso de personas fallecidas) debe haber presentado directamente al responsable de la base de datos el deseo de ejercer sus derechos y, frente a una respuesta negativa o falta de respuesta en el plazo de cinco días hábiles de éste, podrá promover la acción judicial en cuestión. La ley contempla que el proceso será sumario y de trámite urgente, priorizando la protección efectiva de los derechos vulnerados y serán aplicables en lo pertinente al artículo 14° y 15° del Código General del Proceso.

Una vez presentada la demanda, el juez analizará la legitimidad del tratamiento de los datos en cuestión y si corresponde o no la acción de habeas data (Cristina Vázquez Pedrouzo (2011) señala que "para denominar la vía de garantía tendiente a obtener del Juez competente una decisión que permita el acceso a determinada información, se emplea la expresión 'habeas data impropio', reservando 'habeas data propio' o simplemente 'habeas data' para el caso en que la acción refiere al ejercicio del derecho a la protección de datos personales"[28]), si resulta que la acción fuera manifiestamente improcedente se archivará la solicitud y se rechazará toda acción posterior, de lo contrario se continúa el trámite en el Juzgado, convocando a ambas partes a una audiencia pública dentro de los tres días de la fecha presentada la

demanda. La sentencia definitiva que obtenida como resultado del proceso podrá ordenar el acceso, la rectificación, actualización, inclusión o supresión de los datos personales, según corresponda al caso y lo que se haya solicitado en una primera instancia. Esta resolución judicial deberá ser ejecutada con efectos inmediatos. En caso de que se incumpla toda la resolución o parte de ésta, se podrán imponer medidas coercitivas con el fin de asegurar la correcta ejecución de lo dispuesto.

Dentro de la doctrina uruguaya se destaca que el proceso de habeas data constituye un mecanismo de tutela de los derechos fundamentales en el ámbito de las nuevas tecnologías de la información. Carlos E. Delpiazzo expresa que:

> "Frente al «poder informático» de quienes pueden acumular informaciones sobre cada persona en cantidad ilimitada, de memorizarla, usarla y transferirla como una mercancía, el derecho a la intimidad se configura como una nueva forma de libertad personal, ya no caracterizada negativamente como la posibilidad de refutar o evitar el uso de datos referidos a cada uno, sino positivamente como la potestad de ejercer un poder de control sobre las informaciones referidas a la propia persona. Consiste en lo que ha dado en llamarse libertad informática, consistente en el derecho de autotutela de la propia identidad informática, es decir, en el derecho de vigilar los datos personales incluidos en archivos automatizados."[29]

13. COMPARACIÓN INTERNACIONAL

A modo de ejemplificar la importancia de la protección de los datos personales hacemos referencia a normativas que regulan a nivel regional e internacional dichos derechos:

- **Unión Europea -** El Parlamento de la Unión Europea y del Consejo aprobó el 4 de mayo de 2018 el Reglamento 2016/679 siendo aplicable a partir del 25 de mayo de 2018 para 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 (RGPD). Su objetivo central es proteger la privacidad y seguridad de los datos personales de los ciudadanos de la Unión Europea (UE), incluyendo tanto a empresas que operan en la UE como a aquellas que ofrecen bienes o servicios a ciudadanos de la UE, independientemente de si están ubicadas dentro o fuera de la UE.

- **México -** El derecho a la protección de datos personales se encuentra regulado en diferentes ordenamientos según el ámbito de que se trate. En el caso del ámbito privado se regula con la "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (LFPDPPP) publicado en el Diario Oficial de la Federación el 5 de Julio de

2010 teniendo como objetivo la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. En lo que respecta al Sector Público se rige por la "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados" (LGPDPPSO) publicada en el Diario Oficial de la Federación el 26 de enero de 2017 y tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados, responsables en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

- **Chile** - La Ley N° 19.628 sobre Protección de la Vida Privada (LPVP) publicada el 26 de Agosto de 1999, establece las reglas sobre tratamiento de datos personales que realicen tanto los órganos públicos como particulares, determinando un conjunto de derechos de los titulares y las obligaciones de los responsables del tratamiento, teniendo como objetivo principal garantizar el derecho a la privacidad y proteger los datos personales de las personas físicas. A finales del año pasado se publicó la Ley N° 21.719 Protección de los Datos Personales con vigencia a partir del 1° de diciembre de 2026, la cual va a incorporar modificaciones a la antedicha ley la cual establecerá un marco normativo integral para garantizar el derecho a la privacidad y adecuarlo a los desafíos del entorno digital. De esta manera se integra un enfoque centrado en la protección de los derechos fundamentales de los titulares, abarcando diversos aspectos relacionados con el tratamiento de datos personales, regulaciones específicas para categorías especiales, procedimientos administrativos y la creación de una autoridad fiscalizadora.

