

MÓDULO 2.

DERECHO A LA PRIVACIDAD/PROTECCIÓN DE DATOS PERSONALES

Diandra Céspedes S.

1. ¿QUÉ SON LOS DATOS PERSONALES Y POR QUÉ PROTEGERLOS?

Los derechos humanos tienen una evolución constante, por lo que en la *Era Digital* en la que nos desarrollamos, debemos entender que los derechos humanos también pueden ser ejercidos en ámbitos digitales. En ese sentido, “Los derechos digitales no son nada más que los derechos humanos, individuales y colectivos, pero aplicados a Internet” (Naranjo, Diego).

Así como tenemos diversos derechos humanos, también existirán diversos derechos digitales (derechos humanos en entornos digitales):

- Acceso universal e igualitario a Internet
- Libertad de expresión, información y comunicación.
- **Privacidad y protección de datos**
- Educación
- Propiedad intelectual
- Otros

2. LOS DATOS, EL NUEVO PETRÓLEO

A lo largo de los años, la información y los datos que se van generando han ido incrementando enormemente; así como se desarrolla la *Era Digital* también se dice que estamos en la *Era de los datos*.

De acuerdo al Banco Interamericano de Desarrollo¹, solo en el año 2012, se calcula que se crearon más datos que todos los datos producidos hasta la fecha en la historia de la humanidad. Durante el año 2018, produjimos 2,4 EB (Exabytes) de información cada día; que son 2,5 quintillones de bytes de datos o el número 25 seguido de 17 ceros.

1 BID. Curso Datos para la efectividad de las políticas públicas. Plataforma EDX. 2018.

El ritmo de producción de los datos se duplica cada dos años, creando cada vez más terabytes de datos por ser humano en el planeta. Debemos pensar cuántas fotos tomamos, publicaciones e interacciones en las redes sociales, las transacciones bancarias, etc.

Los datos son utilizados por las empresas y los gobiernos, y sirven para poder analizar comportamientos, mejorar servicios y tomar decisiones de política pública. Por ello se dice que los datos son el nuevo petróleo, porque a partir de los análisis de datos se han logrado consolidar diversas empresas y se han generado fuertes ingresos.

Al referirnos a datos vamos a hablar de alguna información o características de algo concreto, y pueden ser cosas como datos de distancia (Ej. Distancia desde la población x hasta la laguna y), hasta datos que pertenecen a las personas, los cuales se denominan como datos personales.

3. DATOS PERSONALES

Los datos personales son cualquier información que permita **identificar, localizar o contactar** de forma directa o indirecta a personas naturales.

Por ejemplo:

- Nombre.
- Dirección de domicilio.
- Edad.
- Lugar de estudio o trabajo.
- Años de experiencia laboral.

4. TIPOS DE DATOS PERSONALES

Existen diversos tipos de datos personales:

Datos Personales Generales: A los que se hacía referencia anteriormente.

Datos Personales Sensibles: Datos personales que se refieren a la esfera íntima de una persona y que pueden llevar a estigmatizaciones o discriminación.

Por ejemplo:

- | | |
|--|------------------------------------|
| • Origen racial o étnico | • Opiniones políticas |
| • Creencias o convicciones religiosas, filosóficas y morales | • Datos relativos a la salud |
| • Afiliación sindical | • Preferencia u orientación sexual |

Datos biométricos: Aquellos datos personales referidos a las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única.

Por ejemplo:

- Huella dactilar
- Reconocimiento facial
- Reconocimiento del iris
- Reconocimiento de la geometría de la mano
- Reconocimiento de retina
- Reconocimiento de voz
- Datos genéticos

5. SUJETOS INVOLUCRADOS EN EL TRATAMIENTO DE DATOS PERSONALES

Al momento de referirnos al tratamiento de datos personales, podemos identificar distintos sujetos involucrados:

- **Titular:** Persona natural sobre quien recae el derecho propietario (la titularidad y pertinencia) de los datos personales.
- **Responsables del Tratamiento de Datos Personales:** Son las personas naturales o jurídicas encargadas de obtener el consentimiento de los titulares de forma directa o indirecta y están a cargo de la recopilación, aplicación de medios de seguridad y tratamiento de datos personales, según corresponda. Se dividen en:
 - **Responsable:** Persona natural o jurídica privada, pública o mixta, que sólo o en conjunto con otros, define los fines, medios y realiza el tratamiento de datos personales a nombre propio, de forma directa o por intermedio de terceros encargados.
 - **Encargado:** Es la persona natural o jurídica privada, pública o mixta a la cual se delega el tratamiento de datos personales a nombre del responsable.

