NUESTRO MUNDO DIGITAL

Claves para tener el control sobre nuestros **datos personales** y privacidad en entornos digitales

GUÍA PARA ADOLESCENTES

AAIP Argentina

Autoridades

Beatriz de Anchorena Titular de la AAIP

Analía Zimmermann Coordinadora Consejo Federal para la Transparencia (CFT)

Analía Martínez Coordinadora de Planificación y Seguimiento de la Gestión

Luciana Carpinacci Directora Nacional de Evaluación de Políticas de Transparencia

Catalina Byrne Directora de Transparencia Activa

Emiliano Arena Director de Evaluación y Participación Ciudadana

Violeta Paulero Directora Nacional de Protección de Datos Personales

Anastasia Dozo Directora de Promoción del Derecho a la Privacidad

Maximiliano Rey Director de Fiscalización y Regulación

Dirección Nacional de Políticas de Acceso a la Información

Luciano Acevedo Director de Contenido y Normativa de Acceso a la Información

Agustín Pérez Aledda Director de Gestión y Control de Acceso a la Información

Dirección de Asuntos Jurídicos

Patricia Beltrame Coordinadora de Asesoramiento Legal

Fernando Fernández Director Técnico Administrativo

Felipe Giménez Coordinador de Presupuesto y Contabilidad

Juan Lagostena Director de Informática e Innovación

Gisela Chesi Auditora Interna

AAIP Argentina

DNPDP Dirección Nacional de Protección de Datos Personales

Autoridades:

Titular de la AAIP **Beatriz de Anchorena**

Directora Nacional de Protección de Datos Personales **Violeta Paulero**

Directora de Promoción del Derecho a la Privacidad **Anastasia Dozo**

Director de Fiscalización y Regulación **Maximiliano Rey**

Equipo responsable de la elaboración de este material:

Responsable del desarrollo del contenido **Gisela Grunin**

Supervisión **Anastasia Dozo** y **Guadalupe Mercado**

Agradecimiento al grupo de adolescentes que hizo una primera lectura y valiosos comentarios de este material.

Noviembre 2024

¿Cómo citar este material?
Agencia de Acceso a la Información Pública (AAIP), “Nuestro mundo digital. Claves para tener el control de nuestros datos personales y privacidad en entornos digitales”. Buenos Aires. 2024.

Índice

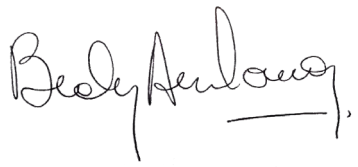
Prólogo

Las tecnologías ofrecen numerosas oportunidades para participar, relacionarse, expresarse y acceder a información, pero también pueden implicar riesgos que afectan la privacidad y la seguridad de nuestra información personal. En un mundo donde los medios digitales son una parte esencial de nuestra vida cotidiana, es imprescindible comprender la importancia de proteger los datos personales y resguardar la privacidad.

Como parte del Plan Estratégico 2022-2026, desde la Agencia de Acceso a la Información Pública (AAIP) elaboramos esta guía con el propósito de acompañar a los adolescentes y concientizarlos sobre el derecho a la autodeterminación informativa. Además, de manera complementaria, desarrollamos otra guía para brindar apoyo a docentes, padres y otras personas adultas que puedan ejercer el rol de educadores.

Este material aborda los principios clave de la normativa argentina sobre protección de datos personales, proporciona herramientas prácticas y ayuda a identificar situaciones que podrían poner en peligro la privacidad de las personas. Asimismo, incluye un cuadernillo con actividades diseñadas para trabajar en modalidad de taller de forma dinámica y participativa.

Esperamos que sea una herramienta valiosa para explorar el mundo digital de manera informada y segura.



Beatriz de Anchorena
Titular de la Agencia de Acceso a la Información Pública (AAIP)

Introducción: ¿Qué vamos a encontrar en este material?

Desde la **Agencia de Acceso a la Información Pública (AAIP)** desarrollamos este material para que adolescentes sepan cómo proteger la privacidad y la seguridad de los datos personales, en especial en los entornos digitales

Con cada acción que hacemos en internet, cada vez que publicamos una foto, chateamos, escuchamos una lista de canciones, vemos un video, hacemos una compra virtual, ingresamos al campus virtual de la escuela, entregamos información personal que es muy valiosa. Estos datos se recopilan, almacenan y analizan en todo momento. Las empresas y otras entidades los utilizan con distintos propósitos, como por ejemplo personalizar servicios y productos y los comparten con otras entidades. Y esto muchas veces representa un desafío para la privacidad de nuestros datos.

¿Cuáles son las consecuencias y riesgos a los que estamos expuestos cuando compartimos nuestros datos personales? ¿Por qué se habla de uso ético de la información?

A través de este material, descubriremos qué son los datos personales, por qué es importante cuidarlos. También, aprenderemos conceptos clave como identidad digital, huella digital y ciudadanía digital, así como también cuáles son las leyes, los derechos que tenemos para proteger nuestros datos personales en internet y cómo hacerlos valer.

Como titulares de esos datos personales, tenemos derecho a saber cómo se van a utilizar, dónde se almacenan, para qué se utilizan y con quiénes se comparten, especialmente cuando se trata de datos sensibles como aquellos que dan información sobre la salud, la orientación sexual, el género, las opiniones políticas, entre otros.

Además, compartiremos algunos consejos útiles para proteger nuestra privacidad en los territorios digitales y reflexionaremos sobre la importancia de comportarse de manera ética y respetuosa con uno mismo y con los demás. Finalmente, veremos casos reales que nos ayudarán a identificar situaciones problemáticas y aprender a prevenirlas para disfrutar de los beneficios de internet de forma segura.

Sobre todo esto vamos a aprender y reflexionar en estas páginas. ¡Empecemos!

1 ¿Qué son los datos personales y por qué es importante protegerlos?

¿Te pusiste a pensar, alguna vez, qué cosas definen quiénes somos? ¿Qué elementos construyen nuestra identidad? No hay una única manera de responder esta pregunta. Podríamos empezar por mencionar el lugar donde nacimos, las experiencias que nos marcaron, la apariencia física, la cultura y las herencias familiares, el signo del zodíaco, los deseos, las creencias, los valores y pensamientos, el carácter y la personalidad, el ADN...

En la construcción de nuestra identidad intervienen muchos aspectos, individuales y sociales. Algunos elementos, o una particular combinación de éstos, son únicos de nuestra persona y pueden servir para identificarnos entre una multitud: nuestros datos personales.

A veces, nos gusta compartir parte de esa información con otras personas. En cambio, otros tipos de datos los reservamos sólo para ámbitos privados o íntimos. Es nuestro derecho poder decidir con quién, para qué y en qué momento revelamos esa información. Es una forma de cuidar nuestra privacidad e intimidad.

En este primer capítulo vamos a conocer sobre la importancia de los datos personales y que estén bien protegidos.

Los datos personales son toda la información asociada a nuestra persona, con la que se puede identificarnos, contactarnos o localizarnos. Esto puede suceder de manera directa o indirectamente, mediante uno o varios elementos característicos de nuestra identidad, ya sea físicos, biológicos, fisiológicos, económicos, culturales, genéticos, etc.

En este sentido, los datos personales son muy variados. Un ejemplo clásico de datos personales son los **identificatorios**, aquellos que suelen pedirnos para realizar un trámite o inscribirnos en la escuela u otra institución: el nombre y apellido, DNI, fecha de nacimiento, dirección, número de teléfono.

Además, existen otros tipos de datos personales que están asociados a aspectos más amplios de nuestra identidad, que se vinculan a nuestras características físicas o circunstancias sociales, económicas, de salud o de educación. Por ejemplo: cuando aparecemos en fotos, audios o videos y también información sobre cómo es nuestra familia, qué actividades hacemos, el género con el que nos identificamos, la orientación sexual, el resultado de un análisis médico, si tuvimos algún conflicto con la ley, las compras que hicimos, nuestras calificaciones de la escuela, el club del que somos hinchas, las rutas de nuestros recorridos, la información genética y biométrica ¡y mucho más!

En la actualidad, todo este tipo de información sobre nosotros se puede recolectar fácilmente por medios digitales y esto nos plantea nuevos desafíos, en especial cuando se tratan de resguardar nuestros datos sensibles.

¿Qué son los datos personales?

Es la información que permite identificar a una persona, directa o indirectamente, por uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social o de cualquier otro tipo.

FUENTE: Proyecto para la actualización de ley de Protección de Datos Personales, elaborado por la AAIP.

¿Qué son los datos sensibles?

En determinados contextos sociales, revelar cierta información muy personal puede ser peligroso. Si se conocen esos datos de una persona, se podrían usar para perjudicarla, afectar su intimidad, hacerle daño, discriminar, ponerla en riesgo o en desventaja. Por eso, se los considera como datos sensibles y tienen una protección mayor.

Los datos sensibles son todos aquellos que permiten conocer aspectos como **origen étnico**; **creencias o convicciones religiosas**, **filosóficas y morales**; **afiliación sindical u opiniones políticas**; **datos relativos a la salud**, **discapacidad**, a la **preferencia u orientación sexual**, **datos genéticos o biométricos**, entre otros.

Nadie puede obligarte a compartir o entregar datos sensibles.

El tratamiento de estos datos debe hacerse con extremo cuidado, respetando la confidencialidad y únicamente pueden ser pedidos y tratados cuando existan razones de interés general autorizadas por ley (ver capítulo 2). Por ejemplo, si usan datos sensibles para hacer investigaciones científicas deben tomarse medidas para impedir que se pueda identificar en forma individual a las

personas que participan. Algunas autoridades públicas, como la policía, también manejan este tipo de datos vinculados a los antecedentes penales e infracciones. También las instituciones y profesionales de la salud deben respetar el principio del secreto profesional y no revelar datos sensibles de sus pacientes.

Datos personales

Permiten identificar a una persona

- nombre y apellido
- profesión
- datos de contacto
- correo electrónico
- información financiera
- o cualquier otro dato que permita identificar a una persona

Datos sensibles

Categoría especial de datos personales

- opiniones políticas
- origen étnico
- convicciones religiosas
- información sobre la salud
- información sobre la orientación sexual
- datos genéticos y biométricos

Cuadro tomado de "Caja de herramientas para el acceso a la información de los archivos", AAIP 2024. Disponible en: www.argentina.gob.ar/sites/default/files/aaip_caja_de_herramientas_archivos.pdf

¿Qué son los datos genéticos y biométricos?

Datos genéticos: es la información sobre las características genéticas de una persona. Por ejemplo, el resultado de un análisis del código ADN puede identificar si alguien tiene alto riesgo potencial frente a algunas enfermedades.

Datos biométricos: es la información sobre los aspectos físicos que son únicos de una persona y permiten identificarla a través del uso de una tecnología. Por ejemplo: el escaneo de la huella digital dactilar o el reconocimiento de imágenes faciales.

