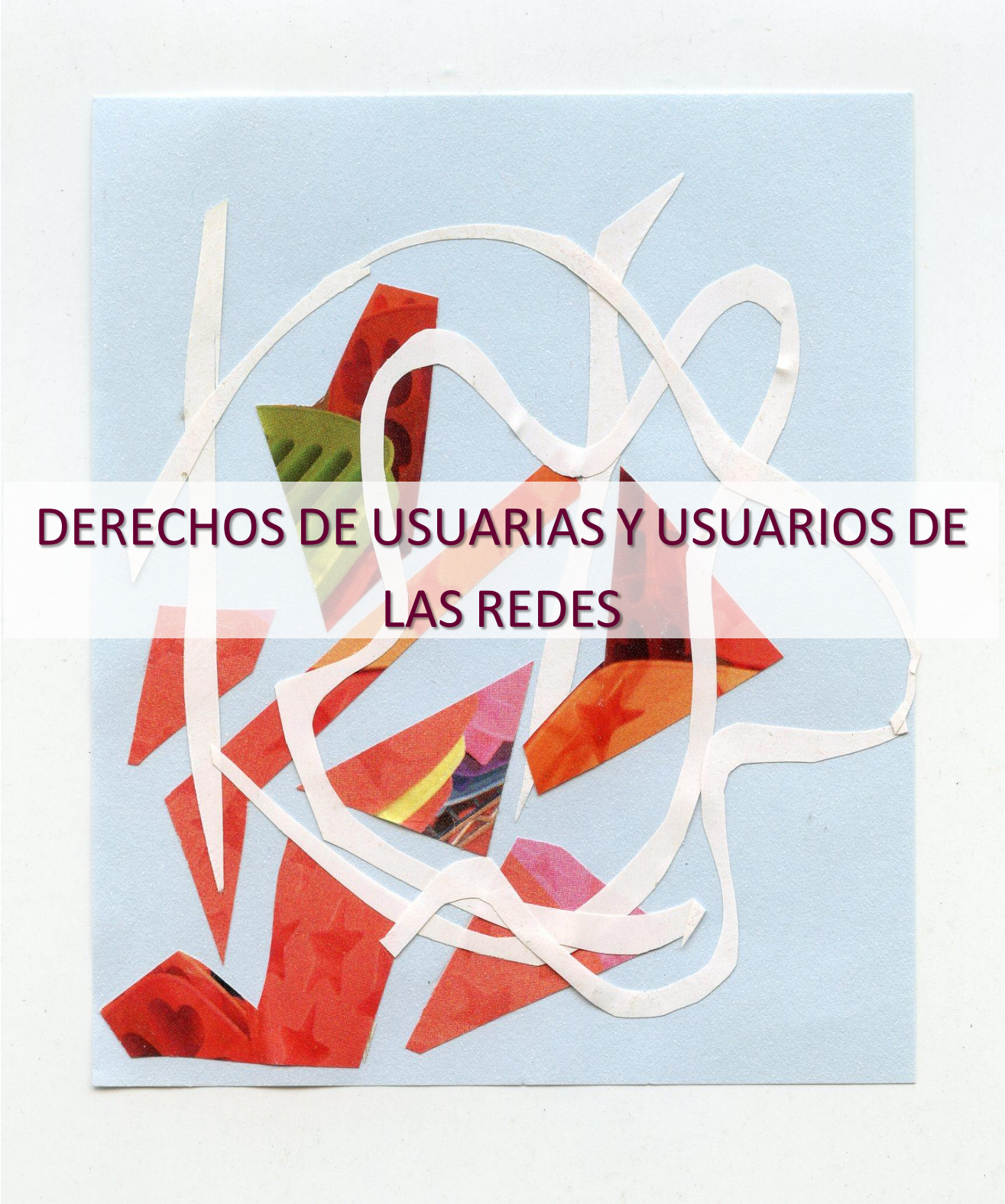
Poder Judicial de la Ciudad de Buenos Aires
Consejo de la Magistratura

PAJDU
Dirección de Participación Ciudadana, Acceso a Justicia y Derechos Universales.



DERECHOS DE USUARIAS Y USUARIOS DE LAS REDES

PROGRAMA DE ACCESO COMUNITARIO A JUSTICIA

Programa de Acceso comunitario a Justicia

Secretaría de Planificación

Dirección de Participación Ciudadana, Acceso a Justicia y Derechos Universales

Consejo de la Magistratura de CABA

ÍNDICE

INTRODUCCIÓN

Las TIC's (Tecnologías de la Información y la Comunicación) inspiran a explorar, a ser creativos, a comunicarse y a aprender, pero es importante que se cuente también con información y estrategias de protección ante los posibles riesgos que pueden surgir en los espacios digitales.