Una persona natural o jurídica podrá tener, al mismo tiempo, la condición de responsable o encargado.

6. MARCO JURÍDICO EN BOLIVIA

La mayoría de los países de la región cuenta con leyes sobre protección de datos personales, siendo Bolivia uno de los pocos que no cuenta con legislación específica.

Tabla 2: Países y leyes de protección de datos personales (LPDP)

PAÍS	¿TIENE LPDP?	¿TIENE AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES (APDP)?
Argentina	Sí, desde 2000	Sí
Brasil	Sí, desde 2020	Sí
Chile	Sí, desde 1999 *Nueva Ley aprobada por el Congreso el 2024. Su promulgación está pendiente.	No
Colombia	Sí, desde 2012	Sí
Costa Rica	Sí, desde 2011	Sí
Ecuador	Sí, desde 2021	Sí
México	Sí, desde 2010	Sí
Panamá	Sí, desde 2019	Sí
Paraguay	Sí, desde 2020	Sí
Perú	Sí, desde 2011	Sí
República Dominicana	Sí, desde 2013	No
Uruguay	Sí, desde 2008	Sí

FUENTE: CARLOS GUERRERO ARGOTE, PARA EL PROYECTO MARCOS LEGISLATIVOS DE DERECHOS DIGITALES MULTICULTURALES PARA COMUNIDADES INDÍGENAS Y MUNICIPIOS EN BOLIVIA: ANÁLISIS COMPARATIVO E INCIDENCIA LEGAL DE LA FUNDACIÓN INTERNETBOLIVIA.ORG. SE HAN AGREGADO MODIFICACIONES PROPIAS.

A pesar de que Bolivia no tiene una ley específica de protección de datos personales, existe normativa dispersa que se refiere de un modo u otro a la protección de datos personales.

La Constitución Política del Estado establece en su artículo 21 que:

Artículo 21. Las bolivianas y los bolivianos tienen los siguientes derechos:

(...)

2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad.

Y el artículo 130, se refiere a la **acción de protección de privacidad**, conocida como habeas data en otros países:

Artículo 130.I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

Así, existe un marco constitucional que determina que tenemos derecho a la privacidad e intimidad, los cuales también se desarrollan en ámbitos digitales. Además, la acción de protección de privacidad resguarda la autodeterminación informativa, debido a que cada una de nosotras es dueña de nuestros datos, y debemos ser quienes determinen qué se hace con ellos.

Otras disposiciones relacionadas con la protección de datos personales las podemos encontrar en:

1. Código Procesal Constitucional.
2. Código Civil.
3. Código Procesal Civil.
4. Código Penal.
5. Código de Procedimiento Penal.
6. Decreto Supremo N° 28168. Acceso a la Información del Poder Ejecutivo.
7. Ley N° 018 del Órgano Electoral Plurinacional.
8. Ley N° 026. Ley del régimen electoral.
9. Ley N° 164. Ley general de telecomunicaciones, tecnologías de información y comunicación.
10. Decreto Supremo No 2617. Reglamento de la Ley N° 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación, para el Sector Postal.
11. Decreto Supremo No 1391. Reglamento General a la Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, para el Sector de Telecomunicaciones.
12. Decreto Supremo N° 1793. Reglamento a la Ley N° 164, para el Desarrollo de Tecnologías de Información y Comunicación.
13. Decreto Supremo N° 2514. Creación AGETIC.
14. Decreto Supremo N° 3251.
15. Decreto Supremo N° 3525.

16. Ley N° 1488. Ley de ciudadanía digital.
17. Ley 548. Código Niña, Niño y Adolescente.
18. Decreto Supremo N° 2377. Reglamento al Código Niña, Niño y Adolescente.
19. Ley N° 393 "Ley de servicios financieros".
20. Ley N° 453 "Ley General de los derechos de las usuarias y los usuarios y de las consumidoras y los consumidores".
21. DECRETO SUPREMO N° 2130. Reglamento a la Ley N° 453, de 4 de diciembre del 2013, General de Derechos de las Usuarias y los Usuarios, las Consumidoras y los Consumidores.
22. RM Ministerio de Justicia 68-09. Reglamento de Procedimientos de Atención y Gestión de Reclamos del Viceministerio de Defensa de los Derechos del Usuario y del Consumidor.

Hay que considerar que el tratamiento de datos personales no se restringe a los límites nacionales.

