CUIDA TU IDENTIDAD DIGITAL Y PROTEGE TUS DATOS PERSONALES:

RIESGOS SOBRE EL TRATAMIENTO DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES

DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES

Industria y Comercio
SUPERINTENDENCIA

El futuro es de todos
Gobierno de Colombia

Industria y Comercio
SUPERINTENDENCIA

CUIDA TU IDENTIDAD DIGITAL Y PROTEGE TUS DATOS PERSONALES:

RIESGOS SOBRE EL TRATAMIENTO DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES

DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES

Bogotá D.C.

2021

El futuro es de todos
Gobierno de Colombia

Industria y Comercio
SUPERINTENDENCIA

ANDRÉS BARRETO GONZÁLEZ
Superintendente de Industria y Comercio

NELSON REMOLINA ANGARITA
Superintendente Delegado para la Protección de Datos Personales

ANGÉLICA MARÍA ACUÑA PORRAS
Secretaria General

JAZMÍN ROCÍO SOACHA PEDRAZA
Jefe de Oficina Asesora Jurídica

ANGÉLICA ASPRILLA
Jefe Oficina de Servicios al Consumidor y Apoyo empresarial OSCAE

NELSON REMOLINA ANGARITA
MARÍA CAMILA NEIRA BAQUERO
CATERINE GÓMEZ CARDONA
Autores primera edición

MARCELA GONGORA
Edición

DIEGO MAURICIO ALFARO MEDINA
Diagramación

BOGOTÁ - COLOMBIA 2021

CONTENIDO

Introducción

Cada día aumenta el uso de servicios digitales, portales, redes sociales y aplicaciones tecnológicas por parte de los niños, niñas y adolescentes (en adelante NNA). Los NNA son personas altamente influenciadas por la tecnología, internet y las redes sociales.

Los menores de edad tienen acceso a internet a través de celulares, tabletas y computadores. La aparición de las redes sociales, los juegos en línea y los espacios de aprendizaje en internet, han abierto nuevos escenarios de interacción para los niños, niñas y adolescentes. Lo que estos desconocen, es que cuando se accede a páginas en internet, de forma casi automática, se recaban Datos que permiten a los portales de internet y a teceros, saber quién ha accedido; en qué ubicación se encuentra y qué tipo de información consume, entre otros.

Así las cosas, los Datos personales de niños, niñas y adolescentes son recolectados, usados y tratados por empresas, personas y entidades públicas ubicadas en difetentes partes del mundo. Adicionalmente, los menores de edad comparten su información personal ignorando los peligros a los que se exponen al suministrar sus Datos y la información de terceros (amigos, compañeros de colegio, su familia) en plataformas web de manera indiscriminada. Nombres; apellidos; fotos; videos; comentarios; la edad; los gustos o preferencias y, Datos como correo electrónico, entre otros, son compartidos por los menores de edad sin pensar que estos forman parte de su información personal y privada, que hacen parte de su identidad digital. Tampoco tienen presente que una vez difunden su información en internet perderán el control de la misma.

El artículo 44 de la Constitución Política de Colombia establece que los niños, niñas y adolescentes gozan de una especial protección por parte del Estado y que no solo son titulares de los derechos constitucionales y legales, sino que debe ser "protegidos contra toda forma de abandono, violencia física o moral, secuestro, venta, abuso sexual, explotación laboral o económica y trabajos riesgosos". Precisa dicha norma que "los derechos de los niños prevalecen sobre los derechos de los demás".

El artículo 15 superior, por su parte, señala que *"en la* **recolección, tratamiento y circulación** *de datos se respetarán la libertad y demás garantías consagradas en la Constitución"*. Esta norma fue reglamentada por la Ley Estatutaria 1581 de 2012 que define "Tratamiento" como *"Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"* [1]

El Título III de la Ley 1581 de 2012, incluye dentro de la Categoría Especial de Datos, los Datos de los niños, niñas y adolescentes, señalando: **"ARTÍCULO 7o. DERECHOS DE LOS NIÑOS, NIÑAS Y ADOLESCENTES.** En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes".

