



GUÍA PARA UNA MEJOR

# PROTECCIÓN DE DATOS PERSONALES



Esta guía fue elaborada por la Fundación InternetBolivia.org y Asociación Aguayo con apoyo del Fondo Indela.

Esta obra está disponible bajo licencia Creative Commons Attribution 4.0 Internacional (CC BY 4.0):  
<https://creativecommons.org/licenses/by/4.0/deed.es>



## GUÍA PARA UNA MEJOR

# PROTECCIÓN DE DATOS PERSONALES

El acceso cada vez más amplio a Internet, el masivo uso de redes sociales y la digitalización de servicios públicos y privados está estrechamente ligado al uso de datos personales, estos datos, al ser utilizados irregularmente, puede vulnerar derechos de la ciudadanía y atentar contra su seguridad.

Ante esta situación, gobiernos de varios países están fortaleciendo sus normativas para la protección de datos personales, al tiempo que las personas están tomando acciones para cuidar sus datos, pero ¿qué son los datos personales y cómo se pueden proteger?

---

## ¿QUÉ SON LOS DATOS PERSONALES?



Un dato es una representación simbólica (numérica, alfabética, espacial, etc.), por ejemplo, una letra, un número, una línea, etc. Un dato en solitario probablemente no nos dice mucho, pero cuando estos datos se juntan unos con otros, se procesan y se analizan adquieren un significado y por tanto un valor.

Estos datos pueden ser personales y no personales. Los datos no personales son aquellos que no identifican a una persona física o no proporcionan elementos suficientes para averiguar la identidad de la persona física, con por ejemplo un árbol, el nombre de una población, el clima.

En cambio, los datos personales son aquellos que sí permiten identificar, localizar o contactar a una persona física. Estos datos pueden ser numéricos, como el número de carnet; alfabéticos, como los nombres y apellidos de una persona; fotográficos, como una selfi, biométricos, como la huella digital, entre otros. Estos datos tienen un valor y, por tanto, deben estar bien cuidados.

# CUÁLES SON LOS

# DATOS PERSONALES

## GENERALES

Información que permite identificar, localizar o contactar de forma directa o indirecta a personas naturales:

- Nombre completo
- Dirección de domicilio.
- Edad.
- Carnet de identidad.
- Fecha de nacimiento
- Estado civil
- Firma
- Correo electrónico
- Número de celular

## SENSIBLES

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

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

## BIOMÉTRICOS

Referidos a las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única.

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

## ¿A QUIÉNES INTERESA LOS DATOS PERSONALES?

Cada día, plataformas digitales como Google, Facebook, Youtube, Tiktok recolectan un gran volumen de datos personales que procesan y analizan para luego mostrarnos publicidad según nuestros intereses, por eso no es raro que busquemos un producto de belleza un día y horas más tarde, mientras navegamos en nuestra red social, aparezca publicidad sobre productos de belleza. Aquí también entran empresas privadas que utilizan nuestros datos personales a cambio de servicios, es el caso de nuestras cuentas bancarias, registro y activación de un teléfono celular, etc.

Los Estados y gobiernos también utilizan nuestros datos personales para ofrecernos servicios como trámites, consulta de información o diseño de políticas. Uno de los más conocidos es el trámite de cédula de identidad, cuyos datos están digitalizados. El tema es que estos datos pueden ser mal utilizados por los gobiernos por ejemplo para controlarnos o acosarnos.

Por último, los delincuentes también se interesan por nuestros datos personales para cometer delitos, por ejemplo, para trata y tráfico, acceso a nuestra cuenta bancaria, chantaje, entre otros.

Por eso es que **el acceso inescrupuloso a nuestros datos personales puede tener consecuencias directas sobre nuestra seguridad.**

# EJEMPLOS DE VULNERACIÓN DE DATOS PERSONALES

En Bolivia ya ocurrieron varios casos de vulneración de datos personales, veamos un par de ejemplos:



## Caso 1: Inscripción de militantes de partidos políticos

### RESUMEN DEL CASO

El año 2018, tras la habilitación de la aplicación “Yo participo”, que permite verificar la militancia política, llovieron reclamos, debido a que cientos de ciudadanos, figuraban como militantes en una organización política a la que, aseguraban, no haberse afiliado. Entre los afectados se encontraban incluso figuras públicas, quienes manifestaron la molestia y el abuso que significaba que hayan usado sus datos para realizar una inscripción a un partido político, cuando ellos nunca dieron su consentimiento.