- **Brasil** - La Ley General de Protección Datos (LGPD) N° 13.709 se publicó el 15 de agosto de 2018 y entró en vigor el 18 de setiembre de 2020. Su propósito es salvaguardar los datos personales, protegiendo los derechos fundamentales de libertad y privacidad de las personas. Estipula el marco legal que cubre las actividades de los controladores y procesadores de datos e instaura requisitos para el procesamiento de estos datos de los ciudadanos.

- **Argentina** - La Ley de Protección de Datos Personales Argentina (PDPA) N° 25.326 fue sancionada el 4 de octubre de 2000 y se promulgó parcialmente el 30 de Octubre de 2000 y tiene por finalidad proteger los derechos de los individuos relacionados con la privacidad y el tratamiento de sus datos personales, garantizando el control y la seguridad sobre la

información personal de los ciudadanos almacenadas en base datos públicas y privadas. El 9 de noviembre de 2022 aprobó la Ley N° 27.699, siendo promulgada el 30 de Noviembre de 2022 denominada Protocolo Modificatorio del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal donde se ratificó el Convenio 108+. Durante el transcurso del año 2023 se presentó un nuevo proyecto de ley con el fin de actualizar y fortalecer el marco legal existente, reforzando la gestión de políticas públicas con el objetivo de dar respuesta a los desafíos que imponen los avances tecnológicos, así como acompasarse con los estándares regionales e internacionales. Algunas de las modificaciones propuestas son el agregado de nuevos términos como la minimización de datos y la neutralidad tecnológica, la incorporación de bases legales adicionales para el procesamiento de datos personales sensibles y una protección especial para los menores. También la obligatoriedad de informar incidentes de seguridad en un plazo de 72 horas, y reformar el cálculo de las multas por infracciones al régimen de protección de datos. Sin embargo, desde su presentación al Congreso, dicho proyecto no tuvo avances significativos.

14. DESAFÍOS VINCULADOS A LA PROTECCIÓN Y LA PRIVACIDAD DE DATOS

En tiempos donde el avance tecnológico va a pasos agigantados, en cuestiones de Big Data, Internet de las Cosas, Inteligencia Artificial, Blockchain, entre otras tecnologías emergentes hacen que la generación, trasmisión y comunicación de datos reporten numerosos beneficios para organizaciones tanto públicas y privadas a nivel local e internacional. No obstante, es fundamental tener presente temas relativos a la privacidad, ética y protección de los datos de los individuos, los riesgos asociados en el uso y sobre todo las consecuencias que pueden ocurrir si esos datos son vulnerados.

Nuevas tecnologías de la información

Un primer desafío, como mencionamos, deriva del ámbito de la protección y la privacidad de los avances tecnológicos. La era digital facilita la vida cotidiana de las personas, pero también lleva a que muchos datos personales sean recopilados, almacenados y procesados en un corto período de tiempo, planteando retos considerables en materia de privacidad. Estas tecnologías involucran un tratamiento masivo y automatizado de datos personales que son susceptibles de vulnerar los derechos fundamentales de los individuos debido a su competencia para procesar grandes volúmenes de datos en tiempo real. A modo de ejemplo, las aplicaciones que se descargan en los teléfonos celulares para entrega de comida a domicilio cuentan con nuestros datos personales de nombre, apellido y dirección, correo electrónico, así como también en algunos casos medios de pagos electrónicos y hasta

ubicación en tiempo real, lo que sin una debida custodia, puede dejar expuestos datos identificatorios inequívocos de la persona.

Evolución de la Normativa y Cumplimiento

Como un segundo nivel de desafío encontramos una dicotomía entre la velocidad frenética de los avances tecnológicos y el progreso de la regulación jurídica. A pesar de que muchos Estados tienen establecidos derechos respecto a la protección de datos, parte de esa normativa no está acompasada a los últimos avances tecnológicos generando brechas legales entre lo que establece la ley y lo que se aplica en la realidad, debiéndose en gran parte por la complejidad y rigidez que tiene la elaboración y discusión de la normativa a nivel parlamentario y en la demora en la adhesión de algunos países a los convenios internacionales. Es primordial comprender que el cumplimiento de la normativa no debe ser vista tan solo como una obligación legal, sino también como una posibilidad para robustecer la confianza y optimizar la gestión de la información de las personas involucradas. La inclusión de programas de cumplimiento efectivos, que abarquen auditorías regulares, formación continua del personal y la designación de delegados de protección de datos, constituye una estrategia clave para garantizar una gestión apropiada y consciente de los datos personales.