Su función inicial es la de brindar información para que el usuario se pueda comunicar transformando las herramientas cotidianas y comúnmente usadas en el desarrollo diario de las actividades racionales humanas, esperando relacionar a las personas y permitiéndoles acceder a la información y al conocimiento, por medio de estas, se puede interactuar fácilmente.

Estas tecnologías son el lugar donde mayor información personal se genera y se comparte, fuente de recursos para identificar a una persona. Los datos que se alojan en la web y se asocian a la identidad de una persona, constituyen la manera que otros usuarios tienen de conocerla.

Pero también existen las siglas TAC significan Tecnologías del Aprendizaje y del Conocimiento, tiene como objetivo establecer una relación entre la tecnología y el conocimiento adquirido a través de la tecnología. A través de estas se crea, se comparte, se difunde y se debate la información relacionada con el manejo del conocimiento tecnológico, llevan el aprendizaje y las herramientas necesarias para la asimilación de información diferente a un nivel donde el cambio y la participación social se hacen evidentes.

Por otra parte, están las TEP son las Tecnologías para el Empoderamiento y la Participación, estas tecnologías hacen referencia al mundo social donde se puede trabajar sin límites y sin tener contacto con otras personas, sino que por el contrario existe una mayor interacción con el computador, donde los usuarios pueden acercarse y colaborar entre sí como creadores de contenidos generado por consumidores en una comunidad virtual.

Las TIC, TAC y TEP se relacionan directamente debido a que se pueden asociar como tecnologías interdependientes e independientes, específicamente porque se refieren tanto a la tecnología, como al conocimiento y al aprendizaje sin importar que cada una de ellas aporte conceptos diferentes

I.- NORMATIVA

LEGISLACIÓN INTERNACIONAL

- Convención sobre los Derechos de los Niños
- Ley 26.388 Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer: Convención de Belem do Para
- Protocolo Facultativo CEDAW
- Convención sobre la eliminación de todas las formas de discriminación contra la mujer [CEDAW]
- Conferencia sobre la Población y el Desarrollo - El Cairo - 1994

LEGISLACIÓN NACIONAL

- Ley n° 25.326 (2000) **"Protección de datos personales"**: tiene por objeto proteger la información personal de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables, y explícita la confidencialidad del responsable del tratamiento de los mismos (incluyendo la protección de la privacidad e intimidad en internet).
- Ley 26.061 de Protección Integral de los derechos de las Niñas, Niños y Adolescentes
- Ley 26485 de Protección Integral contra las Mujeres define violencia contra la mujer, tipos y modalidades. Dispone la promoción de políticas públicas para efectivizar lo establecido en la ley y designa un organismo encargado para ello.
- Ley 26743 de Identidad de Género

CÓDIGO PENAL:

La Ley 26388 incorporó los siguientes delitos informáticos al Código Penal:

- Art. 128: sanciona a quien financie, publique o distribuya toda representación de un menor dedicado a actividades sexuales explícitas o de sus partes genitales con fines predominantemente sexuales.

- Art. 131 del Código Penal. Es la acción deliberada de un adulto de contactar a una persona menor de edad, a través de medios electrónicos y cualquier otra tecnología de transmisión de datos, con el objeto de ganar su confianza y cometer un delito contra la integridad sexual de la misma.

- Art 153: sanciona al que abriere o accediere indebidamente a una comunicación electrónica que no le esté dirigida; o se apoderare indebidamente de una comunicación electrónica; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

- Art. 153 bis: sanciona el acceso no autorizado a un sistema o dato informático de acceso restringido (Acceso indebido).

- Arts. 155: sanciona a quien publique indebidamente una comunicación electrónica, que no estaba destinada a la publicidad, si el hecho causare o pudiere causar perjuicios a terceros.

- Art. 173: sanciona al que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos (Fraude Informático).

- Art. 183: sanciona a quien altere, destruya o inutilice sistemas informáticos o venda o introduzca cualquier programa destinado a causar daños (Daño Informático).

- Art. 184, inc. 5º y 6º: Daño Informático agravado. Cuando el daño es producido a datos, documentos, programas, o sistemas informáticos públicos o bien, cuando se ejecutara en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, medios de transporte, etc.

- Art. 197: sanciona a aquel que entorpezca o interrumpa la comunicación de cualquier tipo o resista con violencia el restablecimiento de la comunicación interrumpida.

