La protección de datos personales desde un enfoque de derechos

Dirección Nacional de Protección de Datos Personales.
Agencia de Acceso a la Información Pública (AAIP),
Jefatura de Gabinete de Ministros

Usar una red social, hacer una compra online, suscribirse a un diario o pagar las cuentas, son acciones digitales que forman parte de nuestra vida cotidiana y en donde cedemos (a veces sabiendo y otras veces no) información personal. Ahora bien, ¿qué son los datos personales? ¿Qué riesgos hay cada vez que compartimos datos? ¿Qué derechos y obligaciones existen en materia de protección de datos personales en nuestro país?

Para empezar, cuando hablamos de datos personales nos referimos a toda aquella información que pueda identificar o hacer identificable a una persona. En este sentido, existen diferentes categorías de datos personales, que implican a su vez diferentes niveles de riesgos.

Están por un lado aquellos datos personales, como pueden ser el domicilio, teléfono, DNI, información crediticia, imagen, etc. Por otro lado, están los datos sensibles, que son aquellos que requieren mayor nivel de protección y cuidado. Se trata de la información vinculada a la intimidad de una persona, que, a partir de un uso indebido, pueda dar origen a discriminación o afectar su integridad. Ejemplos de este tipo de datos son el género, la orientación sexual, afiliación sindical, opiniones partidarias o bien información que revele aspectos como origen étnico, creencias o convicciones religiosas, filosóficas y morales. Los datos genéticos y biométricos son los que pueden revelar información sobre la fisiología y la salud de las personas y se los considera como datos sensibles cuando identifican de manera unívoca a una persona física y pueden revelar información que sea relativa a su salud o fisiología o si su uso pueda resultar potencialmente discriminatorio para esa persona (Resolución 255/2022).

Ahora bien, una característica central de la era digital en la que vivimos, es que con el avance de las nuevas tecnologías y el desarrollo de la Inteligencia Artificial (IA), este

tipo de datos ya no sólo son recolectados, sino también inferidos, analizados y utilizados de forma automatizada para la elaboración de perfiles y la toma de decisiones. En este marco, es que la protección de datos personales se ha posicionado como un tema de agenda prioritaria y una preocupación compartida por parte de la ciudadanía y también por empresas y gobiernos.

Un ejemplo para pensar cómo opera la inferencia de datos en Internet, puede ser la publicidad personalizada. Cuando navegamos por la web, utilizamos motores de búsqueda o compartimos información en redes sociales, generamos una gran cantidad de datos, que incluyen preferencias, intereses, ubicación geográfica y comportamiento en línea. Las empresas, en este caso, utilizan algoritmos avanzados para procesar esa información en tiempo real e inferir preferencias o intereses a partir de las cuales pueden orientar la publicidad para cada público específico.

Sin embargo, esta capacidad de inferir datos que pueden tener a su alcance sectores tanto del ámbito público como el privado, plantea cuestiones importantes acerca de la privacidad y la seguridad de los datos. Cómo operan los algoritmos, qué razonamiento hacen, qué tipo de tratamiento y con qué finalidad, son sólo algunas de las preguntas que aparecen. A medida que las tecnologías continúan evolucionando, resulta fundamental contar con leyes y regulaciones que permitan abordar estos desafíos, brindando nuevas herramientas de empoderamiento a la ciudadanía y preservando sus derechos fundamentales.

Por eso, en un mundo cada vez más conectado, es muy importante conocer cuáles son los riesgos asociados de compartir información de tipo personal así como también saber cuáles son los derechos en relación a la privacidad de datos, para tomar decisiones más informadas.

Cambiar de paradigma: de la protección de los datos, a la protección de las personas

En Argentina, la protección de los datos personales es un derecho constitucional desde la reforma de 1994. La privacidad y la seguridad de los datos personales están protegidas por la Ley 25.326 que establece los principios, derechos y obligaciones para el correcto tratamiento de datos personales. Se trata de una ley sancionada en el año 2000 y que fue pionera en América Latina ya que sentó las bases regulatorias para garantizar que todas las personas puedan controlar la información personal que se encuentra en bases de datos públicas o privadas.