Globalización y transferencias internacionales de datos

En tercer lugar, la universalización de las transacciones comerciales y de servicio sumado al incremento de las transferencias internacionales de datos personales anexan otra capa de dificultad a la protección de datos personales. El reglamento 2016/679 del Parlamento Europeo y del Consejo establece condiciones estrictas para la transferencia de datos personales fuera del Espacio Económico Europeo (EEE) con el fin de garantizar que no se vea deteriorado el nivel de protección de los datos personales relacionados. Asegurar el cumplimiento de estas disposiciones en un entorno globalizado puede resultar desafiante, especialmente cuando se interactúa con jurisdicciones que cuentan con marcos legales de protección de datos menos rigurosos o disímiles.

Un ejemplo de esto fue la sentencia del Tribunal de Justicia de la Unión Europea conocido como Schrems II, que ha puesto de manifiesto la necesidad de realizar una revisión constante y exhaustiva de los mecanismos de transferencia de datos, tales como la implementación de cláusulas contractuales tipo y las normas corporativas vinculantes, a fin de ofrecer las garantías adecuadas en la práctica. Dejando como corolario que cada faceta relativa a salvaguardar el derecho a la protección de datos exige una verificación constante y su actualización conforme a las mejores políticas disponibles en cada momento.

Ética y Protección de Datos

Por último, pero no menos importante, tenemos desafíos ligados a la ética en el tratamiento de datos personales que exceden lo que es el simple cumplimiento o adherencia a la norma. En el mundo actual las decisiones están basadas e impulsadas por los datos que las organizaciones recopilan o de la información que la propia persona comparte o deja pública y en el hecho de la inmediatez o el procesamiento de dicha información se pueden generar vulneraciones a la privacidad y sesgos éticos en el uso de datos personales y generales. Como podría ser el caso de utilizar algoritmos para identificar un patrón de conducta o preferencia, o permitir o no el acceso a un determinado sitio en función de un software de reconocimiento biométrico lo que ocasionen algún tipo de discriminación o prejuicios sociales y culturales que afecten negativamente a las personas y a la sociedad en su conjunto. Desde una perspectiva ética, estas iniciativas deben basarse no solo en marcos legales sólidos y robustos, sino también ser justas, transparentes e imparciales.

15. CONSIDERACIONES FINALES

En el transcurso de este trabajo se ha constatado que nuestro país ha desempeñado un papel destacado en lo que refiere a la protección de datos personales, siendo pionero y referente en la región, adoptando estándares y buenas prácticas de distintos países del mundo. Desde la promulgación de la Ley N° 18.331, Uruguay ha dado pasos firmes en la consolidación de un marco normativo firme, estructurado, que se adapta a las distintas realidades que engloban el país y que es flexible a nuevas actualizaciones al no contener una estructura limitativa ni taxativa en su contenido.

Es fundamental que tanto las instituciones públicas como privadas acompañen los esfuerzos de la legislación uruguaya en protección de datos reforzando su compromiso en el cumplimiento de la ley, priorizando dentro de sus estrategias de negocio acciones acordes a lo estipulado en la normativa vigente.

Uruguay, y en especial la URCDP, ha trabajado en concientizar a distintos sectores de la población, intentando llegar tanto a empresas de distintos tamaños como a familias en su cotidianidad, sin embargo, es importante continuar con este proceso y que no sean situaciones aisladas. Es fundamental continuar con campañas de sensibilización y formación en protección de datos, tanto para los ciudadanos como para los profesionales de las empresas, con pautas definidas provenientes de la URCDP y en especial de las cúpulas directivas de las organizaciones.

Del análisis se desprende que Uruguay ha logrado adecuarse al entorno global en la materia, no obstante, el reto de garantizar que las empresas extranjeras cumplan con la normativa

local cuando operan en su territorio sigue siendo un debe y una tarea compleja de llevar a cabo. La exigencia a otros territorios de la ley de protección de datos debe estar presente al momento de realizar transacciones o acuerdos comerciales, con el fin de garantizar la protección de datos no solo de los uruguayos, sino que la de todos los individuos involucrados.

Como conclusión, a nivel mundial los nuevos desafíos en protección de datos requieren una respuesta integral que combine un estricto cumplimiento normativo, así como la implementación de tecnologías seguras y el fomento de una cultura organizacional centrada en la privacidad. Solo mediante un enfoque proactivo y multidimensional se podrá garantizar una protección efectiva de los derechos individuales en un entorno cada vez más digitalizado, globalizado e interconectado. Por ende es fundamental que los Estados trabajen en comunidad y armonía en pos de velar y garantizar dichos derechos, más allá de las fronteras territoriales.