Dicha situación pudo deberse a que los partidos aprovecharon las firmas de los ciudadanos en actividades democráticas, como la colecta de firmas, participación en debates o apoyo a revocatorios y las inscribieron en alguna organización partidaria.

Las personas afectadas por el erróneo registro, tuvieron que apersonarse a oficinas de los Tribunales Electorales Departamentales para llenar un formulario que les permita depurarse de estas listas.

### DERECHOS VULNERADOS Y NATURALEZA DE LOS DATOS

#### DERECHOS:

- Autodeterminación informativa (Se vincula con varios derechos, no se encuentra expreso en la CPE)
- Honra, honor y reputación (CPE. Art. 21, numeral 2)
- Libertad de pensamiento y expresión (CPE. Art. 21, numeral 3)
- Libertad de asociación (CPE. Art. 21, numeral 4)
- Derechos políticos (CPE. Art. 26)

#### TIPO DE DATOS:

Datos personales: nombre, fecha de nacimiento, firma (utilizados sin consentimiento para una inscripción de militancia política).

### FIGURA LEGAL APLICABLE

#### ÁREA ADMINISTRATIVA

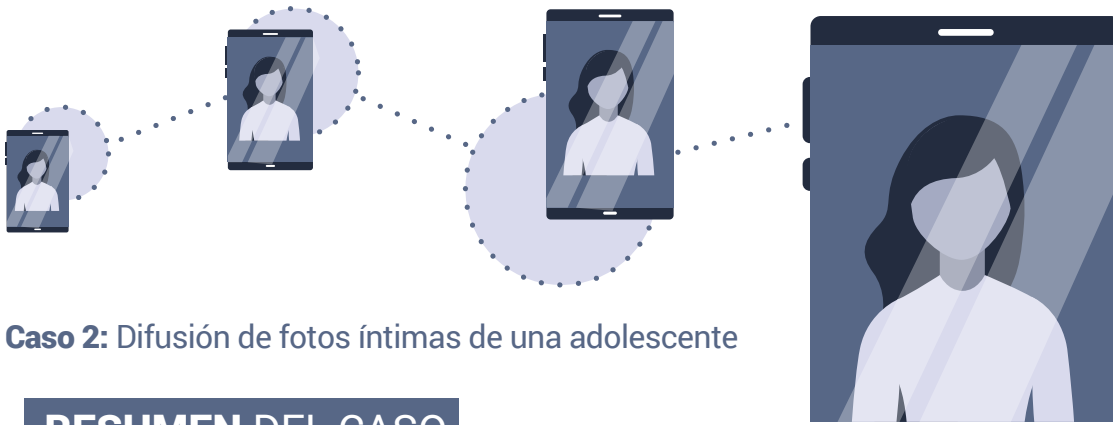
- Solicitud de anulación de registro de organizaciones políticas.

#### ÁREA PENAL

- Falsedad material (Código penal, art. 198) o falsedad ideológica (Código penal, art. 199) (Si existió algún tipo de falsificación).

#### ÁREA CONSTITUCIONAL

- Acción de protección de privacidad (Código Procesal Constitucional, art. 58 y siguientes).



## Caso 2: Difusión de fotos íntimas de una adolescente

### RESUMEN DEL CASO

Una adolescente se creó una cuenta en Facebook y con el tiempo hizo amistad con un hombre que utilizaba una cuenta falsa.

Esta persona enamoró a la menor y consiguió que ella le enviara fotos íntimas además de su usuario y contraseña de Facebook. Un día el hombre accedió a la cuenta en Facebook de la menor y publicó sus fotos íntimas, que fueron vistas por sus familiares, sus amigos y conocidos.

### DERECHOS VULNERADOS Y NATURALEZA DE LOS DATOS

#### DERECHOS:

- Derechos de las niñas, niños y adolescentes (CPE. Art. 58)
- Prohibición de toda forma de violencia contra las niñas, niños y adolescentes, (CPE. Art. 61)
- Privacidad e intimidad (CPE. Art. 21, numeral 2)
- Propia imagen (CPE. Art. 21, numeral 2)
- Honra, honor y reputación (CPE. Art. 21, numeral 2)
- Protección contra la violencia de género (CPE. Art. 15, parágrafo II y III)
- Integridad psicológica (CPE. Art. 15, parágrafo I)
- Derechos sexuales (CPE. Art. 66)

#### TIPO DE DATOS:

Datos biométricos, por tratarse de imágenes que permiten identificar a las personas, en este caso, una adolescente.