Tanto los datos genéticos como los biométricos pueden considerarse como datos sensibles, si revelan información con la que se pueda identificar a una persona y tratarla de forma discriminatoria.

¿Por qué es importante cuidar los datos personales?

Todos estos datos son muy importantes porque nos identifican de manera única e irrepetible. Son una parte fundamental de nuestra **identidad**, a través de la que expresamos nuestra forma de ser, pensar, sentir y actuar en el mundo y a lo largo de toda la vida.

- Aprender a cuidar nuestros datos personales nos ayuda a poder proteger nuestra identidad, privacidad e intimidad.

Así como tomamos precauciones cuando estamos en la calle, como atar la bici con una cadena o guardar la billetera, para cuidar de nuestros datos personales también tenemos que activar estrategias de protección y aprender algunos hábitos seguros cuando usamos internet (ver más en el capítulo 4).

Ser el **primer guardián de nuestros datos en los entornos digitales** ayudará a prevenir algunos problemas: desde estafas virtuales o publicidades invasivas hasta situaciones que puedan afectar nuestra privacidad y dignidad. Por ejemplo, que se viralice una foto que no queremos mostrar, que alguien cree un perfil falso para hacer comentarios en nuestro nombre o que personas desconocidas sepan cómo encontrarnos y nos engañen.

Nuestros datos personales nos pertenecen. Tenemos derecho a elegir y controlar si queremos o no entregarlos. En todos los casos, el tratamiento de los datos debe ser adecuado y respetando lo que establece la ley (ver capítulo 2).

¿Qué es el tratamiento de datos?

Se refiere a todas las acciones que se pueden hacer con los datos:

- recolectar,
- conservar, almacenar,
- ordenar, analizar, relacionar, categorizar,
- corregir, destruir,
- difundir, entregar a otros.

Para hacer cualquiera de estas acciones con nuestros datos, previamente deben habernos informado y tener nuestra autorización (ver más sobre el consentimiento en el capítulo 2). Además, es necesario que en todo momento se respete la confidencialidad de la información.

El tratamiento de datos debe ser acorde a la finalidad y limitarse a los que sean necesarios para la que se los

solicitó. En este sentido, pensemos si realmente son pertinentes todos los permisos que piden algunas de las aplicaciones digitales que usamos. Por ejemplo: ¿Es necesario para su uso que un videojuego o un filtro en tendencia en redes accedan a la agenda de contactos, a la ubicación del dispositivo o al micrófono? Lo que pasa en muchos de estos casos es que hacen un tratamiento excesivo de los datos, porque se pide información que no tiene que ver con el propósito de su uso.

Entonces, podemos detenernos y repensar si estamos dispuestos a entregar los datos a cambio de lo que nos ofrecen.

Probá tus conocimientos:

De entre todos estos datos personales, ¿podés identificar cuáles son datos sensibles?

1. Mis colores favoritos.
2. Mi historia clínica de salud.
3. Mi imagen en videos de sistema vigilancia.
4. Mi huella digital.
5. Mi club deportivo.
6. Mi agenda de contactos.
7. La imagen de mi cara.
8. Mi ropa.
9. Mis datos genéticos.
10. Mi religión.
11. Mi escuela.
12. Mi lista de reproducción musical.
13. Mi firma.
14. La clave para acceder al campus virtual de la escuela.
15. Mi número de documento.

(Respuesta: 2, 4, 7, 9, 10)

2 Conozcamos nuestros derechos

La protección de los datos personales es un derecho humano. En Argentina, existen leyes específicas que garantizan este derecho, para cuidar nuestra intimidad, privacidad y honor. Como adolescentes tenemos una protección especial que también contempla el cuidado de los datos personales.

Además, hoy somos ciudadanos digitales y tenemos derechos y obligaciones para que la convivencia en los espacios virtuales sea segura, respetuosa con los demás, ética, libre, creativa y participativa.

En este capítulo aprenderemos sobre las leyes que protegen los datos personales. Porque para poder exigir que se cumplan todos nuestros derechos es necesario conocerlos bien.

En nuestro país existen normas que garantizan el derecho a la protección de los datos personales y regulan cómo deben tratarse estos datos.

El marco normativo de la protección de los datos personales

- El artículo 43 de la Constitución Nacional establece el derecho a conocer los datos propios que se guardan en registros públicos o privados. Si tienen alguna información falsa o discriminatoria, podemos exigir la supresión, rectificación, confidencialidad o actualización de esos datos.
- La Ley N° 25.326 de Protección de los Datos Personales fue sancionada en el año 2000 y fue precursora en la región, sentando las bases y brindando un fuerte marco regulatorio.
- El Código Civil y Comercial, Ley Nº 26.994, contiene un capítulo dedicado a los derechos personalísimos o "derechos fundamentales" y sus artículos 52, 53 y 55 reconocen los derechos a la intimidad, la integridad, la imagen, la dignidad y la identidad de las personas.

La **Ley N° 25.326 de Protección de los Datos Personales** tiene como objetivo garantizar el derecho al honor, la intimidad y privacidad de las personas. Reconoce los derechos de información, acceso, rectificación y supresión de los datos personales por parte de sus **titulares** (ver Glosario). Además, establece las reglas para el tratamiento de esa información.

Agencia de Acceso a la Información Pública (AAIP)

Es la encargada de aplicar la Ley N° 25.326, a través de su Dirección Nacional de Protección de Datos Personales, controlando la protección integral de los datos personales que estén guardados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados.

Si tenés dudas o necesitás orientación, llamanos al (54-11) 3988-3968 o escribinos al correo electrónico datospersonales@aaip.gob.ar

Esta ley reconoce nuestro derecho a:

- pedir y que nos den información sobre qué datos personales tienen registrados en bancos de datos públicos o privados;
- pedir que nuestros datos sean corregidos o actualizados;
- pedir que sean suprimidos, en los casos en que corresponda;
- pedir que sean guardados confidencialmente;
- que nuestros datos personales no se utilicen ni registren sin nuestra autorización o consentimiento, salvo en casos puntuales (establecidos en el artículo 5 de la ley).

De acuerdo a esta ley, siempre que nos pidan datos personales deben hacerlo en forma legal y con las medidas de seguridad necesarias y tratarlos solamente para la finalidad para la que fueron recolectados en un principio, en forma clara y transparente. **No vale pedirlos en forma engañosa.**

Derecho de información

Nos permite consultar si alguien posee nuestros datos personales, cómo los obtuvo, qué hace con ellos y quiénes son los responsables de la **base de datos** (ver glosario) donde se guardan. El plazo legal para responder es de 10 días corridos.

¿Qué es dar consentimiento para el tratamiento de datos personales?

Se trata de expresar nuestro deseo o voluntad para autorizar el uso de nuestros datos.

El consentimiento siempre debe darse en forma:

- **Libre:** sin ningún tipo de presión.
- **Expresa:** sólo para la finalidad que se informó previamente. Si aceptamos que nos tomen una foto no estamos aceptando también que esa foto sea difundida.
- **Informada:** nos tienen que explicar, en lenguaje accesible y claro, para qué necesitan nuestros datos y quiénes tendrán acceso a ellos.

Además, esta decisión debe poder ser revocada. Es decir que, si en algún momento cambiamos de opinión, retirar el consentimiento tiene que ser tan fácil como haberlo dado.

¿Cómo damos el consentimiento para el uso de nuestros datos? Por ejemplo, cuando firmamos una autorización cediendo el uso de nuestra imagen o cuando aceptamos las condiciones para el uso de alguna aplicación o servicio que requiera nuestros datos.

Según la ley, existen algunas situaciones puntuales en las que no es necesario contar con la autorización del titular para el tratamiento de sus datos. Por ejemplo, cuando están en bases de datos de acceso público; si los pide un organismo del Estado para cumplir sus funciones (para acceder a un beneficio, por ejemplo) o por obligaciones legales (para inscribirse en la escuela, por ejemplo), entre otras.

La Ley N° 25.326 fue pionera en la región, pero desde su sanción en el año 2000 muchas cosas han cambiado. Por eso, la AAIP elaboró una propuesta para actualizarla, basada en estándares y recomendaciones regionales e internacionales, buscando dar respuestas a los nuevos desafíos tecnológicos. La propuesta incluyó importantes aportes de diferentes sectores sociales, que fueron presentados a través de consultas, mesas de diálogo y debates abiertos, transparentes y participativos.

Como resultado de este proceso, la **AAIP** presentó el **proyecto para una nueva Ley de Protección de Datos Personales,** que fue enviado a la Honorable Cámara de Diputados de la Nación para su tratamiento el 29/06/2023 mediante el Mensaje 87/2023. El proyecto contempla tres pilares: i) el derecho humano a la protección de los datos personales y la autodeterminación informativa, ii) la innovación tecnológica –basada en principios éticos– que promueva un desarrollo económico inclusivo, iii) la construcción de confianza a través de reglas de juego claras. Además, este proyecto incorpora los derechos de niños, niñas y adolescentes y la protección especial de sus datos personales.

Además, como nuestros datos atraviesan las fronteras a través de la red de redes que es internet, es necesario coordinar esfuerzos entre países para proteger la privacidad de la población. Para reforzar nuestra legislación, Argentina ratificó el 17/04/2023 el Convenio 108+ del Consejo de Europa, instrumento internacional que tiene la finalidad de proteger la privacidad de las personas contra posibles abusos en el tratamiento de sus datos y también incluye condiciones especiales para el tratamiento de datos personales de niños, niñas y adolescentes.

¿Qué es la autodeterminación informativa?

Es el derecho que tenemos a autorizar o rechazar el tratamiento de nuestros datos personales y de poder controlar lo que se hace con esa información. Este principio se basa en la idea de que las personas tenemos el derecho de tomar decisiones informadas y conscientes sobre el manejo de nuestra información personal.

¿Cómo nos protege la ley si....

...los datos personales registrados son erróneos, desactualizados o no corresponde que los tengan registrados?

Podemos pedir que corrijan el error o actualicen la información. En caso de los datos sensibles, podemos exigir que los supriman o los mantengan en secreto.

...nos perjudica una decisión tomada en base al tratamiento automatizado de datos personales?

El tratamiento automatizado de datos personales son las operaciones o acciones que se llevan a cabo sobre datos personales o conjuntos de datos personales usando sistemas o herramientas tecnológicas sin intervención humana directa.

Si se toman decisiones basadas únicamente en el tratamiento automatizado de nuestros datos y eso nos perjudica, podemos pedirle al responsable de tratamiento (ver glosario) que explique en forma clara la lógica que aplicó para tomar esa decisión.