A pesar de haber significado un hito relevante, esta legislación presenta ciertas limitaciones a la hora de regular el tratamiento de datos personales, precisamente por la velocidad y la magnitud de los cambios tecnológicos que se han sucedido en este tiempo. Basta pensar cuáles eran los celulares que existían en el año 2000 (limitados a llamadas y mensajes de texto) y qué capacidad de procesamiento tienen los celulares hoy.

Es por esto que desde la Agencia de Acceso a la Información Pública se trabajó en un Proyecto de Ley de Protección de Datos Personales, que introduce cambios significativos para abordar estas transformaciones tecnológicas. En primer lugar, este proyecto propone un cambio de paradigma: pasar de un modelo de protección de los datos personales a un modelo de protección de las personas titulares de esos datos. En este sentido, el foco está en el derecho a la autodeterminación informativa, esto es, "el derecho a decidir o autorizar de forma libre, previa, expresa e informada la recolección, uso o tratamiento de los datos personales, así como de conocer, actualizar, rectificar, suprimir o controlar lo que se hace con la información" (Proyecto de Ley de Protección de Datos Personales, 2023). Además, el proyecto contempla algunos principios clave como la responsabilidad proactiva y demostrada, que es un eje transversal que acompaña el cambio de paradigma. Este principio tiene que ver con la exigencia hacia los responsables o encargados del tratamiento de datos, para que implementen medidas técnicas y procesos documentados que lleven al cumplimiento de la ley de forma previa y durante el tratamiento.

En síntesis, esto marca la necesidad de que los responsables adopten un comportamiento proactivo en relación al tratamiento de datos, incorporando buenas prácticas al interior de la empresa u organización, las cuales deben ser demostradas. También se incorpora el principio de neutralidad tecnológica, que permite mantener la vigencia de la ley más allá de los avances tecnológicos que sucedan a futuro y el principio de preeminencia, que sostiene que ante dudas interpretativas en la aplicación, prevalecerá la interpretación más favorable a la persona titular de los datos personales.

A continuación, destacamos cinco puntos relevantes del Proyecto de Ley:

1. Se incorporan nuevos derechos: oposición, decisiones automatizadas y elaboración de perfiles, revisión humana, portabilidad y limitación.

- El derecho a oposición implica que la persona puede oponerse al tratamiento de datos personales o a una finalidad específica, si no ha prestado consentimiento.

- Se incorpora el concepto de "decisiones automatizadas" para referirse al tratamiento de datos realizado por tecnologías que utilizan Inteligencia Artificial (IA). De esta manera, según lo indica el artículo 31 del proyecto de ley, las personas "tienen derecho a no estar sujetas a decisiones basadas en algoritmos o perfiles automatizados que puedan tener efectos significativos sobre ellas." (Proyecto de Ley de Protección de Datos Personales, 2023)

- La persona interesada tiene derecho a solicitar la revisión por una persona humana de las decisiones tomadas de manera automatizada o semiautomatizada que afecten a sus intereses, incluidas las decisiones encaminadas a definir aspectos personales, profesionales, de consumo, de crédito, de personalidad u otros.

- El derecho a la portabilidad refiere al derecho a obtener una copia de los datos personales proporcionados al Responsable de tratamiento o que sean objeto de tratamiento, en un formato que le permita su ulterior utilización por parte de otro Responsable de Tratamiento.

- El derecho a la limitación supone que por pedido de la persona interesada (y de acuerdo a una serie de condiciones que detalla el proyecto de ley) sus datos personales pueden dejar de ser tratados.

2. Se incorpora la aplicación extraterritorial. En la actualidad, el tratamiento de datos es global: los datos se recopilan en un lugar, se almacenan en otro y se procesan en otra parte del mundo, sin que las empresas cuenten necesariamente con oficinas radicadas en el país. Esta información personal merece protección y por eso este proyecto incorpora la posibilidad de fiscalizar a los responsables o encargados de las empresas en base a la ley argentina.

3. Reglas claras y seguras para la transferencia internacional de datos. Se trata de un eje clave para el comercio internacional y la geopolítica, que propone tres formas de transferencias: para los países con legislación adecuada (hay una evaluación a cargo de la Agencia), las garantías apropiadas y los supuestos de excepción.