LEGISLACIÓN DE LA CIUDAD DE BUENOS AIRES

- Ley 5.775/16 para la Prevención del Ciberacoso Sexual a Menores (Grooming)

- Ley 114/98 Protección Integral de los Derechos de las Niñas, Niños y Adolescentes

- Ley 863 de Protección de Menores en establecimientos comerciales que brindan acceso a Internet

- Ley 1845 Protección de Datos Personales

- Ley 5742 - Acoso Sexual Callejero en Espacios Públicos o de Acceso Público CABA

CÓDIGO CONTRAVENCIONAL

- Art. 64: Suministro de material pornográfico a menores de edad a través de medios informáticos.

- Art. 67 (Acoso Sexual) Se entiende por acoso sexual a aquellas conductas físicas o verbales de connotación sexual, basadas en el género, identidad y/u orientación sexual, realizadas por una o más personas en contra de otra u otras, que afectan su dignidad y derechos fundamentales, creando en ellas intimidación, hostilidad, humillación o un ambiente ofensivo en los espacios públicos y en los espacios privados de acceso público. Una de las posibles manifestaciones del acoso es mediante fotografías y grabaciones no consentidas.

- Artículo 71 bis Difusión no autorizada de imágenes o grabaciones íntimas. Quien difunda, publique, distribuya, facilite, ceda y/o entregue a terceros imágenes, grabaciones y/o filmaciones de carácter íntimo sin el consentimiento de la persona y a través de cualquier tipo de comunicación electrónica, de transmisión de datos, páginas web y/o a través de cualquier otro medio de comunicación, siempre que el hecho no constituya delito, es sancionado con una multa de cuatrocientas (400) a mil novecientas cincuenta (1950) unidades fijas o cinco (5) a quince (15) días de trabajo de utilidad pública o con tres (3) a diez (10) días de arresto. El consentimiento de la víctima para la difusión, siendo menor de 18 años, no será considerado válido.
  Tampoco podrá alegarse el consentimiento de la víctima en la generación del contenido como defensa a la realización de la presente conducta.
- Acción dependiente de instancia privada con excepción de los casos donde la víctima sea menor de 18 años de edad.

No configura contravención el ejercicio del derecho a la libertad de expresión

- Artículo 71 ter. - Hostigamiento digital. Quien intimide u hostigue a otro mediante el uso de cualquier medio digital, siempre que el hecho no constituya delito, es sancionado con multa de ciento sesenta (160) a ochocientas (800) unidades fijas, tres (3) a diez (10) días de trabajo de utilidad pública, o uno (1) a cinco (5) días de arresto.
- Acción será dependiente de instancia privada con excepción de los casos donde la víctima fuese menor de 18 años de edad.
- No configura hostigamiento digital el ejercicio del derecho a la libertad de expresión.

- Artículo 71 quater. Agravantes. En las conductas descriptas en los artículos 71 bis y 71 ter, las sanciones se elevan al doble cuando son realizadas:

1. Cuando la víctima fuera menor de 18 años, mayor de 70 años, o con discapacidad.

2. Cuando la contravención se cometa con el concurso de dos (2) o más personas.

3. Cuando la contravención sea cometida por el/la jefe, promotor u organizador de un evento o su representante artístico.

4. Cuando la contravención sea cometida por el/la cónyuge, ex cónyuge, o a la persona con quien mantiene o ha mantenido una relación de pareja, mediare o no convivencia.

5. Cuando la contravención sea cometida por un familiar en el 4to. grado de consanguinidad o 2do. grado de afinidad.

6. Cuando la contravención se cometa con información que no habría sido develada sin que medie el engaño.

7. Cuando la contravención sea cometida mediante la utilización de identidades falsas o anónimas o mediando la suplantación de la identidad de otra persona humana o jurídica.

Artículo 71 quinquies. Suplantación digital de la Identidad Quien utiliza la imagen y/o datos filiatorios de una persona o crea una identidad falsa con la imagen y/o datos filiatorios de una persona mediante la utilización de cualquier tipo de comunicación electrónica, transmisión de datos, página web y/o cualquier otro medio y se haya realizado sin mediar consentimiento de la víctima, siempre que el hecho no constituya delito, es sancionado con una multa de Ciento sesenta (160) a cuatrocientas (400) unidades fijas o uno (1) a cinco (5) días de trabajo de utilidad pública o de uno (1) a cinco (5) días de arresto.

Las sanciones se elevan al doble cuando:

a. La conducta sea realizada con la finalidad de realizar un banco de datos con la información obtenida.
b. La víctima fuera menor de dieciocho (18) años, mayor de 70 años, o con discapacidad.
c. La contravención sea cometida por el/la cónyuge, ex cónyuge, o a la persona con quien mantiene o ha mantenido una relación de pareja, mediare o no convivencia.
d. La contravención sea cometida por un familiar de hasta el cuarto grado de consanguinidad o segundo grado de afinidad.
e. La contravención sea cometida con el objeto de realizar una oferta de servicios sexuales a través de cualquier medio de comunicación.