REFERENCIAS BIBLIOGRÁFICAS

1: Peschard Mariscal, J. (2011). Protección de las niñas, niños y adolescentes en el uso de tecnologías de información y comunicación. México: Instituto Federal de Acceso a la Información y Protección de Datos.

2: Bernier, C. (2011). El memorándum de Montevideo. México: Instituto Federal de Acceso a la Información y Protección de Datos. Página 16.

3: Durán Martínez, A. (2011). Derecho a la protección de datos personales y habeas data. Montevideo: Fundación de Cultura Universitaria.

4: González Fuster, G. (2014). The emergence of personal data protection as a fundamental right of the EU. Springer.

5: Masciotra, M. (2019). Habeas Data: Un proceso urgente tutelador de derechos fundamentales. Buenos Aires: Editorial Jusbaires.

6: Zavala, M. (1982). Derecho a la intimidad. Buenos Aires: Editorial Astrea.

7: Maqueo, M., Moreno, J., & Recio, M. (2016). Protección de datos personales, privacidad y vida privada.

8: Voigt, P. y Von dem Bussche, A. (2017) El Reglamento General de Protección de Datos (RGPD) de la UE: Una guía práctica. 1.ª edición, Springer International Publishing, Cham.

9: Unidad Reguladora y de Control de Datos Personales. (2020). Revista Uruguaya de Protección de Datos Personales (N.º 5).

10: Baridon, M. (2009). La protección de datos personales en el contexto económico. Ciudad, Editorial.

11: Tosi Zás, M. L. (2010). Derecho informático. Montevideo: Facultad de Derecho, Universidad de la República.

12: Piñar Mañas, J. L. (2004). Guía del Derecho Fundamental a la protección de datos de carácter personal. Agencia Española de Protección de Datos.

13: Pérez Luño, A. (2006). La tercera generación de derechos humanos. Navarra, Madrid.

14: Schiavi, P. (2013). La protección de los datos personales en las redes sociales. Estudios de Derecho Administrativo N° 7.

15: Unidad Reguladora y de Control de Datos Personales. (2019, agosto). Revista de Protección de Datos Personales (4.ª ed.). URCDP.

16: Durán Martínez, A. (2012). Derecho a la protección de datos personales y al acceso a la información pública. Montevideo.

17: Schiavi, P. (2015). *Régimen jurídico de la acción de acceso a la información pública en el Uruguay*. Revista de Investigações Constitucionais, 2(2), página 137–168.

18: Schiavi, P. (2017). El derecho al olvido y a la protección de datos personales en Uruguay. Revista de Derecho de la Universidad de Montevideo, (31).

19: Rotondo, F., Delpiazzo, C. E., Mezzadri, E., & Ruanova, M. (2023). Aproximación sobre el derecho al olvido en Uruguay con jurisprudencia nacional y regional.

20: Acosta, L. (2023, junio 7). Derecho al olvido: Por primera vez, una sentencia judicial reconoció su aplicación en Uruguay. Abogados.com.ar. https://abogados.com.ar/index.php/derecho-al-olvido-por-primera-vez-una-sentencia-judicial-reconocio-su-aplicacion-en-uruguay/32416

21: Tribunal Europeo de Derechos Humanos (TEDH). (2008). I. v. Finland (Sentencia de 17 de octubre de 2008).

22: Unidad Reguladora y de Control de Datos Personales. (s.f.). Datos abiertos. https://www.gub.uy/unidad-reguladora-control-datos-personales/datos-y-estadisticas/datos-abiertos

23: Unidad Reguladora y de Control de Datos Personales. (s.f.). Datos abiertos. https://www.gub.uy/unidad-reguladora-control-datos-personales/datos-y-estadisticas/datos-abiertos

24: Unidad Reguladora y de Control de Datos Personales. (2021, diciembre). Memoria anual 2020. URCDP. https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/2021-12/Memoria%202020%20final.pdf

25: Guerra Pérez, W. (2005) “Hábeas data. Normas procesales. Primera lectura de la ley 17838”, en Revista de Derecho Público, n.o VII, Universidad Católica del Uruguay, p. 147. Texto extraído de: Gaiero Guadagna, B., & Soba Bracesco, I. M. (2010). El proceso de hábeas data en el Uruguay (protección de datos personales y acceso a la información pública). Anuario de Derecho Constitucional Latinoamericano, 325–350. http://biblioteca.corteidh.or.cr/tablas/r28363.pdf