Más información:

- **www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales**
- **www.argentina.gob.ar/justicia/derechofacil/leysimple/convenio-de-proteccion-de-las-personas-con-respecto-al-tratamiento-automatizado-de-datos-de-caracter**

Una protección especial

Además, como adolescentes tenemos derechos que nos protegen de manera especial hasta los 18 años. La **Ley N° 26.061 de Protección Integral de los Derechos de Niñas, Niños y Adolescentes** establece el derecho a que se respete nuestra **dignidad, reputación y propia imagen**.

De acuerdo con esta ley (en su artículo 22), en las situaciones que puedan afectar la dignidad o reputación y en aquellas que violan la intimidad, vida privada o intimidad familiar, está prohibido "exponer, difundir o divulgar datos, informaciones o imágenes" que permitan identificar a niñas, niños y adolescentes, en forma directa o indirecta, a través de cualquier medio de comunicación o publicación en contra de su voluntad y la de su familia, representantes legales o responsables.

Esto, por un lado, nos protege evitando que nos expongan públicamente en momentos difíciles. ¿Qué tipo de información no se puede divulgar en estas situaciones? Desde los datos de nuestro nombre, familia, vivienda, escuela, hasta apodos, imágenes y todo lo que permite identificar quiénes somos.

Por otro lado, señala que, si alguien quiere mostrar datos nuestros, como una foto o video, siempre es necesario tener autorización. **A partir de los 16 años, podemos dar nuestro consentimiento, pero antes de esa edad también hace falta contar con la firma de la familia, tutor o responsable adulto.**

¿Qué es la ciudadanía digital?

En el mundo virtual, todos tenemos los mismos derechos y responsabilidades que en el mundo físico: a la privacidad, a la libertad de expresión, a no sufrir discriminación ni violencia y a buscar ayuda si tenemos un problema o algo nos hace sentir mal.

Pensamos en internet como un espacio público, que habitamos con otras personas y donde construimos ciudadanía. Esto significa aprender a ser parte de una comunidad, donde se respetan nuestros derechos, teniendo la obligación de respetar los derechos de los demás, para que todos tengamos las mismas oportunidades.

Como adolescentes, tenemos derecho a estar protegidos de cualquier riesgo, amenaza o vulneración en los entornos virtuales. Las personas adultas, las instituciones, el sector privado y toda la comunidad son corresponsables de garantizar estos derechos y es el Estado el que tiene la mayor responsabilidad de respetarlos, protegerlos y hacerlos cumplir.

¿Qué es la ciudadanía digital?

La ciudadanía digital es conocer y ejercer todos nuestros derechos en internet.

Para eso, es clave aprender ciertas habilidades con las que podamos usar las herramientas digitales en forma responsable, segura, crítica, reflexiva, creativa y participativa y que nos permitan:

- **entender** cómo funciona el ecosistema digital, sus actores principales y sus reglas de juego;
- **promover** una convivencia respetuosa y vínculos saludables, en entornos que sean seguros;
- **participar** activa y positivamente en la creación de contenidos y colaborar en el desarrollo de soluciones que puedan beneficiar a la comunidad.

Más info: **www.argentina.gob.ar/que-es-la-ciudadania-digital**

Para poder ejercer todos nuestros derechos plenamente en los entornos virtuales necesitamos tener ciertas **habilidades digitales** que nos permitan hacer uso de las tecnologías de manera:

- **segura y responsable**, gestionando nuestra identidad digital y privacidad de forma segura. Aprendiendo a identifica posibles riesgos y a conocer las formas de actuar al respecto pedir ayuda. Teniendo comportamientos éti-

cos, con empatía y respeto por las demás personas, en una convivencia digital inclusiva, sin violencias ni discriminación de ningún tipo. Cuidando nuestro bienestar.

- **reflexiva y crítica** comprendiendo y analizando con pensamiento crítico para comprender cómo funcionan las tecnologías, los roles de los diferentes actores que intervienen en la gobernanza y las relaciones de poder en internet, los modelos de negocio, los problemas de la desinformación, la cultura de la influencia, entre otros. Conociendo cómo buscar y contrastar información con fuentes confiables. Reconociendo las formas en que los algoritmos jerarquizan y priorizan los datos que procesan, así como los conflictos éticos que presentan la inteligencia artificial y otras innovaciones tecnológicas.
- **creativa y participativa** siendo capaces de desarrollar contenidos y soluciones digitales, crear, editar, programar y compartir producciones digitales de valor, que sean originales y reconozcan los derechos de autoría. Relacionarnos y participar activamente en la vida pública digital haciendo aportes desde nuestra mirada.

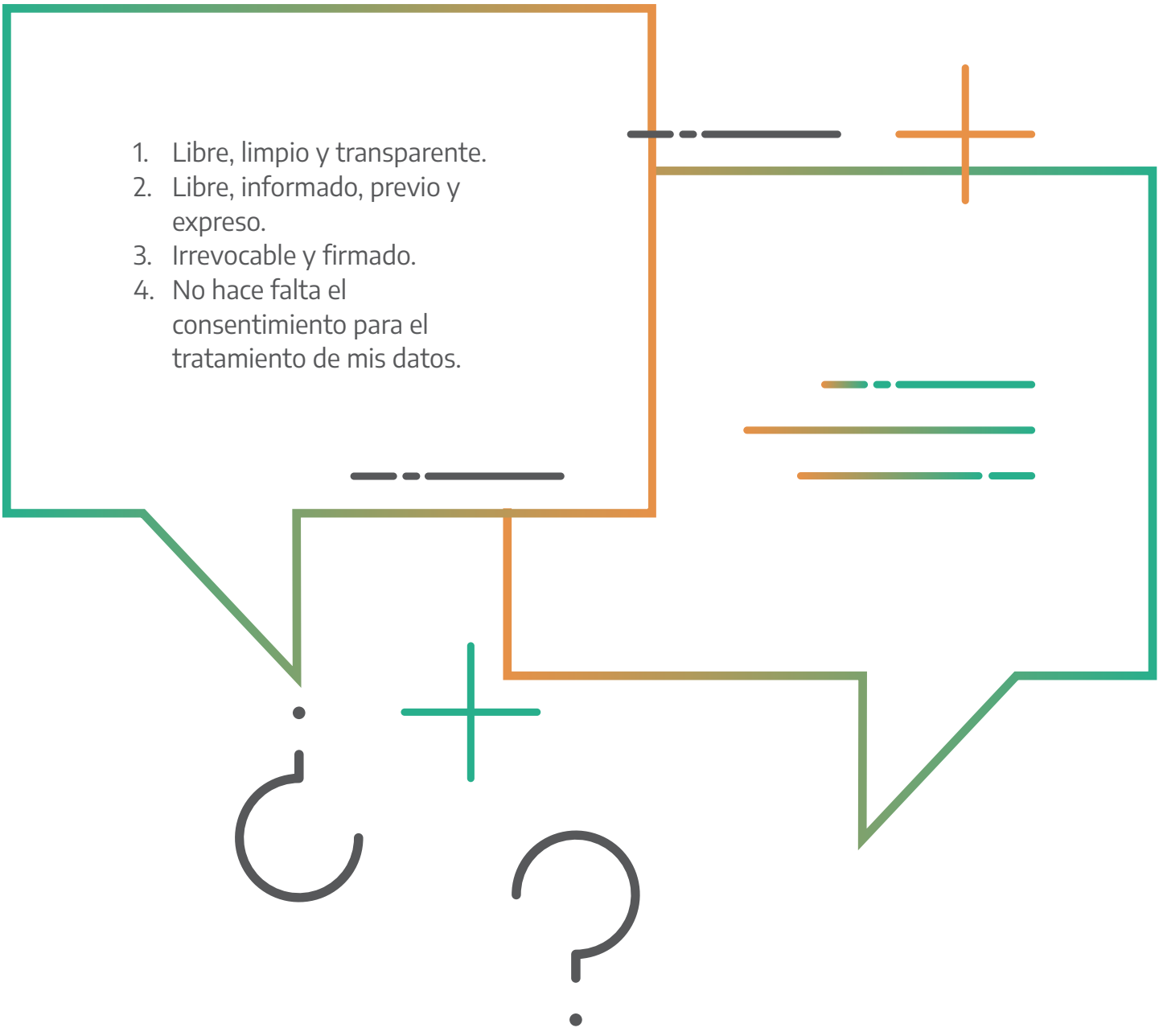
¿Cuáles son nuestros derechos y obligaciones en internet?

En este episodio de la serie “Ciudadanos en internet” de Canal Encuentro Manu, Mica, Bepo y Soni reflexionan sobre sus experiencias digitales, junto a la excéntrica especialista Olga Iride. **www.educ.ar/recursos/117999/identidad-y-datos-personales-en-internet**

Probá tus conocimientos:

El consentimiento para aprobar el tratamiento de tus datos personales por parte de una empresa debe ser:

1. Libre, limpio y transparente.
2. Libre, informado, previo y expreso.
3. Irrevocable y firmado.
4. No hace falta el consentimiento para el tratamiento de mis datos.



(Respuesta: 2)

3 ¿Qué pasa con nuestros derechos y los datos personales en los entornos digitales?

¿Te imaginás un día sin pantallas? Sería casi imposible, ¿verdad? Cada vez pasamos más tiempo haciendo actividades en línea: jugamos, chateamos con amigos, nos enamoramos, alentamos a nuestro equipo, aprendemos cosas nuevas y participamos en lo que nos interesa... La tecnología está presente en nuestro día a día y eso tiene un impacto significativo: su uso trae nuevas prácticas sociales y desafíos que modifican nuestra forma de comprender y estar en el mundo.

En todos estos momentos en los que interactuamos con dispositivos digitales conectados a internet generamos información muy valiosa. Con cada interacción virtual dejamos un rastro de miles de datos, que entregamos a grandes empresas tecnológicas, incluso sin darnos cuenta. Estos datos se usan para identificar y contabilizar nuestros gustos, intereses, deseos y necesidades. La Ley N° 25.326 de Protección de Datos Personales, que conocimos en el capítulo anterior, es la herramienta que tenemos para poder proteger nuestra privacidad.

¿Cómo se construyen la identidad y la huella digital? ¿Qué información entregamos a las plataformas digitales? ¿Quiénes ganan con nuestros datos? ¿Cómo aprovechar todo el potencial de internet en forma segura y haciendo un uso reflexivo? Sobre todo esto continuaremos aprendiendo y reflexionando en este tercer capítulo dedicado a nuestros datos en los entornos digitales.

En internet encontramos miles de oportunidades para divertirnos, conectar con otras personas, inspirarnos, conocer cosas nuevas, expresarnos y participar. Allí pasamos buena parte del día (y de la noche) y se convirtió en un espacio social fundamental de nuestras vidas. Lo que nos pasa en internet nos pasa en la realidad y por eso también ahí creamos una parte importante de nuestra identidad: la identidad digital.