A nivel país, distintas instituciones públicas y privadas manejan nuestros datos. Pero además, los datos personales también son tratados a nivel internacional a partir de las interacciones que hacemos con plataformas de internet y redes sociales: Facebook, Instagram, YouTube, Ebay, entre otros.

Por ello, contar con una normativa nacional permite tener mayores posibilidades de insertarse en debates internacionales para crear marcos regulatorios que sean aplicables a más de un país.

7. ANTEPROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES DE LA AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (AGETIC)

La Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) está trabajando un anteproyecto de ley de protección de datos personales. El documento tiene los lineamientos que se manejan de forma internacional y considera los aspectos establecidos en el Reglamento General de Protección de Datos de la Unión Europea. Puede revisar la última versión pública en el siguiente enlace: <https://www.dataguidance.com/sites/default/files/agetic.pdf>

A pesar de que es un avance importante, existen aspectos que pueden ser mejorados; por ello, La Fundación InternetBolivia.org, la Asociación Civil de Desarrollo Social y Promoción Cultural Libertad (ADESPROC – Libertad), Wikimedia Bolivia y Access Now, realizaron algunas observaciones y recomendaciones:

- a. Incluir la identidad de género dentro de la tipificación de datos sensibles.
- b. El reconocimiento del consentimiento informado en un artículo específico como condición para el tratamiento de datos personales.
- c. La adición del principio de minimización y plurinacionalidad.
- d. Incluir el derecho de las personas trans o hacer énfasis en que la rectificación de sus datos sea garantizada como derecho fundamental.
- e. Reconsiderar la mención a casos o excepciones en los que no procede el ejercicio de los derechos pues los mencionados en la propuesta son aún de muy amplio alcance e interpretación, pudiendo convertirse así en un riesgo al ejercicio de los Derechos Humanos.
- f. Establecer en un artículo específico las condiciones para la legalidad del tratamiento.
- g. Incluir los procedimientos para la elección de la Autoridad de protección de datos para garantizar la autonomía del cargo.
- h. Señalar que la notificación de violaciones seguridad de datos a sus titulares sea obligatoria en cualquier caso, sin importar la magnitud o el esfuerzo que conlleve.

El anteproyecto aún no ha sido presentado ante la Asamblea Legislativa y no se tiene novedades sobre nuevos cambios realizados.

8. DERECHOS DE PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales implica una serie de derechos:

- **Derecho de acceso:** El titular tendrá el derecho de solicitar el acceso a los datos personales que estuviesen en posesión del responsable, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento.
- **Derecho de rectificación y actualización:** el titular tendrá el derecho a obtener del responsable, la rectificación, corrección o actualización de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.
- **Derecho de cancelación:** el titular tendrá derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

- **Derecho de oposición:** el titular podrá oponerse al tratamiento de sus datos personales cuando:
 - Tenga una razón legítima derivada de su situación particular.
 - El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa.
- **Derecho a la portabilidad de los datos personales:** cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.
- **Derecho a no ser objeto de decisiones individuales automatizadas:** el titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana.
- **Derecho a la limitación del tratamiento de los datos personales:** el titular tendrá derecho a que el tratamiento de datos personales se limite al plazo y finalidad otorgado en el consentimiento para ello.
- **Derecho a la información:** el titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparente por cualquier medio sobre:
 - Los fines del tratamiento;
 - La base jurídica para el tratamiento;
 - Tiempo de conservación;
 - El origen de los datos personales cuando no se hayan obtenido directamente del titular; Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá: dirección del domicilio legal, número de teléfono y correo electrónico;
 - La posibilidad de revocar el consentimiento;
 - Entre otros aspectos
- **Derecho de indemnización:** el titular tiene derecho a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación a cualquiera de los derechos sobre protección de datos personales.

9. INTELIGENCIA ARTIFICIAL Y PRIVACIDAD

No existe una definición universalmente aceptada de Inteligencia Artificial; sin embargo, podemos considerar a la misma como el tipo de tecnología que crea sistemas que puedan realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento y la percepción. La inteligencia artificial, o IA, permite que las computadoras simulen capacidades humanas de resolución de problemas.

Para realizar estas tareas, la IA utiliza datos, de ahí su relación con la protección de datos personales. Los datos que se le brindan a los sistemas de IA, son analizados de acuerdo a los parámetros programados, y es en base a ellos que se resuelven los problemas o tareas planteadas.

A pesar de que la IA es una tecnología interesante, hay que considerar que aún es muy limitada y que sólo puede realizar tareas muy concretas.