26: Texto extraído de: Correa Freitas, R. (2005). Habeas data: Ley N° 17.838 de 24 de setiembre de 2004. Facultad de Derecho, Universidad de la República. Página 28. https://www.fder.edu.uy/medios/biblioteca/libros/habeas-data-ley-17838.pdf

27: Gaiero Guadagna, B., & Soba Bracesco, I. M. (2010). El proceso de hábeas data en el Uruguay (protección de datos personales y acceso a la información pública). Anuario de Derecho Constitucional Latinoamericano, 325–350. http://biblioteca.corteidh.or.cr/tablas/r28363.pdf

28: Vázquez Pedrouzo, C. (2011) El régimen jurídico del acceso a la información pública y la protección de datos personales. Revista de Derecho y Tribunales, Montevideo, v. 15, p.59-109, 2011. p. 61.

29: Delpiazzo, C. E. (2004). Aproximación a la ley uruguaya N° 17.838 sobre protección de datos personales y habeas data. Revista Chilena de Derecho Informático, (5). https://doi.org/10.5354/rchdi.v0i5.10742

BIBLIOGRAFÍA

- Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). (2024, 27 de diciembre). Eje 1. Gobernanza de datos. En Estrategia Nacional de Datos del Uruguay 2030. Uruguay. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-datos-2024-2030/ejes-tematicos/eje-1-gobernanza
- Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). (2025, enero). Estrategia Nacional de Datos del Uruguay 2030 [Política pública]. Uruguay.
- Baladán, F. (2018). Protección de datos personales y datos abiertos [PDF]. Unidad Reguladora y de Control de Datos Personales (URCDP). Recuperado de https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/noticias/urcdp---ley-de-proteccion-de-datos-personales.pdf
- Buquet, D. (2009). Uruguay 2008: de las reformas a la competencia electoral. Revista de Ciencia Política, 29(2), 611–632.
- Cayota, D. (2018, 5 de noviembre). Organismos del Estado incumplen la ley de protección de datos personales. El Observador. https://www.elobservador.com.uy/nota/organismos-del-estado-incumplen-la-ley-de-proteccion-de-datos-personales-2018511500
- Delpiazzo, C. E. (2003). Estado de la protección de datos personales en el Uruguay. Derecho Informático IV, 27.

- El País. (2012, 26 de setiembre). Cien denuncias por año por mal uso de bases de datos. El País. https://www.elpais.com.uy/informacion/cien-denuncias-por-ano-por-mal-uso-de-bases-de-datos
- Estrades, C., & Llambí, C. (2013). Lecciones de la crisis financiera de 2008: Respuestas de política a choques externos en Uruguay. The Developing Economies, 51(3), 233–331.
- Gaiero Guadagna, B., & Soba Bracesco, I. M. (2010). El proceso de hábeas data en el Uruguay (protección de datos personales y acceso a la información pública). Anuario de Derecho Constitucional Latinoamericano, 16, 325–349. Recuperado de https://www.corteidh.or.cr/tablas/r28363.pdf
- La Mañana. (2022). Ciberdelitos: el crimen entre lo oculto y lo indiscreto. Recuperado de https://www.xn--lamaana-7za.uy/actualidad/ciberdelitos-el-crimen-entre-lo-oculto-y-lo-indiscreto/
- Papa, G. (2009). La crisis global, sus impactos, respuestas de política económica y estrategias de desarrollo [Informe]. Fundación Friedrich Ebert.
- Pereiro Alonso, C. (2023, agosto). Protección de datos personales: 15 años de la Ley 18.331. Asociación de Estudiantes Universitarios (AEU). https://www.aeu.org.uy/aucdocumento.aspx?6450,15173
- Revista Chilena de Derecho Internacional. (2004). Aproximación a la ley uruguaya No. 17.838 sobre protección de datos personales y habeas data. Recuperado de https://revistas.uchile.cl/index.php/RCHDI/article/view/10742/10997
- Sartori, M. P. (2012, 14 de junio). El gobierno busca equilibrio entre tecnología y privacidad mientras aumentan consultas, denuncias por spam y por “derecho al olvido”. Búsqueda. https://www.busqueda.com.uy/Ediciones/El-gobierno-busca-equilibrio-entre-tecnologia-y-privacidad-mientras-aumentan-consultas-denuncias-por-spam-y-por-derecho-al-olvido--uc4685
- SAP. (s. f.). What is SAP Master Data Governance? En Master Data Governance | SAP Data Cloud. Recuperado de https://www.sap.com/spain/products/data cloud/master data governance/what is data governance.html
- Tuduri, A., & Jackson, M. (2022, 14 de marzo). Luces y sombras de la gobernanza de datos en Uruguay. Datysoc. Recuperado de https://datysoc.org/2022/03/14/luces-y-sombras-de-la-gobernanza-de-datos-en-uruguay/
- Unidad Reguladora y de Control de Datos Personales (URCDP). (2017). Guía: Criterios de disociación de datos personales [PDF]. Recuperado de https://www.gub.uy/unidad-reguladora-control-datos-

personales/comunicacion/publicaciones/guia-criterios-disociacion-datos-personales/guia-criterios-disociacion