El consentimiento de la víctima, siendo menor de 18 años, no será considerado válido.

Acción dependiente de instancia privada con excepción de los casos donde la víctima fuere menor de 18 años de edad.

No configura suplantación de identidad el ejercicio del derecho a la libertad de expresión.

(Modificado por Art. 6 de la Ley Nº 6128, BOCBA 5531 del 07/01/2019)

Esta expresión hace referencia a **la facultad que tiene una persona de solicitar a las empresas o a los motores de búsqueda que eliminen o bloqueen un dato personal** suyo por considerar que afecta alguno de sus derechos fundamentales. El término surgió en 1990 y está relacionado con la protección de datos personales, el derecho a la privacidad y el derecho al honor.

Si bien los motores de búsqueda y las redes sociales no son generadores de información, son los principales vehículos de la misma, permitiendo su difusión masiva. En este sentido, en la red existen contenidos que pueden aparecer en los resultados de una búsqueda en estos espacios que pueden resultar perjudiciales o discriminatorios para la persona implicada. **A partir de este derecho, es posible solicitar la supresión, bloqueo o desindexación de la información publicada** debido a que el usuario la considera perjudicial para sí mismo y, además, obsoleta o no relevante por el transcurso del tiempo.

En nuestro país, este derecho no está en vigencia y sólo se han instrumentado acciones de eliminación de datos para algunos aspectos vinculados al mundo bancario y de las finanzas. El caso más emblemático lo representa el que vivó la modelo María Belén Rodríguez en el año 2006, que se vio inmersa en la situación en la que su nombre aparecía en páginas web vinculadas a ofertas sexuales. En el juicio llevado adelante durante ocho años contra los buscadores **Google** y **Yahoo**!, hubo, en primera instancia, resoluciones favorables a la demandante pero, finalmente en 2014, la Corte Suprema falló en favor de los buscadores. A pesar de la resolución, dicho precedente dejó abierta la posibilidad de hacer un análisis más profundo y darle a la cuestión un tratamiento parlamentario acorde con los tiempos que corren.

¿QUÉ ES LA HUELLA DIGITAL?

La huella digital **es el rastro que dejás al navegar en Internet**.
Cada vez que haces un “click” o das un “me gusta” en las redes sociales, o cuando usas una aplicación desde tu celular o tu computadora, dejás información personal. Los datos que genera tu actividad en la Internet crean lo que se llama “huella digital”.

¿QUÉ TIPO DE DATOS COMPONEN NUESTRA HUELLA DIGITAL?

La huella digital está compuesta por:

Debemos recordar que cuando subimos algún dato o imagen a la web, es difícil de borrar. Aunque se borre una publicación, no se elimina la totalidad de esa referencia

- **Datos públicos**: son los datos de la obra social, cuit o cuil, declaraciones de impuestos, domicilios en las facturas de servicios, resúmenes de tarjetas de crédito, cargos, becas, resultados de sorteos, resoluciones judiciales.
- **Datos publicados por otros**: son fotos, posteos de amigos, familiares, clubes o espacios de pertenencia en redes sociales.
- **Datos que generás vos**: posteos, comentarios, fotos en redes sociales y foros. Formularios que completaste, contenidos que compartiste en plataformas como tu currículum, perfiles en redes de contactos u otros contenidos como listas de reproducción y videos favoritos.

¿PARA QUÉ SE USAN LOS DATOS RECOPILADOS DE NUESTRA HUELLA DIGITAL?

Los proveedores de servicios de Internet y las plataformas y redes que brindan servicios para navegar intercambian información de los perfiles de sus clientes y estadísticas sobre sus transacciones. Esta industria es un enorme motor económico que mueve (y financia) gran parte de Internet.

La tecnología para crear perfiles de los usuarios de Internet se ha vuelto cada vez más sofisticada. Pocos usuarios se dan cuenta del valor de sus huellas digitales.

Las huellas digitales son procesadas por personas y por robots e inteligencias artificiales que forman parte del complejo sistema donde se comparten y monetizan los datos.

¿CÓMO SE RECOPILAN LOS DATOS DE MI HUELLA DIGITAL?