¿Qué es la identidad digital?

Nuestra identidad digital se construye con toda la información vinculada a nuestra persona que existe en internet. Es una parte de la identidad social, que desarrollamos tanto en el mundo físico y en el digital.

Los datos de nuestra identidad digital pueden provenir de:

- **la reputación digital:** es la información sobre nuestra persona que compartimos abierta y voluntariamente. Por ejemplo, al publicarla en redes sociales en modo público. A ello se le suma toda la información que hable de nosotros y haya sido generada por otros usuarios, instituciones, medios periodísticos, o incluso cuentas falsas. Una forma de conocer nuestra reputación digital es ver los resultados que

arroja poner nuestro nombre en un buscador;

- **la huella digital:** el rastro de datos que registran las empresas de servicios digitales con cada comportamiento e interacción que realizamos en la virtualidad, por ejemplo, las páginas que visitamos, las cuentas que seguimos en plataformas, los recorridos que hacemos portando el celular, las canciones que más escuchamos en nuestra lista de reproducción, a qué videos les pusimos "me gusta" y cuántos segundos lo miramos, etc.;
- **los formularios** que completamos, en forma privada y confidencial, con datos identificatorios. Por ejemplo, para poder hacer una compra virtual, abrir una cuenta de correo electrónico o inscribirnos en un curso en línea.

Mirá este video de Educ.ar para conocer más sobre la huella digital: **www.educ.ar/recursos/150452/microaprendizaje-que-es-la-huella-digital**

Con cada interacción virtual dejamos un rastro de miles de datos: las imágenes y textos que publicamos en redes, la geolocalización, los contactos, los hashtag que seguimos, las aplicaciones que descargamos, el tiempo que permanecemos mirando un contenido, los formularios que completamos, los filtros graciosos, los "me gusta", las compras, las videollamadas, las consultas en el buscador o el chat de inteligencia artificial generativa, ¡y más!

¿Qué es geolocalización?

Es la posibilidad de ubicar un dispositivo -el celular, la tableta, la notebook o cualquier otro- a través de Sistemas de Información Geográfica. Podemos activar o desactivar esta función, que envía información sobre el lugar en el que estamos a través de una red de satélites alrededor del mundo.

La geolocalización es muy útil en muchas situaciones, por ejemplo, si queremos conocer la ruta hacia un destino, o ver qué comercios y servicios se encuentran en una zona. Pero a la vez es un gran desafío para la privacidad de las personas, porque permite el monitoreo y la vigilancia. A su vez, esta información es recolectada por las empresas para conocer hábitos y patrones de movimiento de sus usuarios (Ver más sobre la creación de perfiles en el capítulo 3).

Cada acción que hacemos en internet deja información precisa acerca de quiénes somos. **Tenemos derecho a decidir quién conoce datos de nuestra identidad digital**.

¿Qué podemos hacer para tener el control de nuestros datos en internet?

- **configurar los niveles de privacidad** de dispositivos, redes sociales y otras plataformas (ver más en el capítulo 4),
- **ser conscientes de los permisos que damos** a las empresas que administran los servicios o herramientas digitales que usamos, por ejemplo, cuando aceptamos las condiciones de uso y privacidad de cualquier aplicación muchas veces les estamos dando acceso a nuestros datos,
- **diferenciar qué compartimos en forma pública y privada**. Tener en claro qué información dejamos al alcance de todo el mundo y **evitar exponer aquello que nos puede afectar** o no queremos que se muestre o recuerde "por siempre".

Veremos más de este tipo de estrategias de cuidado en el capítulo 4.

¿Se puede modificar o borrar un contenido en internet?

Es muy difícil. Es posible borrar una publicación, pero alguien pudo haber descargado esa información antes o replicarla en otra parte. Entonces, nunca tenemos la seguridad de haber eliminado el contenido por completo. Por eso siempre es muy importante pensar bien antes de compartir algo en modo público.

Nuestros datos personales son valiosos

En internet, nuestros datos son productos valiosos y codiciados, se recolectan muchas veces sin siquiera enterarnos. Es la primera vez en la historia que se recolectan tantos datos y se infieren muchos más y que existe la capacidad para recolectarlos, almacenarlos y procesarlos a gran escala.

Muchas de las aplicaciones y plataformas que usamos a diario requieren que ingresemos nuestros datos personales, por ejemplo, al abrir una cuenta en el campus virtual de la escuela o iniciar sesión en un videojuego. Pero, como ya vimos, generamos muchos más datos que los que ingresamos conscientemente en un formulario.

¿Qué otros datos pueden extraer? Todos los posibles, mientras usamos estas tecnologías ¡y cuando no las estamos usando también! Desde las selfies que compartimos y los comentarios que hacemos públicos voluntariamente, hasta la música, las pelis y los videos que consumimos, las grabaciones de voz que guardan los asistentes virtuales (como Siri o Alexa), con quiénes interactuamos y cuándo lo hacemos, incluso el tipo de dispositivo y de red que usamos para conectarnos, cuánta batería gastamos, nuestro horario de descanso y donde nos encontramos en cada momento.

Algunas aplicaciones toman datos dentro y fuera de su propia plataforma:

Datos extraídos de las actividades que hacemos **dentro de la aplicación**

- vistas de publicaciones y videos;
- tiempo de exposición;
- reacciones;
- palabras clave y hashtag;
- textos e imágenes publicadas;
- red de contactos

Datos extraídos por **fuera de la plataforma**

- geolocalización;
- agenda de contactos;
- tipo de dispositivo;
- imágenes y audios;
- búsquedas externas a la aplicación;
- dirección de IP;
- dispositivo de audio;
- estado de batería;
- operador de telecomunicaciones y tipo de red a la que se conecta;
- zona horaria;
- patrones y ritmos de pulsación de teclas

Todas estas acciones se convierten en **datos cuantificables y agrupables**, que unas pocas y grandes empresas tecnológicas **recolectan, almacenan, procesan y analizan** en forma automatizada. Estas técnicas automáticas de extracción y procesamiento de datos personales en redes sociales y sitios web se conocen como ***data scraping***. **El objetivo es elaborar perfiles y construir patrones predecibles de nuestras conductas.**

¿Qué es la elaboración de perfiles?

¿Cómo hacen las plataformas para saber exactamente qué productos y contenidos ofrecernos? La elaboración de perfiles es parte de la respuesta.

Con la descomunal cantidad de datos disponibles en internet, las empresas de tecnología pueden hacer un tratamiento automatizado de los datos y construir **perfiles de usuarios**. Esto es, analizar y agrupar aquellos usuarios que tengan características similares y así llegar a identificar con bastante precisión nuestros g**ustos, deseos, preocupaciones y miedos**. El objetivo es **anticipar posibles comportamientos** de las personas y tener en cuenta esto para tomar decisiones.

Al aceptar las condiciones de uso, cedemos en forma voluntaria toda esta valiosa información a las empresas. Éstas se comprometen a que nuestros datos no sean utilizados en forma desleal o fraudulenta, aunque a veces sea difícil de comprobar.

Este uso intensivo de nuestros datos trae beneficios y a la vez plantea algunos riesgos y desafíos para la protección de los derechos a la intimidad, a la autodeterminación y a la dignidad.

Entre los **beneficios**, ya nos dimos cuenta que cuanto más nos conoce la plataforma que usamos, mejores cosas nos recomienda que sean de nuestro interés. Por eso, no prestamos nuestra cuenta de reproducción musical a nadie que pueda alterar nuestra selección (ver más adelante sobre las burbujas de filtros). Pero, además, el procesamiento de datos es muy beneficioso para la investigación de problemas científicos y sociales, así como para la optimización de muchos de los servicios que aprovechamos, por ejemplo: conocer la ruta más eficiente para llegar a un destino, que un comercio analice las compras de sus clientes y administre mejor el stock de mercadería, que se simplifiquen ciertos trámites en oficinas públicas y se mejoren tratamientos de salud, entre otros.

Respecto de los **desafíos**, aún hay mucho por debatir y clarificar en relación con este modelo tecnológico y económico que pone en tensión el concepto de privacidad, en un contexto caracterizado por la extracción de datos, la economía de la atención y la vigilancia extrema.

Para que este modelo funcione, hemos llegado a traspasar algunos límites que plantean dilemas éticos. En este sentido, es importante conocer que muchas de las aplicaciones que usamos a diario (como por ejemplo las redes sociales o algunos de los juegos en línea) se diseñan con **patrones adictivos o engañosos**[1] **porque necesitan mantenernos mucho tiempo frente a las pantallas** entregando nuestros datos. Las empresas aseguran que el mecanismo es así para mejorar nuestra experiencia de uso de sus productos, pero en algunas ocasiones se pudo comprobar que también fueron usados para manipular, moldear, vigilar y hasta definir elecciones en países.

Por todo esto, es necesario conocer las políticas de privacidad de las empresas con las que interactuamos y vale la pena volver a preguntarnos, ¿es realmente gratis la experiencia digital o estamos entregando más de lo que en verdad queremos?

1 La AAIP participó en la elaboración del Informe de la Red Global para el Cumplimiento de la Privacidad 2024 sobre patrones de diseño engañosos, 2024. Disponible en www.argentina.gob.ar/noticias/la-aaip-comparte-los-resultados-del-estudio-global-sobre-disenos-de-sitios-web-y

La **AAIP** y otras once autoridades internacionales que trabajan por la protección de datos personales se pronunciaron de manera conjunta sobre el crecimiento global del **uso de técnicas de data scraping**. El objetivo de la declaración fue acompañar a la ciudadanía y a las empresas para identificar acciones para mitigar los riesgos. Para las personas usuarias, recomendaron **limitar el intercambio de información personal**, así como **conocer las políticas de privacidad y las declaraciones de uso de datos personales** de las empresas antes de compartirla o aceptar términos y condiciones. Respecto de las empresas, señala que son responsables de garantizar el cumplimiento de las leyes en materia de privacidad y protección de datos personales.

Mirá este video del canal Encuentro para conocer más sobre ventajas y desventajas de las tecnologías de la vigilancia y aprender cómo saben las redes lo que nos gusta gracias a las matemáticas.
www.youtube.com/watch?v=kDkt_ACEUBU

¿Qué es el modelo de extractivismo de datos y la economía de la atención?

“Cuando un servicio en línea es gratuito, uno no es el cliente. Uno es el producto”. Esta frase se popularizó para explicar en forma simple cómo funciona el modelo de negocios predominante en internet, basado en extraer y monetizar los datos de los usuarios. Esto requiere que los usuarios le dediquemos atención a las pantallas y permanezcamos allí mucho tiempo, generando y entregando datos.