Además, que detrás del funcionamiento de la IA, existen diferentes temas que deben ser considerados: los datos, cómo son obtenidos los datos, las relaciones verticales en el desarrollo y uso de la IA, los impactos ambientales, las condiciones laborales, entre otros.

Al basarse en el análisis de datos, la IA debe tener consideraciones respecto a la privacidad y la protección de datos personales. Aún existen vacíos legales respecto a cómo se regulará el desarrollo y uso de la IA, y es importante tener una visión crítica y buscar soluciones para que pueda usarse como una herramienta que fortalezca las actividades humanas y no se convierta en una amenaza a los derechos de las personas.

Un ejemplo reciente es cómo META ha determinado a través de cambios en su política de privacidad, el uso de datos de usuarios de Instagram y Facebook para entrenar su inteligencia artificial. Esta determinación ha sido suspendida en la Unión Europea debido a su normativa en protección de datos personales; no obstante, en otros lugares, continúa.

Mientras no se tengan regulaciones concretas para la IA, la normativa sobre protección de datos personales puede aplicarse a estos sistemas para garantizar los derechos de las personas.

10. CASOS DE VULNERACIONES CONTRA LA PRIVACIDAD

El uso de datos, implica tanto beneficios como riesgos. Entre los riesgos, se pueden tener casos en los que hayan filtraciones o usos no autorizados que pueden implicar vulneraciones a diferentes derechos.

En Bolivia han existido casos de vulneraciones contra la protección de datos personales relacionados con:

- a. Búsqueda de la implementación de una cédula de identidad digital sin considerar que no se tiene un marco legislativo para la protección de datos personales.
- b. Uso indiscriminado de cámaras de reconocimiento facial en unidades educativas.
- c. Casos de robos bancarios virtuales realizados a través del uso no autorizado de datos personales para suplantar temporalmente líneas de celulares de las personas afectadas, y así, realizar retiros y transferencias de dinero.
- d. Exposición de datos de salud por parte de autoridades y entidades públicas.
- e. Exposición de videos y/o fotografías de carácter sexual, reales y simulados, utilizando la filtración de datos personales como forma de violencia de género.
- f. Ciberestafas que realizan por medio de Whatsapp con el crackeo de cuentas.
- g. Publicación no autorizada de datos personales obtenidos en la aplicación Grindr, que incluyen datos de salud.
- h. Utilización de datos personales para la inscripción no autorizada de personas en partidos políticos.

11. RECOMENDACIONES DE POLÍTICA PÚBLICA

Es importante poder abordar la protección de datos personales, que se relaciona con muchos derechos, de forma responsable. Como fue mencionado, los datos personales están siendo cada vez más usados, lo que puede permitir que se tomen decisiones informadas, puede hacer que las políticas públicas se basen en evidencia, mejorar servicios, etc. Sin embargo, se debe tener un marco robusto de protección a los derechos de las personas.

Por ello, se recomienda:

- a. El debate y la aprobación de una ley de protección de datos personales (LPDP).
- b. Que a partir de la aprobación de la LPDP, se pueda planificar de forma estratégica la implementación plena de un gobierno digital.

- c.** La incorporación del Estado en los debates internacionales en protección de datos personales, para hacer frente a posibles malos usos de los datos personales por parte de empresas transnacionales, considerando que su actuación va más allá de nuestras fronteras nacionales.
- d.** Que cualquier normativa o política pública tenga como eje central el respeto irrestricto a los derechos de las personas.
- e.** La participación activa de la población en la creación de leyes y políticas públicas relacionadas con la protección de datos personales.
- f.** Realizar procesos de capacitación y concientización sobre la relevancia de la protección de datos personales.

A pesar de no contar con una normativa expresa para la protección de datos personales, existen también buenas prácticas que como personas, organizaciones o instituciones podemos implementar:

- a.** Brindar información comprensible, accesible y confiable sobre el proceso de recolección, tratamiento y publicación/difusión de datos personales.
- b.** Establecer qué datos se recolectan.
- c.** Indicar el propósito de esta recolección de datos.
- d.** Establecer quiénes van a tener acceso a estos datos y qué datos se harán públicos.
- e.** Determinar el tiempo que se van a almacenar los datos.
- f.** Indicar la forma en la que se puede acceder, cambiar, borrar los datos; es decir, la forma en la que se pueden ejercer los derechos de protección de datos personales.
- g.** Determinar canales de contacto para hacer preguntas relacionadas con la privacidad y protección de datos personales.
- h.** Idealmente, toda la información mencionada debe ser accesible siempre en los sitios webs u otras plataformas digitales que se utilicen.