Los datos **se recopilan a través de las "cookies"**. Las "cookies" son una cadena de letras y números, sin ningún significado intrínseco que un sitio web envía a su navegador web. **Esta información permite a los proveedores de servicios de Internet vincular todas las acciones realizadas por un usuario y convertirlas en un hilo conectado.**

Las cookies son necesarias para aumentar la usabilidad de Internet, por ejemplo si entrás muy seguido a una página, al haber guardado las cookies se cargará más rápidamente que si entrás a una página nueva. También pueden ayudar a que las transacciones individuales sean más seguras.
No podemos navegar sin cookies. Este es el motivo por el cual hay cookies por todas partes.

Las empresas usan los datos de las huellas digitales para crear "perfiles" de usuarios y vender estos datos a otras empresas como potenciales consumidores de sus productos.

¿CÓMO GESTIONO MI HUELLA DIGITAL?

- Los sitios te avisan que están recolectando datos. Decidí si las autorizaciones para recolectar cookies que das a los sitios que navegás son permanentes o transitorias.
- Configurá la privacidad de tus redes sociales para que no se exponga toda tu información personal.
- Navegá de incógnito
- Configurá el Do not Track
- Configurá las alertas de Google para que no existan datos personales innecesarios en la web. Podés ver cómo hacerlo en este tutorial de Con vos en la Web
- Denunciá aquellas páginas que exponen información personal sin tu consentimiento.

La huella digital incluye las publicaciones que un usuario realiza, aquellas en las que sea etiquetado o mencionado, las fotos o videos personales o subidos por otros, las páginas web donde se cite su nombre, las cuentas de usuario en redes sociales que estén asociadas a su nombre real, las noticias referidas a su persona, y la participación como usuario en foros, salas de juegos, de chat u otros.

CÓMO SE CONSTRUYE LA HUELLA DIGITAL:

Puede ser de tres maneras:
→ **ACCIÓN PROPIA:** Publicaciones que hace un usuario en redes sociales, blogs, sitios web como diarios o foros, dando su identidad.

→ **OMISIÓN:** No tener cuentas en redes sociales o participación web es de por sí un dato que se incluye en nuestra identidad digital cuando alguien busca información sobre nosotros.

→ **ACCIONES DE OTROS:** Publicaciones en donde el usuario es citado o nombrado por otro.

DATOS PERSONALES Y PRIVACIDAD

Los datos personales son información de cualquier tipo que puede ser usada para identificar, contactar o localizar a una persona. Entre ellos **se encuentran número de documento, nacionalidad, sexo, estado civil, número de teléfono y/o celular, huellas digitales, dirección de correo electrónico, actividades, etcétera**.

CONFIGURACIÓN DE SEGURIDAD EN DISPOSITIVOS. ATRIBUTOS PARA TENER UNA CONTRASEÑA ROBUSTA

Personal: cada persona que acceda a un sistema o aplicación debe tener su propia contraseña.
Secreta: sólo el usuario de la contraseña debe conocerla.

Intransferible: la contraseña no debe ser revelada a ningún tercero para su uso
Modificable: El cambio de contraseña debe ser realizado por el usuario titular. Sólo en situaciones excepcionales, podría ser cambiada por un administrador; por ejemplo cuando el usuario la hubiera olvidado o si estuviera en riesgo la seguridad de la organización.
Difícil de descifrar

CONFIGURACIÓN DE SEGURIDAD EN DISPOSITIVOS. CONTRASEÑAS ROBUSTAS

Que contengan al menos 3 de los siguientes 4 tipos de caracteres: mayúsculas, minúsculas, números y/o símbolos.
La longitud debe ser de al menos 9 caracteres.
Diferir en al menos 4 caracteres respecto de la clave anterior.

Se sugiere evitar:
2 caracteres iguales consecutivos
Palabras demasiadas simples o muy frecuentes, fracciones del nombre y/o apellido, fechas como cumpleaños o aniversario.
Reutilización de al menos las 2 últimas contraseñas que ya se hayan empleado.
Compartir o revelar las contraseñas a otras personas.
Informar las contraseñas en ninguna solicitud electrónica (cuestionario, encuesta, mail).

¿CÓMO DETECTAR UN PERFIL FALSO?

Suelen tener pocas imágenes personales.
Suelen tener pocos amigas/os y, por lo general, son del mismo sexo.
No suelen tener mucha actividad en las redes en lo que respecta a posteos, comentarios, actualización de estados.

¿QUÉ ES VIRALIZACIÓN?

La dinámica de internet y las redes sociales permite que **algunos contenidos comiencen a ser compartidos rápidamente por distintos usuarios**. A este proceso se lo llama viralización.
Un contenido puede popularizarse por ser gracioso, polémico, atractivo, de denuncia o por otras razones. En la mayoría de los casos es difícil prever su viralización y alcance, pudiendo llegar a cientos, miles o hasta millones de personas.