- Unidad Reguladora y de Control de Datos Personales. (2020). Revista Uruguaya de Protección de Datos Personales (N.º 5). https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/Revista%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%2C%20edici%C3%B3n%202020.pdf
- Organización Internacional para las Migraciones. (s. f.). Tres desafíos vinculados a la protección y la privacidad de datos. IOM Blog. Recuperado de https://weblog.iom.int/es/tres-desafios-vinculados-la-proteccion-y-la-privacidad-de-datos

MARCO NORMATIVO

Declaración Universal de Derechos Humanos.
Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica.
Directiva 95/46/CE de 24 de octubre de 1995 del Parlamento Europeo.
Convenio N° 108 del Consejo de Europa.
Convenio N° 108+ del consejo de Europa
Constitución de la República Oriental del Uruguay.
Ley N° 9.155 de 04 de diciembre de 1933 – Código Penal.
Ley N° 15.982 de 14 de noviembre de 1988 – Código General del Proceso.
Ley Nº 17.838 de 24 de setiembre de 2004.
Ley N° 18.331 de 11 de agosto de 2008.
Ley N° 18.381 de 17 de octubre de 2008.
Ley N° 18.719 de 27 de diciembre de 2010.
Ley N° 18.996 de 07 de noviembre de 2012.
Ley N° 19.030 de 27 de diciembre de 2012.
Ley N° 19.286 de 25 de setiembre de 2014.
Ley N° 19.355 de 19 de diciembre de 2015.
Ley N° 19.438 de 14 de octubre de 2016.
Ley N° 19.670 de 15 de octubre de 2018.
Ley N° 19.889 de 09 de julio de 2020.
Ley N° 19.924 de 18 de diciembre de 2020.
Ley N° 19.948 de 16 de abril de 2021.
Ley N° 20.075 de 20 de octubre de 2022.
Decreto N° 664/008 de 22 de diciembre de 2008.

Decreto N° 414/009 de 31 de agosto de 2009.
Decreto N° 30/014 de 11 de febrero de 2014.
Decreto N° 54/017 del 20 de febrero de 2017.
Decreto N° 64/020 de 17 de febrero de 2020.
Resolución N° 989/010 de 30 de julio de 2010 de la URCDP.
Resolución N° 105/015 de 23 de diciembre de 2015 de la URCDP.
Resolución N° 68/017 de 26 de abril de 2017 de la URCDP.
Resolución N° 07/020 de 18 de febrero de 2020 de la URCDP.
Resolución N° 30/020 de 12 de mayo de 2020 de la URCDP.
Resolución N° 33/020 de 2 de junio de 2020 de la URCDP.
Resolución N° 35/020 de 9 de junio de 2020 de la URCDP.
Resolución N° 59/020 de 8 de diciembre de 2020 de la URCDP.
Resolución N° 23/021 de 8 de junio de 2021 de la URCDP.
Resolución N° 41/021 de 8 de setiembre de 2021 de la URCDP.
Resolución N° 52/021 de 7 de diciembre de 2021 de la URCDP.
Resolución N° 58/021 de 21 de diciembre de 2021 de la URCDP.
Resolución N° 32/024 de 10 de setiembre de 2024 de la URCDP.
Dictamen N° 10/010 de 16 de abril de 2010 de la URCDP.
Dictamen N°1/014 de 04 de febrero de 2014 de la URCDP.
Dictamen N° 5/019 de 23 de abril de 2019 de la URCDP.
Dictamen N° 4/021 de 23 de marzo de 2021 de la URCDP.
Dictamen N° 12/021 de 29 de junio de 2021 de la URCDP.
Dictamen N° 3/022 de 15 de marzo de 2022 de la URCDP.
Sentencia Definitiva Nº 1410/2023 de 21 de diciembre de 2023 dictada por la Suprema Corte de Justicia.
Sentencia Definitiva N° 193/2022 de Tribunal de Apelaciones Civil de 6° Turno de 3 de octubre de 2022.
Sentencia Nº 273/2010 del Tribunal de lo Contencioso Administrativo (TCA) del 1° de Setiembre de 2010
Informe N° 305/019 de 13 de setiembre de 2019 de la URCDP.