4. Tratamiento de datos de niños, niñas y adolescentes. Se añade un artículo específico dedicado a la protección especial de los datos de las infancias y adolescencias, que reconoce como válido el consentimiento desde los 16 años en adelante y refuerza deberes de los responsables de tratamiento, entre otros aspectos.

5. Obligación de notificar incidentes de seguridad. Si bien la legislación contempla el principio de seguridad de los datos donde indica que los responsables del tratamiento deberán adoptar medidas de ciberseguridad para garantizar la protección y confidencialidad de los datos personales, este proyecto de ley añade la obligación de notificar cualquier tipo de incidente de seguridad a la autoridad de aplicación (AAIP) dentro de las 72 horas de haber tomado conocimiento del hecho.

Medidas para proteger la privacidad y seguridad de tus datos personales

En la actualidad, la Ley de Protección de Datos Personales, contempla una serie de principios y derechos que es fundamental conocer para proteger la privacidad y seguridad de los datos personales. Por un lado, los datos tratados deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. ¿Qué significa esto? Significa que los datos siempre tienen que ser correctos, veraces, estar actualizados, y deben ser los mínimos e indispensables para realizar la actividad o finalidad declarada por el responsable. Además, una vez cumplida la finalidad y el plazo de conservación, deben ser destruidos.

Para que el tratamiento se realice conforme a la Ley (sea lícito), quien trate los datos deberá registrarse como responsable ante la AAIP y declarar las bases de datos en su poder. Esto permite que las personas puedan contar con información disponible sobre en qué bases están inscriptas, para qué se utilizan los datos, por cuánto tiempo los conservan y cuáles son los canales habilitados para ejercer sus derechos. Para esto, se puede consultar el **buscador web del Registro Nacional de Bases de Datos Personales.**

Por otra parte, la normativa argentina establece en su artículo 9 el principio de seguridad de los datos, donde indica que quienes traten datos personales deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales. Por esto, la Agencia de Acceso a la Información Pública emitió la **Resolución 47/18** que contiene recomendaciones sobre estas medidas, para administrar, planificar, controlar y mejorar la seguridad al procesar datos personales. Esta resolución anima a los responsables a tomar medidas que prevean los posibles riesgos y a documentar y rendir cuentas sobre los procesos, de manera que puedan transparentar las iniciativas llevadas a cabo para proteger los datos personales.

La integridad y la confidencialidad de los datos, son dos puntos a destacar de esta resolución. La integridad refiere a las recomendaciones para asegurar la completitud, (que los datos requeridos en los formularios estén completos a la hora de recolectar);

minimizar los errores de ingreso (que la información esté ingresada de forma clara y concreta); y asegurar la integridad (verificar la exactitud del dato ingresado). En cuanto a la confidencialidad, se destacan los siguientes puntos: asegurar la confidencialidad durante el proceso de recolección (cifrar la comunicación cliente-servidor); limitar el acceso a la recolección de datos; y limitar el acceso no autorizado durante la recolección.

En resumen, conciliar los principios de protección de datos personales con los principios de la seguridad de la información es fundamental para proteger los derechos de las personas.

La importancia de conocer cuáles son tus derechos y hacerlos valer

Toda vez que se otorgan datos personales, las personas tienen derecho a contar con información clara y accesible en relación a la cesión, uso y finalidad con la que se recolectan y tratan, especialmente cuando involucra datos sensibles. En esta línea, la normativa argentina sobre protección de datos personales reconoce que las personas tienen derecho a la información, acceso, rectificación, actualización, y supresión de sus datos personales. A continuación, repasamos cada uno de ellos.

Derecho a la información

Los titulares de los datos tienen derecho a contar con información sobre la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. Esto puede ser consultado en el buscador del Registro Nacional de Bases de Datos Personales, mencionado anteriormente. Además, los responsables de tratamiento tienen la obligación de brindar información a los titulares de los datos, especificando la finalidad de tratamiento, el tipo de datos que se van a tratar, el plazo de conservación, la existencia de cesiones o transferencias, las medidas de seguridad aplicadas para cuidar los datos, los canales habilitados para que las personas ejerzan sus derechos o realicen consultas, entre otros.