¿A quién no le pasó que, mientras estaba haciendo algo, tuvo el impulso de chequear el celular y terminó quedándose ahí mucho tiempo, escroleando hasta el infinito? No es algo casual, es **planificado**. Muchas de las plataformas que usamos están diseñadas con **mecanismos adictivos, para captar y mantener nuestra atención**. Para eso, aprovechan algunas de las vulnerabilidades humanas: nos ofrecen un "golpe de felicidad" inmediato, pero tan efímero que enseguida buscamos obtener otro impulso, generando un vínculo de dependencia.

Así ocurre, por ejemplo, cada vez que recibimos una **notificación pendiente** en el celular o **validación social** a través de un 'Me gusta' en una publicación. El mismo efecto se activa en nuestros cerebros al abrir un cofre de **recompensa** en los videojuegos o en las aplicaciones de apuestas virtuales. Otros trucos de diseño adictivo son los contenidos **visualmente atractivos** y muy **personalizados**, el **escroleo sin límite**, la **actualización** de información (similar al funcionamiento de las máquinas tragamonedas del casino), entre otros mecanismos que fragmentan nuestra atención y pueden tener impacto en nuestro bienestar y salud mental.

Con este tipo de estrategias, las empresas compiten por captar nuestro tiempo y recolectar información.

Luego, pueden compartir esos datos con otras compañías comerciales (de publicidad, de seguros y otros rubros), para su uso en campañas políticas (como ocurrió por ejemplo con la influencia en votantes indecisos en las elecciones estadounidenses de 2018. Un suceso conocido como el "escándalo de *Cambridge Analytic*") o para el control y la vigilancia de la población.

Los impactos de este modelo están siendo estudiados por muchas disciplinas. Algunos autores hablan de "sociedad de la información", "capitalismo de vigilancia", "extractivismo de datos", "economía de la atención", entre otros.

Conociendo cómo fueron diseñadas las aplicaciones que usamos, podemos tomar decisiones para controlar de manera consciente cómo usamos nuestro valioso tiempo.

Algunas recomendaciones en este sentido son:

- desactivar notificaciones,
- tener una actitud crítica y reflexiva sobre los contenidos que vemos,
- establecer límites en el tiempo de uso, para equilibrar la conexión virtual con otras prácticas sin conexión.

“El dilema de las redes sociales”

En este **documental ficcionado**, estrenado en 2020 en la plataforma Netflix con dirección de Jeff Orlowski, muchos de los CEO de las grandes empresas tecnológicas describen en primera persona en qué consiste el negocio de las redes sociales, el poder que ejercen y los mecanismos adictivos que utilizan para mantener la atención de los usuarios.

Entrenamiento con datos

La abundancia de datos que generamos a diario también es utilizada para entrenar distintos algoritmos y sistemas basados en inteligencia artificial. Esto presenta algunos problemas y desafíos si no se toman medidas adecuadas en todas las etapas: desde el diseño del sistema, la creación de la base de datos con la que se lo entrena, hasta los criterios para la interpretación de los resultados. En todos estos momentos pueden tomarse decisiones que estén influidas por las creencias, prejuicios o “sesgos” de las personas involucradas en el proceso. Esto puede llevar a que el sistema finalmente entregue conclusiones incorrectas, que luego impactan en forma directa en nuestras vidas, de maneras que pueden amenazar nuestros derechos humanos. Por ejemplo, cuando se entrenó a una IA para reconocer rostros humanos con una base de datos de imágenes de personas caucásicas no pudo reconocer a las personas negras. ¿Qué crees que se pudo haber hecho para mitigar este resultado discriminatorio?

Estos avances, nos obligan a repensar cómo hacer de esta tecnología un uso ético, responsable y respetuoso de nuestros datos personales. Necesitamos que el diseño, entrenamiento y programación de avances tecnológicos como la IA contemplen, en forma consciente y premeditada, criterios diversos e inclusivos para su funcionamiento.

¿Qué es un algoritmo?

Se puede definir como una receta o una serie de pasos con instrucciones precisas para resolver un problema. Por ejemplo, para detectar patrones entre enormes volúmenes de datos.

Los algoritmos que ejecutan las máquinas son creados por equipos humanos, que comprenden el mundo desde su propia perspectiva cultural y social. Por eso, muchas veces sus diseños contienen las creencias, valores o intereses de quienes los crearon. Esto puede influir en decisiones automatizadas que perjudiquen o excluyan a ciertas personas, aunque no haya sido planeado de esa manera.

Cuidado con los **filtros graciosos**

¿Te sumaste, o conocés a alguien, a usar filtros para ver cómo luciría tu rostro en la vejez? Se viralizó como el desafío **#10YearsChallenge.** Para muchos fue divertido, pero tal vez no sepamos con claridad qué datos estuvimos entregando a cambio de pasar un buen rato. Algunos expertos afirman que las imágenes y demás datos que compartimos en ese tipo de aplicaciones, en realidad, pueden servir para entrenar herramientas de reconocimiento facial, que pueden ser usadas tanto con fines comerciales como de vigilancia.

Fuente: www.bbc.com/mundo/noticias-49012256

Hoy tenemos algoritmos responsables de definir los resultados de diversas **evaluaciones automatizadas**, por ejemplo, para brindar diagnósticos médicos, otorgar una beca de estudio, definir el precio de un viaje en una plataforma de traslados o la adjudicación de planes o prestaciones sociales. Hay organizaciones defensoras de los derechos humanos en internet que alertan sobre conflictos de **discriminación o injusticia algorítmica** cuando los criterios de evaluación automatizada no fueron justos.

A su vez, aún hay muchas preguntas por responder vinculadas a los derechos de **propiedad intelectual** y **derechos de autor** de los datos que utilizan los modelos de **inteligencia artificial generativos**. ¿Hemos dado permiso para que usen nuestros datos así? Posiblemente sí, tal vez aceptamos las condiciones de uso de algún producto que se mostraba gratuito sin haber leído la letra chica del contrato.

¿Qué es la inteligencia artificial?

La Inteligencia Artificial (IA) es un área de conocimiento de las Ciencias de la Computación que pone el foco en el desarrollo de sistemas y programas capaces de realizar tareas y resolver problemas de forma distinta a los métodos de programación habitual y con resultados similares a los obtenidos por personas.

Con el objetivo de atender riesgos y preocupaciones durante el uso de la Inteligencia Artificial (IA), los equipos técnicos de la AAIP desarrollaron la **Guía para entidades públicas y privadas en materia de Transparencia y Protección de Datos Personales para una Inteligencia Artificial responsable**, una herramienta diseñada para abordar el ciclo de vida completo de los sistemas de IA; su diseño, implementación

y mantenimiento. En esta Guía podés encontrar varias definiciones del concepto de inteligencia artificial y mucho material interesante. **www.argentina.gob.ar/sites/default/files/aaip-argentina-guia_para_usar_la_ia_de_manera_responsable.pdf**

Fuente: "Diez preguntas frecuentes y urgentes sobre Inteligencia Artificial". Fundación Sadoski, 2024. program.ar/wp-content/uploads/2024/08/Diez-preguntas-frecuentes-y-urgentes-sobre-Inteligencia-Artificial.pdf

¿Usás un **chat de inteligencia artificial** generativa?

Le consultamos a uno de los más conocidos si, al usarlo, existen riesgos relacionados con la protección de datos personales y esto es lo que respondió:

Usar este chat puede tener algunos riesgos en cuanto a la protección de tus datos personales. Cuando compartes información como tu nombre, dirección o detalles de contacto, esta podría ser guardada y utilizada sin que tú lo sepas. Además, los chats pueden ser atacados por hackers, lo que podría permitirles acceder a tus datos.

Otro riesgo es que tus datos se usen para enviarte publicidad sin tu consentimiento. Aunque se tomen medidas de seguridad, siempre hay la posibilidad de que ocurra algún error y tus datos se filtren.

Para protegerte, evita compartir información personal en chats públicos o con personas que no conoces. Lee las políticas de privacidad para saber cómo se manejarán tus datos y usa contraseñas seguras. También es importante mantener tus dispositivos actualizados para evitar problemas de seguridad.

Recuerda, cuidar tu privacidad en internet es muy importante. Mantente informado y consciente de los riesgos para navegar de manera segura. Proteger tus datos es protegerte a ti mismo.

Fuente: OpenAI. Respuesta generada por ChatGPT sobre los riesgos de usar chats en relación con la protección de datos personales. Consultado el 19 de julio de 2024, en chat.openai.com.

Datos personales, redes e inteligencia artificial:

¿Qué información nuestra usan las plataformas digitales para entrenar herramientas de IA? ¿Cómo podemos protegernos? Escuchalo en el podcast de la organización no gubernamental **Chequeado**: open.spotify.com/episode/2tN5AH95FDgiH2p-6DXa0vB?si=a370ec532eb34f30

Burbujas polarizadas

En los entornos digitales, este modelo de extractivismo de datos y elaboración automatizada de perfiles **nos propone ver únicamente aquellos contenidos que se predice que nos gustan o interesan**. El problema es **todo lo que no vemos**, lo que el algoritmo no programa para mostrarnos y queda oculto a nuestros ojos porque es diferente a lo que ya conocemos y confronta nuestra forma de entender lo que pasa en el mundo.

Así, quedamos atrapados en "jaulas de confort" (Esteban Magnani, 2019) y en lo que se conoce como **"filtro burbuja"**, junto a otras personas con las que pensamos igual y reafirmamos nuestras mismas creencias. Esto puede conducir a **"cámaras de eco"** en las que tenemos la ilusión de que nuestra postura es la mayoritaria y no hay lugar a otras perspectivas que puedan completar nuestra visión.

En las redes sociales, la dinámica de **polarización** (Ernesto Calvo y Natalia Aruguete, 2020), por un lado, nos acerca a quienes tenemos más afinidad y mayor número de conexiones y, por otro lado, nos aleja de los que piensan distinto. Esto es una dificultad importante para las democracias. Porque no favorece los debates ni los consensos en puntos de acuerdo a los que se pueden llegar aun teniendo otras diferencias. Tensan las grietas que nos separan cada vez más y generan más odio e intolerancia a lo diferente.

Este contexto, por un lado, nos obliga a ser cada vez más conscientes y responsables del tratamiento que permitimos sobre nuestros datos. Por otro lado, nos desafía a pensar otros modelos de tecnologías que promuevan la diversidad en las formas de mirar y habitar el mundo. Imaginar un mundo digital con otras reglas es posible.

¿Qué es la paradoja de la privacidad?

¿Te preocupa tu privacidad en internet pero **aceptás términos sin leer**? Bueno... ¡Ahí está la paradoja! Muchas veces, aunque sepamos que nuestros datos personales pueden estar en riesgo, preferimos seguir usando aplicaciones que nos hacen la vida más fácil y no nos preocupamos por evitarlo. Mirá este reel y conocé más sobre la "paradoja de la privacidad":
instagram.com/p/CuHzgJMAtjU/
Más info: asociación **Chicos.net**

No estás solo

La AAIP como autoridad de aplicación de la Ley de Protección de Datos Personales acompaña y puede asesorar para hacer valer tus derechos.