### FIGURA LEGAL APLICABLE

#### ÁREA PENAL

- **Alteración**, acceso y uso indebido de datos informáticos (Código Penal, art. 363 ter)
- **Pornografía** (Código Penal, art. 323 bis), con agravante por tratarse de una niña, niño o adolescente.
- **Grooming** (No se encuentra en el Código Penal).

#### ÁREA CONSTITUCIONAL

- Acción de protección de privacidad (Código Procesal Constitucional, art. 58 y siguientes).

## ¿QUIÉN DEBE PROTEGER NUESTROS DATOS PERSONALES Y CÓMO?

Como garante de la seguridad y del monopolio de la fuerza, los Gobiernos tienen el deber de garantizar la protección de nuestros datos personales.

Según la Constitución Política del Estado, las bolivianas y los bolivianos tenemos derecho a la privacidad, intimidad, honra, honor, propia imagen y dignidad (Art. 21 CPE). Asimismo, contamos con la Acción de protección de privacidad, que puede interponerse cuando una persona sea impedida de conocer, objetar u obtener la eliminación o rectificación de los datos

registrados en medios físicos o digitales. También existen artículos en leyes, decretos supremos y resoluciones, pero no es suficiente.

Bolivia debería contar con una Ley de Protección de Datos personales que establezca por ejemplo a quién le pertenecen esos datos, cómo se protegen, cómo la ciudadanía puede ejercer un control sobre sus datos, quién es el responsable de protegerlos, qué sucede cuando se vulneran, etc.

## ¿CÓMO PODEMOS CUIDAR NUESTROS DATOS PERSONALES?

Si bien el gobierno y las empresas utilizan nuestros datos para brindarnos servicios, es la ciudadanía la que sigue siendo propietaria de sus datos. Por lo tanto, todas las entidades públicas o privadas que quieran usar nuestros datos, deberían pedirnos nuestro consentimiento antes de hacerlo.

Además, deberían garantizarnos una adecuada gestión de nuestros datos aplicando los denominados derechos ARCO, es decir el derecho a acceder, rectificar, cancelar y oponernos al tratamiento de nuestros datos personales si así lo queremos. Este es uno de los caminos para ejercer este derecho.

## ¿EN QUÉ CONSISTEN LOS DERECHOS ARCO?

**Derecho de Acceso.** Este derecho nos permite conocer qué entidad privada o de gobierno tiene o trata nuestros datos, además que nos permite obtener una copia de ese archivo. Un ejemplo podría ser el acceso a nuestro historial médico, algo que en la actualidad es difícil de hacer y muchas veces es negado.

**Derecho de rectificación.** Los datos personales que manejan estas entidades deben ser exactos, por tanto, este derecho nos da la posibilidad de corregir y actualizar los datos personales que estén almacenados en bases de datos, por ejemplo, si existe un o más datos erróneos en el formulario de Registro Único de Estudiantes (RUDE) que facilita el Ministerio de Educación o cualquier otro trámite, deberíamos tener los mecanismos para corregirlo.

**Derecho a la cancelación.** Así como damos nuestro consentimiento para que nuestros datos sean tratados, este derecho permite solicitar la cancelación o supresión de datos personales de los archivos, registros, expedientes o sistemas donde se encuentran. Por, ejemplo, en Bolivia, cuando una persona ya ha cumplido su condena y pasa una cantidad de años, puede pedir la cancelación de sus antecedentes penales.

**Derecho de oposición.** Este derecho permite a las personas oponerse a la recolección o tratamiento de su información personal bajo una razón legítima. Esto caso aplicaría más a las empresas privadas, por ejemplo, si un servicio pide varios datos personales y considero que uno de ellos es innecesario, puedo oponerme a dárseles.



## ¿PUEDEN LOS GOBIERNOS MUNICIPALES PROTEGER NUESTROS DATOS PERSONALES?

Al igual que el gobierno nacional, los gobiernos municipales prestan servicios que utilizan datos personales, es el caso del pago de impuestos (RUAT), catastro, sistema de ventanilla única, sistema de cámaras de vigilancia, entre otros. Aunque estos servicios se utilizan y están cada vez más digitalizados, no es costumbre de los gobiernos municipales determinar aspectos con relación a la protección de datos personales de la ciudadanía.

En este marco, la elaboración y vigencia de leyes municipales concretas que regulen la protección de datos personales en los trámites de los gobiernos autónomos municipales permitiría garantizar los derechos de la ciudadanía, se tendría una visión clara sobre las responsabilidades en el tratamiento de datos personales y se contribuiría a prevención de incumplimiento de deberes por parte de los funcionarios públicos.