La información disponible permite a los titulares contar con herramientas para decidir si brindar o no sus datos personales para el tratamiento, esto es lo que la Ley de Protección de Datos denomina "consentimiento informado", que tiene que ser previo y libre. Aquí es necesario hacer una salvedad, ya que no todo tratamiento de datos requiere del consentimiento del titular. En algunos casos existen motivos como el interés público (por ejemplo la acción del Estado) donde no es viable solicitar el consentimiento a cada persona. En esos casos, la posibilidad de contar con información sobre el tratamiento también es fundamental.

Finalmente, la información sobre el tratamiento debe tener un alto nivel de publicidad, ser accesible y estar expresada de manera sencilla, para que sea comprensible por todas las personas. Conocer las políticas de privacidad es fundamental para saber con qué empresas se comparten los datos, cuáles son las finalidades y cómo los cuidan.

Derecho de acceso

Los titulares de los datos tienen derecho a solicitar y obtener información de sus datos personales, para lo cual antes deben acreditar su identidad. Una vez acreditada la identidad y realizado el pedido de acceso, quien trate los datos debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

Ahora bien, el derecho de acceso sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo que lo justifique. En el caso de datos de personas fallecidas, los sucesores universales pueden ejercer este derecho en su representación. La información solicitada debe ser suministrada en forma clara, exenta de codificaciones y acompañada de una explicación, en lenguaje accesible y comprensible.

Derecho de rectificación, supresión y actualización

Todas las personas tienen derecho a que sus datos personales sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad. Quienes traten los datos tienen un plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o bien, de haber advertido el error o falsedad para realizar la rectificación, supresión o actualización de los datos personales.

Si existe alguna cesión o transferencia de datos, los responsables o encargados del tratamiento tienen la obligación de avisar sobre la rectificación o supresión al cesionario. Un ejemplo de esto, son los datos crediticios que tratan los bancos, los cuales a su vez informan al Banco Central. Si un cliente realiza una rectificación, supresión o actualización de sus datos personales, el banco en este caso tiene la obligación de informar al Banco Central y demás entidades donde cede esos datos personales.

Un aspecto a considerar, es que el derecho a supresión no puede realizarse en todos los casos. El ejercicio de este derecho se limita cuando puede atentar a derechos o intereses legítimos de otras personas, o en los casos en que existe una obligación legal de conservar los datos, por ejemplo como sucede con los antecedentes penales.

¿Cómo podés realizar una denuncia?

Si una empresa u organismo público se niega a informar qué datos personales posee o a rectificar, actualizar o suprimir información incorrecta o brinda una respuesta que no te resulta satisfactoria, podés realizar una denuncia.

Para esto, las personas titulares pueden ingresar a través de la plataforma “Trámites a Distancia” con clave fiscal de la AFIP nivel 2 o superior y buscar e ingresar en el trámite “Denuncia por incumplimiento Ley de Protección de Datos Personales”. Luego completar los campos del formulario, adjuntar la documentación que solicita el sistema y confirmar el trámite. Este trámite también puede realizarse de manera presencial o por correo postal, siguiendo una **serie de pasos.**

La AAIP a través de la Dirección Nacional de Protección de Datos Personales se encargará de evaluar el pedido y en caso de corresponder, iniciará acciones administrativas ante el responsable de la base de datos.

Recomendaciones para proteger tus datos en web y redes sociales

- Leé las políticas de privacidad y de uso de tus datos personales de redes sociales y aplicaciones.

- Verificá que las aplicaciones o redes sociales que utilices tengan canales para conocer, rectificar, actualizar o suprimir tus datos recopilados. Recordá que podés denunciar ante la AAIP si te niegan alguno de estos derechos.

- Ingresá tus datos personales solo en sitios con candado gris o verde y con HTTPS al inicio de la barra de direcciones.
No compartas tus datos con destinatarios desconocidos.

- Eliminá con frecuencia tus datos de actividad en web y aplicaciones.

- Usá contraseñas seguras:

- Mínimo ocho caracteres.

- Combinación de mayúscula, minúsculas, números y caracteres especiales.

- Sin información personal.

- Una diferente para cada cuenta.

- Renovalas con frecuencia.

- Utilizá sistemas de doble verificación o de autenticación en dos pasos.