¿Por qué es tan importante la vinculación de esta temática con la ESI?

En Argentina, la Ley 26.150, sancionada en 2006, estableció que es un derecho recibir educación sexual, en forma integral y transversal a las diferentes áreas, desde el nivel inicial al terciario. Su

enseñanza se basa en cinco ejes: el cuidado del cuerpo y la salud, la igualdad de género, la promoción de los derechos humanos, el respeto por la diversidad y la valoración de la afectividad.
Uno de los objetivos de la ESI es la prevención de toda forma de violencia, coerción y abuso sexual.
¿Cómo? Educando en los principios de equidad de género y trabajando juntos (docentes y estudiantes) en la deconstrucción social de formas de relación y mandatos culturales que reproducen desigualdades y violencias. Las TIC se convirtieron en importantes espacios de socialización. En nuestros usos, costumbres y consumos digitales también se construyen y refuerzan identidades.

Los sesgos y mandatos sexistas están presentes tanto en las diferenciales formas de acceso y uso de los dispositivos, así como en los contenidos digitales con representaciones sociales con estereotipos de género. Por esta razón, se propone incluir la reflexión sobre la cultura digital articulada con la ESI que promueve una reflexión crítica sobre estos comportamientos y mensajes sexistas.
En clave de género, de derechos y ciudadanía, podemos preguntarnos: ¿Cuáles son los roles y modelos de género a los que las y los adolescentes tienen acceso (y a los que no) en los entornos digitales? ¿Cómo estamos reproduciendo las desigualdades en estos ámbitos digitales? ¿Qué otras representaciones podemos habilitar desde la ESI que sean más plurales, diversas y respetuosas?

II.- CIBERDELITOS

Son conductas ilegales realizadas por ciberdelincuentes que actúan en grupos o trabajan solos a través de dispositivos electrónicos y redes informáticas. Son estafas, robo de datos personales, de información comercial estratégica, robo de identidad, fraudes informáticos cometidos por ciberdelincuentes que actúan en grupos o trabajan solos

CIBERBULLYING ¿Qué es?

Es el acoso que se da repetidas y sostenidas veces (insultos, chantaje, coacción, humillación, injurias, calumnias vejaciones), se produce entre iguales, mediante el uso de las nuevas tecnologías (telefonía móvil, internet -foros, chats, correo electrónico videojuegos online). Puede ser anónimo o existir contacto o relación previa.

- PEDIR AYUDA: No aislarse. Hablar con padres o adultxs de confianza
- MANTENER NUESTRA PRIVACIDAD. NO enviar imágenes o información personal
- NO CEDER AL CHANTAJE
- GUARDAR LAS PRUEBAS: No borrar mensajes o todo aquello que pueda servir como prueba

GROOMING ¿Qué es?

Es un delito penado por la ley n° 26. 904 que incluye prisión de 6 meses a 4 años a quien por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier tecnología de transmisión de datos, contacte a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

RECOMENDACIONES PARA CASOS DE GROOMING

No borrar ningún contenido del dispositivo que se haya recibido; ya que las conversaciones, las imágenes y los videos que fueron intercambiados con el acosador serán guardadas como prueba. Fotografiar o capturar la pantalla, y almacenar esta información en algún otro dispositivo.

El ciberbullyng se puede prevenir

No denunciar al perfil acosador en las redes sociales, ya que al bloquear al usuario se puede perder información necesaria para una eventual investigación. Además, porque el abusador puede crear un nuevo perfil y continuar realizando estas acciones.

No amenazar al acosador porque puede dificultar la tarea de los investigadores.

Sobre la actitud para con los/as/es NNYA involucrados/as/es

No recriminar: hay que recordar que los/as menores son siempre víctimas y que los abusadores son especialistas en conseguir lo que buscan.

No culpabilizar: la persona adulta debe evitar fomentar la vergüenza sobre lo sucedido. El acosador utiliza la extorsión, como por ejemplo hacer público el material íntimo entregado si no cumplen con nuevos pedidos.

Dialogar: los mayores deben acompañar, contener y orientar en estas situaciones. Es necesario fomentar el diálogo para acompañar de la mejor manera en una situación que es angustiante y vergonzosa.

Denunciar: es un delito, y debe denunciarse para que se inicie una investigación sobre el caso.