Si tenés dudas o necesitás orientación, llamanos al (54-11) 3988-3968 o escribinos a **datospersonales@aaip.gob.ar**

Probá tus conocimientos:

¿Público, privado o íntimo?

La dinámica de compartir parte de la vida por redes sociales cambió los límites de lo que hoy consideramos del ámbito público o del privado, en relación a lo que pasaba hace pocos años atrás. Es importante aprender a diferenciar qué corresponde a cada espacio y tomar precauciones para no exponer información por demás. ¿Dónde ubicarías cada situación?

Lo íntimo:
lo guardo únicamente para mí.

Lo privado:
lo comparto solo con las personas más cercanas y de confianza, familia y amistades.

Lo público:
si quiero, lo puedo compartir con todo el mundo.

1. Las fotos de mis vacaciones.
2. Una transmisión en vivo de la compe de freestyle.
3. Un video en el que se me ve sin ropa.
4. Una grabación del almuerzo familiar con mis primitos haciendo monerías.
5. Un tutorial donde enseño a pasar el último nivel de un videojuego.
6. Una invitación para la inauguración de la radio escolar.
7. Un audio de mi pareja.
8. Mi adhesión a la campaña por adopción responsable de mascotas.
9. Las fotos de un cumpleaños con mi grupo de amigos.

Respuestas: Íntimo: 3 - 7 / Privado: 1 - 4 - 9 / Público: 2 - 5 - 6 - 8

4 ¿Cómo cuido mis datos personales en los entornos digitales?

En casa, cerramos la puerta para cuidar que no entre cualquier persona, por una cuestión de seguridad. Del mismo modo, cuando estamos en internet, necesitamos tener algunos hábitos de protección que nos ayuden a resguardar nuestros datos personales. Por ejemplo, tener contraseñas fuertes y aprender a configurar los niveles de privacidad de las plataformas y dispositivos que usamos.

A su vez, los entornos digitales son espacios de convivencia social donde es importante tratarnos con respeto y establecer acuerdos sobre lo que compartimos en público o preferimos mantener en la intimidad. En este sentido, recordemos que difundir información privada de otras personas sin su autorización es violencia digital y su impacto puede ser devastador. ¿Qué podemos hacer para una mejor convivencia digital?

En esta sección compartimos algunos consejos útiles para tomar el control de nuestra privacidad en territorios digitales y para reflexionar sobre la importancia de un comportamiento ético y comprometido con una cultura de respeto y cuidado propio y de los demás.

Para cuidarnos y tener una convivencia digital respetuosa:

- Limitar la información sobre nuestra persona que está accesible en redes sociales u otras plataformas.
- Administrar las opciones de quién puede ver nuestra actividad en línea. Evaluemos qué queremos mostrar a todo el mundo (público), a nuestros contactos más cercanos (privado) y de aquello que reservamos para la intimidad.
- Ser conscientes de las consecuencias de lo que compartimos públicamente en internet y del uso que se le puede dar a esa información.
- Pensar antes de publicar sobre otras personas: ¿cómo se sentirá con esa publicación?
- Pedir ayuda a alguien de confianza, si hay algo que nos incomoda, si vemos o sufrimos alguna agresión en línea. A veces da miedo o vergüenza, pero estas situaciones nos pueden pasar a cualquiera y siempre es posible encontrar una solución.

Pedir permiso es clave

Antes de compartir o publicar una foto o texto de otra persona o mencionarla con etiquetas en redes sociales es importante preguntar si está de acuerdo.

Lo mismo vale si queremos enviarle algo íntimo por mensajería. Por ejemplo, algunas chicas reciben por Whatsapp imágenes íntimas del cuerpo de varones que no habían solicitado ver. Si no hay autorización, es acoso y violencia.

¿Compartir contraseñas es una prueba de amor?

Las claves son personales y privadas. Nunca se comparten, por mucho amor que nos tengamos. Construyamos relaciones basadas en la confianza y no en los celos y el control. Si estás en una situación de violencia con tu pareja, podés hablarlo con tu red de apoyo y pedir ayuda a una persona adulta de tu confianza.

Usar una ilustración como avatar del perfil de usuario puede ser una gran idea para evitar exponer nuestra propia imagen.

Las redes sociales y plataformas conectivas tienen términos y condiciones para el ingreso que es relevante atender. La mayoría de ellas establece una edad mínima para el ingreso que en Argentina está establecida en 13 años (y en otros países en los 16).

Para mantener seguros nuestros dispositivos:

- Nunca compartir las contraseñas.
- No utilizar redes wifi de acceso público o desprotegidas.
- Recordar cerrar siempre la sesión de nuestros correos, redes sociales, campus educativos, etc.
- Configurar la privacidad de los sitios, aplicaciones y redes sociales que utilizamos.
- Desconectar la geolocalización cuando no la necesitamos.
- Mantener el sistema operativo del dispositivo siempre actualizado.

- Desconfiar de correos electrónicos o mensajes de contactos desconocidos que inviten a realizar alguna acción, como hacer clic, descargar algo o proporcionar información confidencial.
- Evitar instalar programas o aplicaciones dudosas o innecesarias. No descargar juegos de sitios no oficiales. Pueden ser un peligro tanto para la máquina como para nosotros.
- Revisar términos y condiciones antes de aceptar cualquier contrato. Chequear a qué partes del dispositivo se dará acceso. Por ejemplo, evaluar si necesario que acceda al micrófono o a la agenda de contactos.

Más info: **www.argentina.gob.ar/justicia/convosenlaweb** y en **www.argentina.gob.ar/aaip**

¿Me han engañado?

En este sitio se puede ingresar un correo electrónico y comprobar si fue alcanzado por una filtración de datos en alguna de las plataformas que hayamos usado. Si tus datos están en riesgo, ¡cambiá la clave ahora! Un consejo: no uses la misma clave para todo, porque si se filtra tendrán acceso a todas tus cuentas.
haveibeenpwned.com/

¿Qué es el robo de identidad y de datos personales (phishing)?

Una forma muy común de robo de datos personales es la suplantación de identidad, es decir, hacerse pasar por otra persona o institución conocida para pedir sus datos mediante engaños (puede ser por correo electrónico, llamadas telefónicas, enlaces a sitios web maliciosos, descargar e instalar archivos afectados, etc.). Así, luego pueden acceder en forma fraudulenta a cuentas en aplicaciones, billeteras virtuales, plataformas de compra, etc. utilizando los datos personales de esa persona. Por eso, es muy importante prestar atención a nunca compartir contraseñas de acceso.

¿Qué es una **cookie**?

Algunos sitios web recopilan información de las acciones del usuario, a través de las llamadas **“cookies”**. Muchas veces nos avisan previamente qué tipo de información procesan y tenemos que expresar nuestro acuerdo para poder seguir viendo sus contenidos.

Una cookie es un archivo de datos que algunos sitios web, cuando los visitamos, envían a nuestro dispositivo para recopilar información. Su función es identificar y recordar cada usuario con sus configuraciones.

A la vez, permite crear un patrón del historial de navegación. Algunas cookies tienen usos de vigilancia invasiva y pueden afectar la privacidad. Por eso, se recomienda configurarlas con las mínimas autorizaciones posibles y eliminarlas periódicamente. También se puede habilitar la función de “no rastreo” tienen la mayoría de los navegadores o directamente usar aquellos servicios que no registran la información de sus usuarios.

Más info: **www.argentina.gob.ar/justicia/convosenlaweb/situaciones/tengo-que-aceptar-las-cookies-cuando-navego-en-internet**

La privacidad en redes sociales

Podemos elegir quién puede ver nuestras publicaciones agrupando según el nivel de confianza: mejores amigos, familia, personas conocidas, usuarios desconocidos, etc. Además, podemos regular a quién autorizamos o no el etiquetado de fotos donde aparecemos y filtrar quiénes pueden contactarnos, por ejemplo, que solo sean “amigos de mis amigos” o que no se le permita a cualquier usuario escribirnos al chat de mensajería. Es importante darse un momento para explorar a conciencia todas las opciones de configuración de cada plataforma.

Buenas prácticas

- Mantener nuestros perfiles en modo privado, para que solo las personas que elijamos puedan ver lo que publicamos.
- Evitar exponer datos personales, como direcciones, escuela, horarios de actividades.

- Revisar la lista de usuarios que tienen acceso a ver nuestros contenidos y a hablarnos por mensajería.
- Bloquear a los usuarios que nos incomoden o molesten.

¿Sabemos realmente quién está del otro lado de la pantalla?

Un contacto no es lo mismo que un amigo. En internet es muy fácil que alguien se haga pasar por otra persona y nos engañe. No sabemos si ese contacto desconocido es realmente quien dice ser. Por eso, es importante configurar las opciones de privacidad en las plataformas para que solamente podamos interactuar con los perfiles que elijamos. Y nunca compartamos información privada o sensible con gente a la que no conozcamos fuera de internet.

Es importante tomar estos cuidados porque hay personas que se aprovechan del anonimato de internet para acosar y hacer daño.

Cultura de la influencia

Hay personas que deciden mostrar públicamente sus vidas a través de las redes sociales, pero es importante tener en claro dos cosas:

- Lo que vemos en las pantallas no es todo. Siempre es un recorte, una construcción sobre algunos aspectos de lo que en realidad les pasa a esas personas.
- Configurar en modo público las cuentas en redes sociales conlleva riesgos.

Una cuenta pública está muy bien cuando tiene un objetivo claro y para eso necesita tener más alcance y seguidores, como por ejemplo para apoyar una causa, gestionar un emprendimiento, mostrar una expresión artística o compartir recomendaciones u opiniones sobre una temática delimitada.

En cambio, cuando se trata de perfiles personales es importante que estén en modo privado y que podamos elegir a conciencia con quién compartir cada momento de nuestra vida.

¿Cómo crear una contraseña segura?

Una contraseña es una combinación de números, letras y símbolos creada para proteger la información y los datos personales almacenados en cualquier dispositivo electrónico (computadora, tabletas y celulares). Otros tipos de contraseñas son: accesos con huella digital; reconocimiento facial o dibujo de patrones. Necesitamos contraseñas seguras para que no puedan descifrarlas los ciberdelincuentes que buscan robar información o violar nuestra privacidad.

Una contraseña debe tener:

- 8 caracteres como mínimo. A mayor cantidad de caracteres, es más segura;
- letras mayúsculas y minúsculas, números y símbolos;
- una contraseña segura es fácil de recordar pero difícil de adivinar.