Progresivamente han venido aumentado los casos que evidencian los riesgos y peligros a los que se ven expuestos los NNA en las redes sociales digitales, se ha puesto de presente que *"Los niños, niñas y adolescentes tienen cada vez mayor acceso a los distintos sistemas de comunicación, que les permiten obtener todos los beneficios que ellos representan, pero esta situación también ha llevado al límite el balance entre el ejercicio de los derechos fundamentales y los riesgos —para la vida privada, el honor, buen nombre, y la intimidad, entre otros — que, así como los abusos de los cuales pueden ser víctimas — como discriminación, explotación sexual, pornografía, entre otros — pueden tener un impacto negativo en su desarrollo integral y vida adulta"*[2] .

Finalmente, se ha enfatizado en la necesidad de proteger *"la información personal de niñas, niños y adolescentes sin que se afecte su dignidad como personas ya que ellos tienen una expectativa razonable de privacidad al compartir su información en ambientes digitales, dado que consideran que se encuentran en un espacio privado"*[3] . Es muy importante no perder de vista lo anterior, pues, a partir de la información que existe sobre NNA en internet o redes sociales digitales se crea la identidad digital de aquellos, la cual incide en su presente y futuro como seres humanos.

La Superintendencia de Industria y Comercio, como Autoridad Nacional de Protección de Datos Personales ha venido desarrollando textos para promover el debido Tratamiento de los Datos personales de los NNA. En línea con lo anterior, ha publicado los documentos: (1) Desarrollo de contenido para los adolescentes[4] (2016) y (2) Guía para el Tratamiento de Datos personales para el sector de la educación pública y privada[5] (2015).

1 Cfr. Literal g) del artículo 3 de la Ley Estatutaria 1581 de 2012
2 Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes - Memorandum de Montevideo- (2009). En: http://www.iijusticia.org/Memo.htm#_ftnref6
3 Ibid
4 Allí se desarrollan los siguiente temas : ¿Qué son los datos personales (y ejemplos)?, Quiénes pueden conocer tus datos personales?; Clasificación de datos personales; ¿Por qué son importantes los datos personales?; ¿Qué puedes hacer para proteger tus datos personales? Y ¿Qué puedes hacer si sabes que alguien está usando tus datos personales sin autorización?

La presente guía es complementaria a las anteriores y tiene como objetivo brindar herramientas sobre protección de Datos personales, de tal modo que los NNA sepan cómo proteger su identidad digital y ante qué peligros están expuestos. Asimismo, busca crear conciencia en los menores para que entiendan las responsabilidad que tienen de cuidar y respetar tanto sus Datos personales como los de otros.

IDENTIDAD DIGITAL Y DATOS PERSONALES

Todo lo que se hace en internet deja huella y una vez se pone información en la red se pierde control sobre la misma porque puede ser recolectada y usada por terceros. Igualmente, cada vez que los NNA se registran en las redes sociales, en páginas de internet, aplicaciones o en las páginas de juegos en línea, están creando una identidad digital a partir de sus Datos personales[6]. Datos necesarios para los registros en línea tales como el nombre; el apellido; correo electrónico; fotos o el tipo de contenidos que consumen en internet construyen la identidad digital.

Es tanta y diversa la clase de datos personales que los NNA publican en las redes sociales que para algunos estamos en una época de *"striptease informativo"*[7]. Algunas personas prácticamente publican todo en internet sin saber que están condenados a ser esclavos vitalicios de la información que publiquen así traten de eliminarla de la red.

Esa información es utilizada para, entre otros, crear perfiles virtuales sobre cada persona. En este sentido en la sentencia T-414 de 16 de junio de 1992[8] , la Corte Constitucional señaló que esos "perfiles virtuales" pueden construirse a partir de los Datos de una persona y precisó lo siguiente:

> "El "perfil de datos" de la persona se constituye entonces en una especie de "persona virtual" sobre la cual pueden ejercerse muchas acciones que tendrán repercusión sobre la persona real. Desde el envío de propaganda no solicitada, hasta coerción u "ostracismo" social como en el caso que se presenta. Un "buen" manejo de Bancos de Datos permitiría identificar hasta perfiles poblacionales desde distintos puntos de vista, lo cual constituye un evidente peligro de control social de aquellos que ostentan "poder informático", no solamente contra la libertad de las personas individuales sino contra la de sectores sociales más amplios.