EL GROOMING PUEDE DERIVAR EN OTROS GRAVES DELITOS

III.- VIOLENCIA DIGITAL CONTRA LAS MUJERES

La ciberviolencia de género es una violación a los derechos humanos con características y consecuencias reales específicas y debe entenderse como una continuidad de las formas de violencia, desigualdad y discriminación sistemática hacia las mujeres.
La violencia digital contra mujeres, adolescentes o niñas es aquella que se comete a través de dispositivos móviles, Internet, plataformas de redes sociales, correo electrónico o cualquier otro medio de transmisión de datos. La violencia digital puede afectar algunos de los derechos digitales, como la privacidad, la identidad, la libertad de expresión, la participación en la vida pública, la reputación y la dignidad, y pueden conducir a formas de violencia sexual y de violencia física. A su vez, los medios electrónicos pueden usarse como modalidad específica para cometer o agravar diferentes tipos de violencia contra las mujeres, como la psicológica y/o la simbólica

SEXTORSIÓN

Es un tipo de chantaje a través del cual se amenaza a la persona destinataria con revelar información íntima de carácter sexual, a cambio de nuevo material, dinero u algún otro requerimiento. La extorsión puede provenir de la persona con la cual se compartió el material o bien, de una tercera, producto de un acceso ilegítimo a dicha información. El delito de extorsión definido por el Código Penal establece que será reprimido el que por amenaza de imputaciones contra el honor o de violación de secretos obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos.

Descontextualización de la situación: la imagen o video consentida y apropiada en el momento de intimidad se viraliza

Exposición: las imágenes viralizadas son recibidas por personas que no son los destinatarios originales. Cuantas más personas vean la imagen o video, más expuestos estarán los protagonistas

Estafa romántica - Romance Scam: Es una forma de estafa que consiste en crear un perfil en línea –en un sitio web de citas– con el fin de fingir interés y generar una relación afectiva con otra persona, explotando los intereses que esta última ha expresado para luego engañarla y obtener dinero o información confidencial con distintos pretextos. Esta conducta encuadraría en el Art. 172 y subsiguientes del Código Penal.

SEXTING ¿Qué es?

Es una práctica sexual basada en el intercambio de imágenes, videos y/o mensajes de contenidos eróticos-pornográficos con el consentimiento de las personas participantes de la práctica. El

problema se plantea cuando una de las partes, **sin consentimiento** y a través de las TIC's distribuye este material con el claro objetivo de perjudicar a la persona propietaria de las imágenes.

¿CÓMO PROTEGER LA IMAGEN PERSONAL?

- Considerar las posibles consecuencias.
- No mostrar aquello que puede identificarte.
- Utilizar apps de mensajería que permitan eliminar la imagen/video en el tiempo que el emisor elija.
- Hay apps que permiten bloquear las capturas de pantalla o notifican si el receptor del material lo ha hecho.
- Usar apps que permitan pixelar/difuminar aquello que te haga identificable en la imagen.
- No guardar este tipo de material en los dispositivos, pero de hacerlo, utilizar algún tipo cifrado para mejorar su resguardo.
- Evitar sextear a través de redes de WiFi públicas.

La difusión de imágenes íntimas sin consentimiento es un tipo de violencia que **conlleva una violación a la privacidad y exposición de la intimidad.** Se ejerce con el fin de **humillar, amedrentar o chantajear a una persona**. Casi la totalidad de las víctimas son mujeres y en general de parte de quienes fueron sus parejas. Las consecuencias para la víctima pueden llegar a ser muy graves, llegando a afectarla emocionalmente hasta el punto de conmover fuertemente su cotidianidad y poner en riesgo su integridad física.
La situación es clara e inadmisible cuando estamos frente a personas adultas que ejercieron presión, manipulación, abuso, violencia sexual y/o grooming para producir o conseguir ese material, que puede ser considerado pornográfico. **Pero, ¿qué ocurre si el material se compartió entre pares adolescentes?**
Los abordajes de las conductas violentas entre adolescentes en la escuela no buscan un castigo, sino que **deben dar lugar a la reflexión, el diálogo colectivo, el aprendizaje y abogar por una resolución consensuada**

¿QUÉ ES EL CONSENTIMIENTO?