Normativa internacional:

Reglamento 2016/679 - 25 de mayo de 2018 - Parlamento de la Unión Europea.
Ley N° 19.628 - 26 de agosto de 1999 - Protección de la Vida Privada - Chile.
Ley N° 25.326 - 4 de octubre de 2000 - Ley de Protección de Datos Personales Argentina - Argentina.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares - 5 de Julio

de 2010 - México.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados - 26 de enero de 2017 - México.
Ley N° 13.709 - 15 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - Brasil.
Ley N° 27.699 - 30 de noviembre de 2022 - Protocolo Modificatorio del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal donde se ratificó el Convenio 108+ - Argentina.

ANEXOS

ANEXO 1: FORMULARIO PARA COMUNICAR UNA VULNERCIÓN DE SEGURIDAD DE DATOS PERSONALES - URCDP

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Anexo

Datos necesarios para la comunicación de vulneración de seguridad de datos personales

Los sujetos obligados a realizar las comunicaciones deberán completar los siguientes datos:

A. **Datos identificatorios de la persona o entidad que realiza la comunicación:**
   Nombre de la entidad/Nombres y apellidos
   Documento de identificación
   Calidad
   Dirección
   Teléfono
   Correo electrónico

B. **Datos identificatorios del responsable de la base de datos y del delegado de protección de datos personales en su caso:**
   Nombre de la entidad/Nombres y apellidos
   Documento de identificación
   Dirección
   Teléfono
   Correo electrónico
   Nombre del delegado de protección de datos personales
   Correo electrónico del delegado de protección de datos personales

C. **Datos identificatorios del encargado de tratamiento de datos personales (eventual):**
   Nombre de la entidad/Nombres y apellidos
   Documento de identificación
   Dirección
   Teléfono

D. **Datos identificatorios de la base de datos personales:**

Nombre de la base de datos

Ubicación de la base de datos

Número de inscripción de la base de datos en la URCDP (de corresponder)

Cantidad de personas que integran la base de datos

Tipos de datos personales que integran la base de datos

E. **Información temporal de la vulneración de seguridad**

Fecha de inicio (exacta, estimada, no conocida)

Fecha de detección (exacta, estimada, no conocida)

Circunstancias detalladas de su detección:

Si ya se inició el procedimiento para la resolución de la vulneración y sus razones en caso negativo

Si la vulneración ya está resuelta y su fecha de resolución:

Justificación de por qué se notificó tardíamente a la URCDP (después de las 72 horas - eventual)

F. **Información sobre la vulneración de de seguridad (descripción) :**

Referencia del incidente (ejemplos):

- Acceso o difusión no autorizados
- Modificación no autorizada
- Desaparición o pérdida
- Medio por el que se materializó
- Dispositivo perdido, robado o desechado
- Documentación perdida, robada, guardada en lugar no seguro, desechada
- Correo electrónico abierto o perdido
- Eliminación incorrecta de datos en papel
- Datos personales mostrados a la persona incorrecta

- Datos personales utilizados sin el consentimiento del titular
- Publicación no intencionada
- Error humano
- Revelación de datos personales en forma verbal no autorizada
- Datos personales enviados por error
- *Malware*, *Phishing*, o intrusión de un tercero ajeno
- Eliminación incorrecta de datos
- Datos personales enviados por error
- Otros

G. **Medidas preventivas que se realizaron antes de la vulneración:**

H. **Información acerca de los datos personales afectados**

- Datos básicos
- Datos sensibles
- Datos especialmente protegidos
- Datos de localización del titular
- Otros

I. **Información acerca de los titulares de los datos personales**

- Clientes
- Usuarios
- Suscriptores
- Alumnos
- Pacientes
- Otros
- Cantidad de titulares estimados que sus datos fueron vulnerados

J. **Posibles consecuencias de la vulneración (corresponde realizar un detalle de las consecuencias)**

K. **Medidas realizadas para minimizar el impacto de la vulneración (corresponde realizar un detalle de las medidas)**

L. **Comunicación a los interesados:**

Si se comunicó la vulneración de seguridad a los titulares de los datos vulnerados

Fecha en la que se informó o se tiene previsto informar

Número de personas a las que se informó o se tiene previsto informar

Medios o herramientas para la comunicación a los titulares

Justificación para no informar o motivos por los que no se ha informado a la fecha del informe

ANEXO 2: EJEMPLO DE CLAUSULA DE CONSENTIMIENTO INFORMADO

CLAUSULA DE CONSENTIMIENTO INFORMADO

De conformidad con la Ley Nº 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP), los datos suministrados a partir del (indicar fecha) por usted quedarán incorporados en la base de datos (indicar nombre), la cual será procesada exclusivamente para la siguiente finalidad: (indicar).

