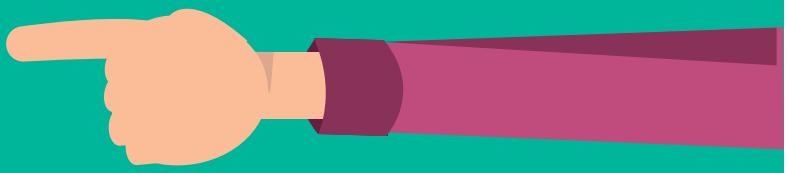


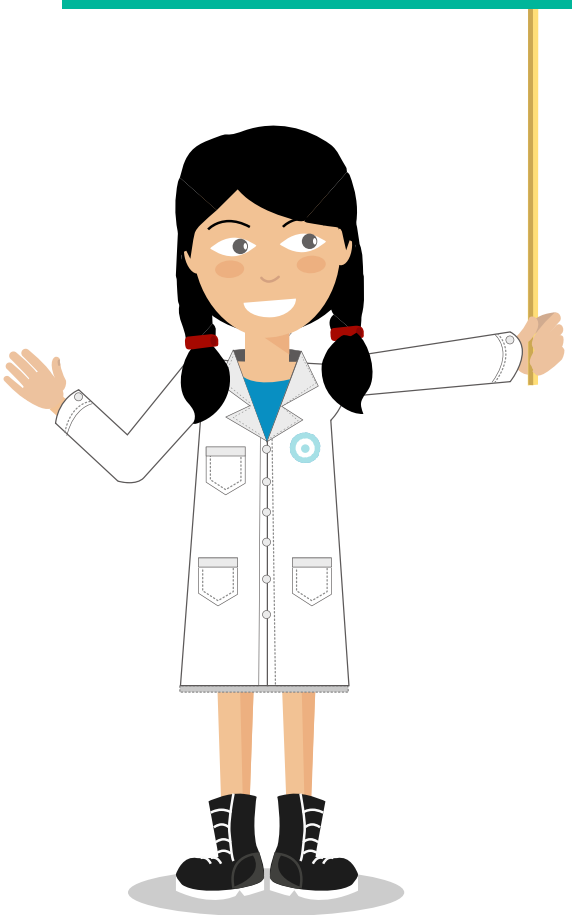
DATOS PERSONALES Y AMENAZAS EN LA WEB: LEYES QUE TE PROTEGEN

EL PROBLEMA DE LA PRIVACIDAD EN LA WEB

Muchas veces subís tus fotos, videos o archivos personales a la web desconociendo los **riesgos** que esto implica. Pero ¿sabías que existen **leyes** que garantizan tu protección ante cualquier tipo de violación a tu **privacidad e intimidad?**

Una de ellas es la **ley 25.326 de Protección de Datos Personales** que resguarda la información personal que se encuentren en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que se registre sobre ellas. Esto está establecido en nuestra **Constitución Nacional,** en el tercer párrafo del **artículo 43:**

> "Toda persona podrá interponer esta acción (acción expedita y rápida de amparo) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística".



¿QUÉ SON LOS DATOS PERSONALES?

Los **datos personales** son información de cualquier tipo referida a las personas, por ejemplo: nombre y apellido, número de documento, domicilio, dirección de correo electrónico, número de teléfono, fecha de nacimiento, etc.
Existe un tipo especial de datos personales que se denominan **datos sensibles.** Estos cuentan con una mayor protección porque se relacionan con temas delicados o íntimos, como el origen racial o étnico, opiniones políticas, creencias religiosas, filosóficas o morales, afiliación sindical e información sobre la salud o la sexualidad de las personas.

En el caso de los **datos relativos a la salud**, la ley contempla que los establecimientos sanitarios, ya sean públicos o privados, y los médicos y otros profesionales de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes siempre que respeten los principios del secreto profesional.

¿QUÉ DERECHOS CONTEMPLA LA LEY DE PROTECCIÓN DE DATOS PERSONALES?

Esta ley otorga los siguientes derechos:

- **Derecho de información:** toda persona puede **pedir información** sobre la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. Esta consulta, que es **pública y gratuita**, se puede realizar en la **Dirección Nacional de Protección de Datos Personales,** que cuenta con un **Registro Nacional de Bases de Datos**, en el cual tienen que inscribirse todos los archivos, registros, bases o bancos de datos públicos y privados destinados a proporcionar informes.

- **Derecho de acceso:** permite a cada persona conocer la información sobre sí mismo que esté disponible en una base de datos. Con solo demostrar la identidad, el individuo tiene el derecho a obtener información de sus datos personales incluidos en las bases de datos públicas o privadas, destinadas a proveer informes. El responsable de la base de datos en cuestión debe proporcionar la información solicitada dentro de los diez días corridos de haberle sido solicitada.

- **Derecho de rectificación o actualización:** si los datos personales están anotados en forma incorrecta o desactualizada en una base de datos, la persona afectada tiene derecho a pedir que sean **corregidos o actualizados.**
- **Derecho de supresión:** se puede pedir que **se elimine la información** sobre la persona que sea falsa o esté disponible en forma ilegal.

¿CÓMO SE AUTORIZA EL USO DE LOS DATOS PERSONALES?

Para que los datos puedan ser utilizados se requiere la **autorización o consentimiento** de la persona afectada.