Ideas para no olvidar la contraseña:

- Usar las primeras iniciales de una frase o canción.
- Reemplazar las vocales por números o símbolos.
- Usar iniciales de palabras que te sean familiares como por ejemplo: **CZ_Tt6m_ **(CafeZapatos_TomatesTokio6musica_)

¿Cómo evitar que nos roben las contraseñas?

- Evitar contraseñas débiles, como 123456 o TuNombre1234. Evitar datos predecibles, como nuestro nombre o fecha de nacimiento.
- No usar la misma clave para todo.
- Guardarlas en un documento cifrado en un procesador de texto o elegir gestores de contraseñas de empresas de seguridad reconocidas. No pegar las contraseñas en el monitor o el teclado.
- Cambiarla cada 60 o 90 días.

Más info: **www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-crear-una-contrase%C3%B1a-segura**

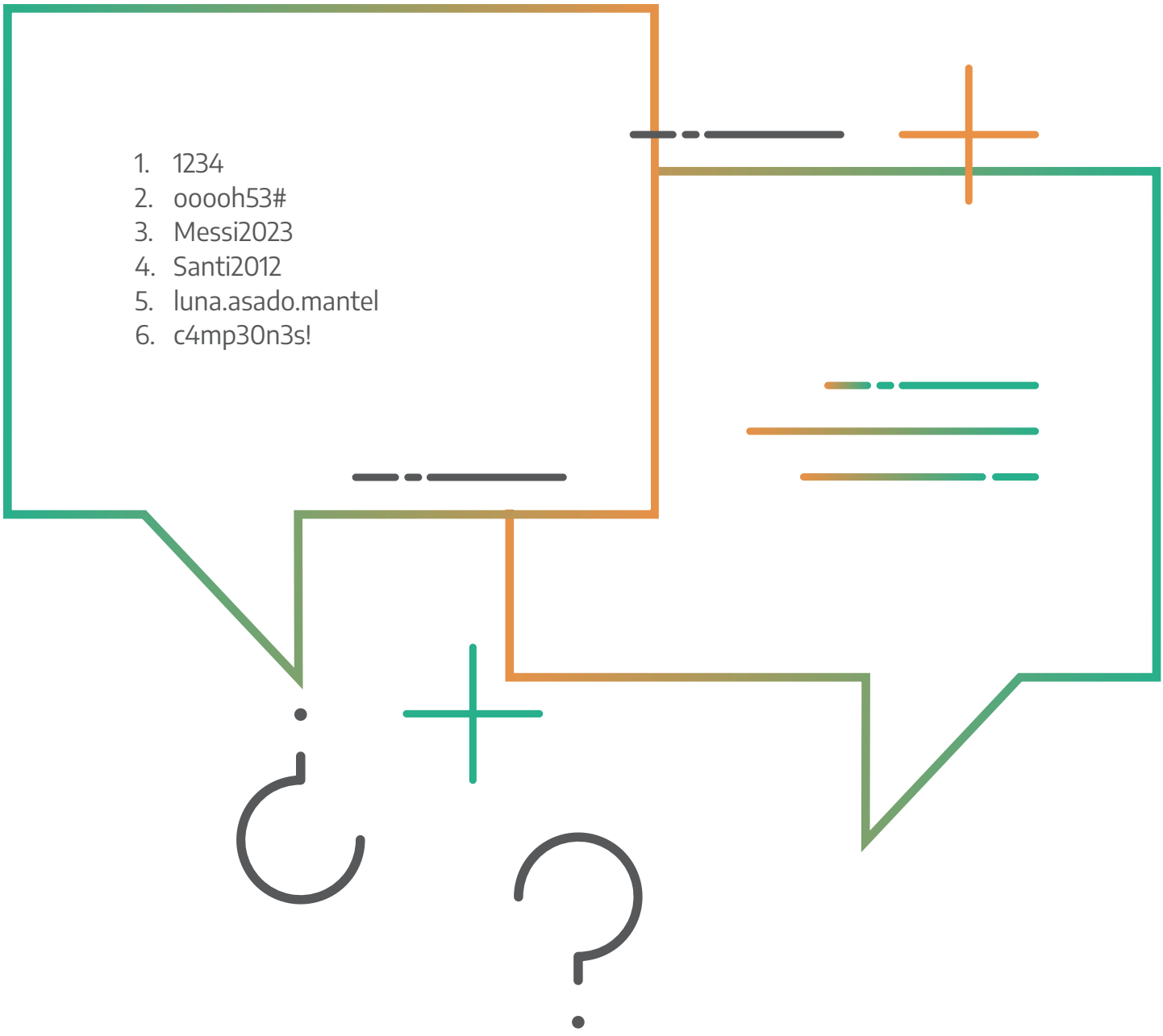
Tené cuidado a quién dejás entrar a tu vida online

Mirá este video de la publicidad de un banco privado que busca que tomemos conciencia sobre a quiénes damos acceso a nuestros datos, muchas veces sin prestarle la debida atención: **www.youtube.com/watch?v=TiN7dFdYaPg**

Probá tus conocimientos:

¿Cuáles contraseñas son más seguras?

1. 1234
2. ooooh53#
3. Messi2023
4. Santi2012
5. luna.asado.mantel
6. c4mp30n3s!



Respuestas: 2, 5, 6

5

¿Qué podemos hacer si tenemos un problema con nuestros datos personales en entornos digitales?

En este capítulo, conoceremos las historias de Bauti, More, Martu, Cata y Leo, cinco adolescentes que tuvieron diferentes problemas con el tratamiento de sus datos personales. Aprenderemos todo lo que podemos hacer y a quiénes acudir en caso de tener que enfrentar una de estas situaciones. También nos informaremos acerca de cómo actúa la Agencia de Acceso a la Información Pública (AAIP) cuando las empresas o entidades responsables de tratamiento de los datos personales no cumplen con sus obligaciones.

5 historias con datos personales en juego **¡Conocelas!**

Bauti

Derecho de conocer qué **datos personales** sobre mí tiene una empresa

Bauti, de 13 años, completó un formulario en línea con sus datos personales para abrir una cuenta en una nueva plataforma de videos en vivo. Tenía una bonificación para usarla gratis por tres meses y le interesó probarla. Pasado ese plazo, les escribió un correo pidiendo la baja y que borraran sus datos. Pero la empresa no respondió.

¿Qué pasó?

- La empresa niega el derecho de Bauti a conocer los datos personales que tiene almacenados en su base y a pedir que se eliminen.

¿Qué se puede hacer?

- Buscar las formas de contacto con la empresa y reiterar el pedido, mencionando que es un derecho contemplado en la Ley 25.326.
- Pedir asesoramiento en la Agencia de Acceso a la Información Pública.

Buenas prácticas para prevenir

- Conocer los términos y condiciones que aceptamos para el uso de aplicaciones y servicios en línea.
- Desinstalar aplicaciones que no usamos de los dispositivos.
- Cuando dejamos de usar un servicio, podemos pedir a la empresa la cancelación de nuestros datos personales de sus bases de datos.

More

Derecho a que se revisen las decisiones tomadas con base en el tratamiento automatizado de **datos personales**

More tiene 16 años y aplicó a una beca para un curso de idiomas que quiere hacer durante el verano. Completó un formulario digital con sus datos personales y entregó un texto donde relató su pasión por los idiomas y por qué necesitaba la beca para ingresar a la institución. Luego, recibió un correo informando que había sido rechazada, sin ninguna explicación. Ella sospecha que no fue bien evaluada.

¿Qué pasó?

- Su presentación fue analizada en forma automatizada (ver glosario) y una máquina tomó una decisión que la perjudica. Si los criterios de evaluación fueron inadecuados o poco transparentes, los resultados pudieron arrastrar sesgos discriminatorios.

¿Qué se puede hacer?

- Solicitar a la institución que explique la lógica y los criterios que usó la máquina para evaluar la postulación y pedir que una persona revise la decisión.
- Pedir asesoramiento en la Agencia de Acceso a la Información Pública.

Buenas prácticas para prevenir

- ¡Conocer nuestros derechos a la protección de datos personales para hacerlos valer!

Martu

Derecho a la **protección de imágenes** de niñas, niños y adolescentes

Martu tiene 12 años y es arquera del equipo de hockey del club de su barrio. El entrenador tomó fotos del último partido y su mamá las encontró en el sito web del club. Las chicas y sus familias no habían firmado ninguna autorización que permitiera al club difundir esas imágenes.

¿Qué pasó?

- El club publicó imágenes de las chicas sin el consentimiento de sus familias. En internet, quedan visibles a todas las personas y así quedan expuestas a que cualquier pueda descargarlas, copiarlas y usarlas en otros contextos.

¿Qué se puede hacer?

- Como adolescentes, podemos expresar si queremos o no que se publiquen nuestras imágenes y deben respetar esa decisión.
- Desde el club, deben dar de baja la publicación de las fotos en forma inmediata, hasta tener el consentimiento de las chicas y sus familias.
- Desde las familias, estar atentas al uso de las imágenes de sus hijos e hijas y reclamar que no se compartan sin su autorización.

Buenas prácticas para prevenir

- Tener en cuenta que deben pedirnos la autorización para el tratamiento de nuestras imágenes antes de difundirlas. Además, deben avisarnos previamente con qué fin las van a usar. Por ejemplo, si damos consentimiento para publicar las fotos en la web del club, eso no habilita al club a usarlas también en otros espacios, como por ejemplo en volantes de promoción de las actividades.
- Recordemos que, en cualquier momento, podemos arrepentirnos y retirar el consentimiento para que dejen de publicar nuestras fotos.
- Los clubes y otras instituciones pueden armar una guía con los pasos a seguir para pedir la autorización de uso de las imágenes a sus socios y, si tienen menos de 16 años, también deben tener la autorización de sus familias.

Thiago

Derecho a que los datos que nos pidan entregar sean **pertinentes y no excesivos**

Thiago, de 16 años, es un crack jugando al LOL y sabía que tenía posibilidades de ganar el campeonato que organizaba su municipio. Así que no dudó en completar el formulario de inscripción con todos sus datos personales. Hasta que algo le llamó la atención. ¿Era realmente necesario que le pidieran una imagen escaneada de su DNI como requisito para una competencia de videojuegos?

¿Qué pasó?

- Los organizadores del torneo pretendían recoger datos que eran excesivos en relación con la finalidad de la actividad.

¿Qué se puede hacer?

- Pedir a los organizadores que se constate la identidad de los participantes mostrando su DNI, pero sin necesidad de que guarden la imagen.
- Consultar con la AAIP y solicitar que se contacte con la municipalidad responsable del torneo para que aclaren el uso que le darán a los datos que no son necesarios para llevar adelante la actividad.