Los datos personales serán tratados con el grado de protección adecuado, tomándose las medidas de seguridad necesarias para evitar su alteración, pérdida, tratamiento o acceso no autorizado por parte de terceros.

El responsable de la Base de datos es (indicar) y la dirección donde podrá ejercer los derechos de acceso, rectificación, actualización, inclusión o supresión, es (indicar).

ACEPTO **NO ACEPTO**

ANEXO 3: FORMULARIO PARA EJERCER EL DERECHO DE ACCESO DE DATOS PERSONALES – URCDP

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Formulario para ejercer el derecho de acceso de datos personales

Montevideo, ...de.....de .....

Datos del responsable de la base de datos o del tratamiento

Nombre del responsable:.....
(Persona Física):.....
(Empresa Privada):.....
(Organismo Público):.....
Dirección.....
Ciudad.....Departamento.....
Teléfono.....
Correo electrónico.....

Datos del solicitante (titular de los datos personales)

Sr/Sr .....con domicilio en .....
.....Departamento.....C.P.....
Teléfono.....Correo Electrónico.....

Cédula de Identidad Nº.....de la que se adjunta fotocopia.

EJERCE POR ESTE MEDIO EL DERECHO DE: ACCESO, conforme a lo previsto en el artículo 14 de la Ley N° 18.331 de Protección de Datos Personales y Acción de "Habeas Data" de 11 de agosto de 2008, **SOLICITANDO:**

A) Se me proporcione en forma gratuita toda la información que sobre mi se encuentre en su/s base/s de datos o registro/s, en el plazo máximo de cinco (5) días hábiles a contar desde la recepción de esta solicitud. Vencido dicho plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas, quedará habilitada la acción de Habeas Data.
La referida información debe ser amplia y suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible.

B) Se me suministre la información, de acuerdo con los datos arriba indicados, de la siguiente manera:

Torre Ejecutiva Sur - Liniers 1324 Piso 4
Montevideo - Uruguay
gub.uy/urcdp

Uruguay Presidencia | agesic

Personalmente	Telefónicamente	Por correo electrónico	Otro (aclarar)

Firma del solicitante _____

El formulario debe completarse y presentarse en el organismo o empresa en el que desee ejercer el derecho.

ANEXO 4: FORMULARIO PARA EJERCER EL DERECHO DE RECTIFICACIÓN, ACTUALIZACIÓN, INCLUSIÓN O SUPRESIÓN DE DATOS PERSONALES - URCDP

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Formulario para ejercer el derecho de rectificación, actualización, inclusión o supresión de datos personales

Montevideo, ...de.....de .....

Datos del responsable de la base de datos o del tratamiento

Nombre del responsable:.....
(Persona Física):.....
(Empresa Privada):.....
(Organismo Público):.....
Dirección.....
Ciudad.....Departamento.....
Teléfono.....
Correo electrónico.....

Datos del solicitante (titular de los datos personales)

Sr/Sr .....con domicilio en .....
.....Departamento.....C.P.....
Teléfono.....Correo Electrónico.....
Cédula de Identidad Nº.....de la que se adjunta fotocopia.

Ejerce por este medio el derecho de:

Rectificación	Actualización	Inclusión	Supresión

conforme a lo previsto en el artículo 14 de la Ley Nº 18.331 de Protección de Datos Personales y Acción de "Habeas Data" de 11 de agosto de 2008, **SOLICITANDO:**

A) Se proceda en forma gratuita a efectuar en el plazo de cinco (5) días la:

Rectificación	Actualización	Inclusión	Supresión

de los datos relativos a mi persona, de acuerdo a la información que detallo al final de la presente solicitud. Vencido dicho plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas, quedará habilitada la acción de Habeas Data. Si el responsable de la Base de Datos considera que la rectificación, actualización, inclusión o supresión no procede, deberá informar dentro del plazo de cinco (5) días, las razones por la que estima no corresponde. B) Una vez realizada la rectificación, actualización, inclusión o supresión, se me comunique dicho extremo de la siguiente manera:

Personalmente	Telefónicamente	Por correo electrónico	Otro (aclarar)

Datos que deben:

Rectificarse	Actualizarse	Incluirse	Suprimirse

1).....
2).....
3).....
4).....

Firma del solicitante _____

El formulario debe completarse y presentarse en el organismo o empresa en el que desee ejercer el derecho.