Es muy importante que, antes de dar la autorización, la persona se informe sobre la **finalidad** para la que serán usados los datos y a quiénes pueden ser entregados. Siempre deberá ser respetada la finalidad para la que se autorizó el uso de los datos.

En el caso de **menores de 18 años**, los padres o representantes legales deben dar la autorización en su nombre.

En ciertos casos, no se requiere la autorización: si los datos utilizados incluyen solo el nombre, DNI, ocupación, identificación tributaria o previsional, fecha de nacimiento y domicilio; si son datos incluidos en fuentes de acceso público irrestricto como la guía telefónica, o si los requieren organismos estatales en ejercicio de su función o en cumplimiento de una ley.

RIESGOS Y AMENAZAS WEB

La circulación de imágenes, videos e información en Internet conlleva algunos riesgos, problemas o situaciones a tener en cuenta a la hora de publicar nuestros propios archivos.

Al momento de compartir en la web hay que saber identificar y cuidarse de conductas como el **grooming, el ciberbullying y el sexting**. Pero, ¿de qué se tratan estas conductas?

GROOMING

El **grooming o ciberacoso** es la acción deliberada de un adulto de acosar sexualmente a un niño, niña o adolescente mediante el uso de Internet.

Los sujetos que realizan grooming –también llamados groomers o acosadores– suelen generar un perfil falso en Internet haciéndose pasar por un menor de edad y buscan así generar confianza con un niño, niña o adolescente para entablar una relación de amistad. Una vez logrado esto, los acosadores suelen pedirle a la víctima fotos o videos con contenido sexual. Cuando lo consiguen, suele iniciarse un período de chantaje en el que el sujeto amenaza al menor con hacer público ese material si no envía nuevos videos o fotos o si no accede a un encuentro personal. Otras veces, en el marco de la relación de confianza previamente entablada, el menor de edad accede a un encuentro personal con el groomer desconociendo la identidad del acosador.

En otras oportunidades, el sujeto obtiene fotos o videos sexuales de la víctima, sin necesidad de contacto previo, mediante el robo de contraseña o hackeo de cuentas y posteriormente inicia el período de chantaje.

Con respecto a estas conductas se debe saber que en noviembre de 2013 se sancionó la **Ley 26.904** en la que se incorporó la figura de grooming o ciberacoso sexual al **artículo 131 del Código Penal**. Esta modificación establece que será **penado** "con prisión de 6 meses a 4 años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

CIBERBULLYING

Se habla de **ciberbullying** cuando un menor sufre amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por otro menor mediante la publicación de textos, imágenes, videos y audios a través de medios electrónicos, como teléfonos celulares, correo electrónico, mensajería instantánea, redes sociales, juegos online, entre otros.

Las víctimas de ciberbullying suelen tener cambios en la conducta: tristeza o depresión y variación en su rendimiento escolar. Por lo general, están en contacto permanente con dispositivos electrónicos para mantenerse al día sobre las publicaciones que hacen sobre ellos en las redes sociales y otros medios. Uno de los síntomas que se presenta con frecuencia es el deseo de estar a solas en sus habitaciones.

SEXTING

El **sexting** implica la circulación de un contenido sexual a través de dispositivos móviles como teléfonos celulares, tabletas, etc.

La denominación surge de la combinación de las palabras en inglés sex (sexo) y texting (enviar mensajes de texto por teléfono celular). El término fue ampliando su significado con los avances tecnológicos. Actualmente describe al envío de imágenes y videos con contenido sexual, de sí mismo o misma, no solo vía mensaje de texto sino, también, mediante mensajería instantánea, foros, posteos en redes sociales o por correo electrónico.

Cuando una imagen es enviada a uno o varios contactos, estos pueden reenviarla e introducirla a la web. La circulación de las imágenes puede viralizarse, de manera rápida y fácil como cuando se propaga un virus. Puede incluso caer en manos de personas con malas intenciones, que editen nuestro material y lo hagan circular buscando perjudicarnos.

Por eso es necesario ser muy cuidadoso al momento de enviar datos personales, fotos o videos ya que, una vez enviados, podemos perder el control sobre su circulación y difusión.

Fuentes:

Dirección Nacional de Protección de Datos Personales
www.jus.gob.ar/datos-personales.aspx

Programa Con Vos en la Web
www.convosenlaweb.gob.ar

Ficha del documento

Nivel: Nivel Básico de Educación Secundaria

Disciplina: Ciencias Sociales

Fecha De Publicación: 15/04/2018

ACTIVIDAD
para el aula

EJERCICIO DE DEBATE Y REDACCIÓN

1. Formar equipos de dos o tres personas.

2. Investigar en diarios, revistas o internet noticias acerca de casos de grooming o ciberbullying.

3. Responder las siguientes preguntas:

- ¿Quiénes suelen ser las víctimas?
- ¿Cómo afecta el acoso la conducta de las víctimas?
- ¿De qué manera operan los acosadores?
- ¿De qué forma se los puede detener?

4. Debatan en el grupo:

- ¿Cómo es su experiencia con las redes sociales?
- ¿Comparten información sobre su vida cotidiana en las redes sociales? ¿Qué tipo de información suelen compartir?
- ¿Alguna vez se sintieron intimidados por otro usuario? ¿Por qué? ¿Cómo lo manejaron?

5. A partir de la información reunida redacten un breve informe sobre la problemática tratada.

Si les gustó la actividad y quieren compartirla con nosotros, pueden mandar su trabajo a congresodeloschicos@congreso.gob.ar