Buenas prácticas para prevenir

- Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

Cata

Derecho a la protección frente a abusos de **llamados publicitarios**

Cata se descargó una aplicación gratuita de retoques fotográficos porque quería editar las fotos de su cumple de 15. Se creó una cuenta como usuaria para poder acceder a todos los filtros que ofrece. En el formulario completó datos personales, como el nombre, el teléfono, el correo electrónico y también aceptó dar acceso a sus fotos, agenda de contactos, cámara y ubicación. Poco después, empezó a recibir mensajes publicitarios en su celular desde números desconocidos.

¿Qué pasó?

- La aplicación compartió los datos personales de sus usuarios con otras empresas, por ejemplo, de marketing, con o sin contar con su consentimiento en forma expresa y sin ofrecer toda la información claramente.

¿Qué podemos hacer?

- Incluir el número de teléfono en el Registro Nacional No llame, de la AAIP: **https://nollame.aaip.gob.ar/**
- Si nos siguen llamando a pesar de estar en el registro, podemos hacer una denuncia en el sitio web del Registro.

Buenas prácticas para prevenir

- Conocer los términos y condiciones antes de aceptar los contratos de uso de los servicios.
- Podemos retirar el consentimiento y pedir que se elimine nuestra información de las bases de datos de las empresas.
- Evaluar qué aplicaciones o servicios realmente queremos usar y descartar los que no sean necesarios.

¿Qué es el **Registro Nacional No Llame**?

Es una base de números telefónicos de las personas que expresaron que no quieren recibir llamadas publicitarias por vía telefónica, así como por aplicaciones de mensajes de texto o mensajería instantánea.

Una vez que se inscribe un número en el Registro, las empresas ya no pueden llamar para publicitar, ofertar, vender o regalar bienes o servicios. Si después de 30 días siguen haciéndolo, se puede realizar una denuncia ante el Registro.

El Registro se creó por la Ley 26.951 y el organismo a cargo de administrarlo es la Dirección Nacional de Protección de Datos Personales de la **Agencia de Acceso a la Información Pública**.

Conocé más: **nollame.aaip.gob.ar**

Leo

Derecho a la confidencialidad los **datos personales**

Leo y sus compañeros usan una plataforma educativa para sus clases en línea de 4to año de la escuela secundaria. Hace unos días, descubrieron que ingresando el apellido de sus compañeros pueden ver sus calificaciones y datos personales, incluyendo documento, correo electrónico, número de teléfono y dirección de sus casas.

¿Qué pasó?

- La empresa no resguarda correctamente los datos personales de sus usuarios y de esa forma pone en riesgo la confidencialidad de la información que tiene en su poder.

¿Qué podemos hacer?

- Pedir a la empresa que use mecanismos más seguros para no revelar la información de los usuarios.
- Pedir asesoramiento en la Agencia de Acceso a la Información Pública, llamando al (5411) 3988-3968 o escribiendo un correo a **datospersonales@aaip.gob.ar**

Buenas prácticas para prevenir

- Es importante conocer los términos y condiciones que las empresas nos piden aceptar para usar este tipo de servicios. Al aceptar el contrato, expresamos nuestro consentimiento para el tratamiento de nuestros datos personales, pero debe hacerse en forma segura.
- Pedir a la empresa que informe los mecanismos de seguridad que tienen disponibles para el tratamiento de datos personales. Elegir aquellas que tengan los estándares de seguridad más altos posible.

En caso de que las empresas o entidades responsables de tratamiento de los datos personales no cumplan con alguna de sus obligaciones, podemos acudir a la AAIP.

- Para enviar una consulta o pedir orientación, hay que llamar al (011) 3988-3968 o escribir a: **datospersonales@aaip.gob.ar**

- Para hacer una denuncia por incumplimiento de la Ley de Protección de Datos Personales, se debe ingresar a la sección de "Trámites" de su sitio web o al siguiente enlace: **www.argentina.gob.ar/servicio/denunciar-incumplimientos-de-la-ley-de-proteccion-de-datos-personales**

5 consejos

para proteger los datos y la privacidad de niños, niñas y adolescentes en entornos digitales

Limitar la exposición personal

No es necesario que **toda su información** personal esté en los perfiles de sus redes sociales o sitios webs.

Usar un avatar o un seudónimo puede ser más conveniente que una foto y el nombre y apellido.

Administrar preferencias de privacidad

Dialogá sobre lo que quieren mantener para su intimidad y qué quieren hacer público. Tendrán herramientas para **configurar la privacidad** de los perfiles que crean.

Preguntá ¿Quién querés que conozca esto? ¿Qué pasaría si alguien accede a esta información?

Diferenciar entre amistades reales y contactos virtuales

Explicales por qué no deben hablar, ni compartir información o fotos con **personas que no conozcan** en la vida real.

Existen usuarios creados para robar información, acosar y hacer daño en Internet.

Identificar correos electrónicos o mensaje seguros

Dales **herramientas** para que identifiquen remitentes seguros de correos y mensajería instantánea y eviten compartir datos involuntariamente.

Promovamos este hábito a todas las personas.

Configurar dispositivos para reducir riesgos

Ayudalos a configurar y usar dispositivos móviles y computadoras **de manera segura**.

- Evitar instalar programas o aplicaciones dudosas o innecesarias.
- No utilizar redes de Internet de acceso público.
- Mantener cerradas sesiones de usuario sin uso.
- Habilitar la geolocalización cuando la necesitan.

Solicitá asesoramiento o denunciá el incumplimiento de la Ley N° 25.326 de Protección de Datos Personales **ante la AAIP en** datospersonales@aaip.gob.ar

AAIP
Transparencia
Acceso a la Información
Protección de Datos Personales

Glosario

Anonimización: la aplicación de medidas dirigidas a impedir la identificación o reidentificación, ya sea por el Responsable, Encargado o un Tercero, de una persona humana, sin esfuerzos o plazos desproporcionados o inviables, teniendo en cuenta factores como los costos y el tiempo necesario para la identificación o reidentificación de la persona a la luz de la tecnología disponible en el momento del tratamiento.

Autodeterminación informativa: el derecho de la persona a decidir o autorizar de forma libre, previa, expresa e informada la recolección, uso o tratamiento de sus datos personales, así como de conocer, actualizar, rectificar o suprimirlos, o controlar lo que se hace con su información. Comprende un conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales.

Base de datos: conjunto de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica. Indistintamente, se la puede denominar también como archivo, registro, fichero o banco de datos.

Consentimiento del Titular de los datos: toda manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica por medio de la cual el Titular de los datos o su representante, o el Titular de la responsabilidad parental, guarda o tutela en caso de niña o niño, acepta, mediante una declaración o una clara acción afirmativa, que se traten sus datos personales.

Datos biométricos: aquellos datos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única, tales como imágenes faciales o datos dactiloscópicos, entre otros.

Datos genéticos: aquellos datos relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre su fisiología o salud.

Datos personales: información referida a personas humanas determinadas o determinables. Se entiende por determinable la persona que puede ser identificada directa o indirectamente por uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social o de otra índole.

Datos personales sensibles: aquellos que se refieren a la esfera íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad, a la preferencia u orientación sexual, datos genéticos o biométricos cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su Titular y que estén dirigidos a identificar de manera unívoca a una persona humana.

Elaboración de perfiles: toda forma de tratamiento automatizado o parcialmente automatizado de datos personales consistente en utilizar éstos para evaluar determinados aspectos de una persona humana; en particular, para analizar o predecir cuestiones relativas al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, etnia, género o movimientos de dicha persona.

Incidente de seguridad de datos personales: ocurrencia de uno o varios eventos en cualquier fase del tratamiento que atenten contra la confidencialidad, la integridad y la disponibilidad de los datos personales.

Responsable de tratamiento de datos personales: persona humana o jurídica, pública o privada, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

Titular de los datos: persona humana cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

Tratamiento de datos: cualquier operación o conjunto de operaciones, automatizada, parcialmente automatizada o no automatizada, realizada sobre datos personales, que permita, de manera enunciativa, la recolección, conservación, organización, estructuración, almacenamiento, modificación, relacionamiento, evaluación, bloqueo o destrucción, publicación y, en general, su procesamiento, así

como también su cesión a través de comunicaciones, consultas, interconexiones o transferencias.

Las definiciones corresponden al texto del proyecto para una nueva ley de protección de datos personales. **www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf**

Bibliografía y referencias utilizadas

AAIP - Proyecto para actualización de ley de Protección de Datos Personales, 2023. Disponible en: **www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf**

AAIP- Guía para entidades públicas y privadas en materia de Transparencia y Protección de Datos Personales para una Inteligencia Artificial responsable. Disponible en: **www.argentina.gob.ar/sites/default/files/aaip-argentina-guia_para_usar_la_ia_de_manera_responsable.pdf**

Calvo, Ernesto; Aruguete, Natalia. Fake News, trolls y otros encantos, Ed. Siglo XXI editores, 2020.

Fundación Sadoski, "Diez preguntas frecuentes y urgentes sobre Inteligencia Artificial", 2024. Disponible en: **program.ar/wp-content/uploads/2024/08/Diez-preguntas-frecuentes-y-urgentes-sobre-Inteligencia-Artificial.pdf**

Magnani, Esteban, La jaula del confort, Ed. Autoría, 2019. Disponible en: **www.estebanmagnani.com.ar/2019/10/30/la-jaula-del-confort/**

Red Iberoamericana de Protección de Datos, Recomendaciones Generales para el Tratamiento de Datos en Inteligencia Artificial, 2019. Disponible en: **www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf**

Red Global para el Cumplimiento de la Privacidad 2024 sobre patrones de diseño engañosos, 2024. Disponible en: **www.argentina.gob.ar/noticias/la-aaip-comparte-los-resultados-del-estudio-global-sobre-disenos-de-sitios-web-y**

UNICEF, Comunicación, infancia y adolescencia: Guías para periodistas. Protección de datos personales. 2017. Disponible en: **www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-4_ProteccionDatos_Interior_WEB.pdf**

Normativa

Convención internacional sobre los Derechos del Niño
www.argentina.gob.ar/normativa/nacional/ley-26061-110778

Constitución Nacional
www.argentina.gob.ar/normativa/nacional/ley-24430-804

Código Civil y Comercial de la Nación - Ley Nº 26.994
www.argentina.gob.ar/normativa/nacional/ley-26994-235975

Ley N° 25.326 de Protección de los Datos Personales
www.argentina.gob.ar/normativa/nacional/ley-25326-64790

Ley N° 27.483. Convenio para la protección de personas en el tratamiento automatizado de datos personales
www.argentina.gob.ar/normativa/nacional/ley-27483-318245

Ley N° 26.061 de Protección Integral de los Derechos de Niñas, Niños y Adolescentes
www.argentina.gob.ar/normativa/nacional/ley-26061-110778

www.argentina.gob.ar/AAIP
@AAIPargentina
aaipargentina
@AAIPargentina
datospersonales@aaip.gob.ar

AAIP
Argentina

Presidencia de la Nación
República Argentina