Es la manifestación de nuestra voluntad a realizar o participar de una actividad determinada. Son sus características:

- **ACTIVO:** Si dice "no", es "no". No decir "no", no significa dar consentimiento. Solo "sí" significa "sí".
- **ESPECÍFICO:** Aceptar tomarse una foto no significa autorizar que se archive o divulgue. **REVERSIBLE:** Se puede cambiar de opinión en cualquier momento.
- **ENTUSIASTA:** Parte del deseo de querer hacerlo.
- **UNA ELECCIÓN LIBRE:** no hay consentimiento con chantaje, presión o cualquier tipo de violencia. **EN IGUALDAD DE CONDICIONES:** No es posible en vínculos con desigualdad de

poder. Si alguien está borracho/a, dormido/a o en situación vulnerable no está en condiciones de dar su consentimiento

CIBERCONTROL Y VIOLENCIA EN NOVIAZGOS

Las primeras señales que alertan sobre la violencia en un noviazgo, como los celos excesivos, el control, las amenazas o la desvalorización, muchas veces pasan inadvertidas. Es común que entre adolescentes estas formas de violencia se ejecuten con el uso de la tecnología, que permite controlar minuto a minuto las actividades de la otra persona, sus horarios, forma de vestirse, sus vínculos afectivos, hasta su geolocalización.

En este sentido, algunas adolescentes relatan el enojo de sus parejas si no les responden a todos sus mensajes de inmediato ("*me clavaste el visto*") o cuando las ven conectadas por la noche ("*¿con kien estás a esta hora*?").

Desde la ESI, se identifican situaciones de violencia en la pareja, se favorece la reflexión sobre los estereotipos de género y promueven vínculos saludables, respetuosos y solidarios. La violencia en los vínculos de pareja se considera como una problemática social y de salud pública, no es un asunto privado.

La reflexión sobre las ideas del amor romántico, celos y control es uno de los contenidos enfocados en la prevención. Los mitos del amor romántico refuerzan y normalizan mandatos y roles estereotipados para mujeres y varones, que justifican socialmente las relaciones de poder desiguales entre los géneros: ***los celos son expresión de amor, amar es sufrir y sacrificarse por la otra persona el amor todo lo puede y lo perdona, existe una única pareja predeterminada para mí y es para siempre, el amor es heterosexual, el amor verdadero es lo que me completa como persona y da sentido a mi vida…***

¿Qué otros mandatos fortalecen los mitos del "amor romántico"? ¿Cómo construimos vínculos amorosos que sean respetuosos de las decisiones libres de cada persona?

En la Web circulan los datos personales que compartimos en: redes sociales, en los sitios que frecuentamos, en formularios digitales, en sitios de juegos y de compras, pero también circulan otros datos nuestros que muchas veces desconocemos.

IV.- PHISHING ¿Qué es?

La palabra **phishing** quiere decir suplantación de identidad.
Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esa persona.
Los ciberdelincuentes envían correos electrónicos falsos como anzuelo para "pescar" contraseñas y datos personales valiosos.

¿CÓMO PREVENIRLO?:

- **No contestar formularios en línea** enviados por destinatarios desconocidos.
- **No responder a ningún correo electrónico, teléfono o fax, que solicite divulgar información personal.**
- **No enviar ni compartir ningún código de seguridad**
- **Desconfiar de los archivos adjuntos:** pueden causar la descarga de la clave de registro o software "spyware" en su computadora.
- **Utilizar un antivirus** actualizado.
- **Actualizar el sistema operativo.**

V.- ¿DÓNDE DENUNCIAR UN DELITO INFORMÁTICO?

Centro de Ciberseguridad (BA-CSirt)

Gobierno de la Ciudad Autónoma de Buenos Aires
Teléfono: 4323-9362 de 9 a 17hs
ciberseguridad@ba-csirt.gob.ar

CONSAVIG Comisión Nacional Coordinadora de acciones para la elaboración de sanciones de la violencia de género

Corrientes 327, piso 14.
Teléfono: 5300-4000. Int. 76633

Línea 144

Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires

Observatorio de Derechos en Internet - Centro de Protección de Datos Personales
4338-4900 Int. 3754/3752
odei@defensoria.org.ar / cpdp@defensoría.org.ar

División de Delitos Cibernéticos contra la Niñez y Adolescencia

Policía Federal
4630-7237
ciberneticosnya@policiafederal.gov.ar
delitostecnologicos@policiafederal.gov.ar

Fiscalía de la Ciudad 0800 33 (FISCAL) 347225

http://www.fiscalias.gob.ar/en-linea
denuncias@fiscalias.gob.ar
Unidad Fiscal Especializada de Violencia contra las Mujeres 6089-9074 o 6089-9000. Int. 9259 ufem@mpf.gov.ar

Centro de Justicia de la Mujer

Av. Don Pedro de Mendoza 2689
Lunes a Viernes de 9 a 18
0800-999-68537

EQUIPO

Mg. Jessica Malegarie
Directora

María Cecilia Sánchez
Coordinadora

Emma Torres

Abog. María Laura Lastres

Carlos Benítez Rojas

11-6507-7447

p.aj.du (Participación Ciudadana, Acceso a Justicia y Derechos Universales)