Cualquier publicación en internet viaja rápidamente y puede dejar una huella permanente. Es por esta razón que se debe ser cuidadoso con el tipo de información que se comparte en internet, pues los Datos de cada persona tienen valor y pertenencen únicamente a los Titulares de la información.

Esa identidad digital que se construye ahora puede afectar toda la vida del NNA. Por ejemplo, las fotos que publican en internet podrían ser tenidas en cuenta por terceros cuando hagan parte de un proceso de selección laboral.

5 Esa guia tiene como objetivo orientar a las instituciones educativas y a los padres y representantes legales de los niños, niñas y adolescentes acerca del derecho constitucional que tienen todas las personas a conocer, actualizar y rectifcar su información personal, especialmente en el marco de las actividades del sector educativo, tanto público como privado, y el adecuado tratamiento de los mismos, de acuerdo con la normatividad vigente, particularmente el artículo 15 de la Constitución Política y la Ley Estatutaria 1581 de 2015. En la misma se analiza el tema de los los procesos de inscripción y matrículas, el aanejo de expediente académico y las ayudas financieras y becas.

6 Sanz, J., 2020. Sé Legal En Internet. Agencia Española para la Protección de Datos.

7 Cfr. Remolina Angarita, Nelson. Striptease informativo, redes sociales, ley de protección de datos personales y ética empresarial. Columna de opinión publicada en el periodico Ambito Jurídico de Legis. Bogotá, noviembre 15-28 de 2010, pág. 12. Disponible en: http://habeasdatacolombia.uniandes.edu.co/?p=149

8 Corte Constitucional, sentencia T-414 del 16 de junio de 1992. MP. Ciro Angarita Barón. El texto oficial puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

ALGUNOS RIESGOS O PELIGROS

Progresivamente han venido aumentado los casos que evidencian los riesgos y peligros a que se ven expuestos las NNA que interactúan en las redes sociales digitales y otros canales digitales. Esas redes y tecnologías, por sí solas no son el problema, pero infortunadamente, algunas personas han encontrado en las mismas un escenario perfecto para realizar conductas indebidas. El acoso sexual "grooming", el acoso online "ciberbullying", los chantajes, la pornografía, las amenazas e invasiones de su privacidad están al orden del día.

Esta cuestión es muy grave si se tiene en cuenta que millones de NNA pasan varias horas del día conectados a internet, intercambiando opiniones, documentos, imágenes, etc a través de las redes sociales digitales y otras herramientas de comunicación. Muchas de ellas y ellos suben a la red contenidos – fotos, videos, etc- sobre ellos, su familia, sus amigos o terceros. Algunos de éstos, los puede condenar en el futuro -por tratarse de fotos o videos en situaciones comprometedoras- o por lo menos convertirse en un germen de burlas, discriminaciones, entre otras. No es gratuito que se haya afirmado que los NNA de hoy gastarán mucho tiempo y dinero en el futuro tratando de borrar su información del pasado[9] .

A continuación, se explican los principales peligros a los cuales están expuestos los NNA en las redes. Dichos riesgos deben ser conocidos por los menores para que estos sean conscientes de los riesgos que pueden encontrar al ingresar a aplicaciones, redes sociales, páginas web o páginas de juegos en línea.

• Ciberbullying o Troleo

El ciberbullying es el uso de las redes sociales o plataformas digitales para humillar, difamar o acosar a una persona. Es una manera de maltrato que puede ocasionar daños físicos y psicológicos[10]. El troleo, por su parte, es la provocación a otros mediante insultos u obscenidades.

En la regulación colombiana, la Ley 1620 de 2013 *"por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar" define* **Acoso escolar o bullying** *como la "conducta negativa, intencional metódica y sistemática de agresión, intimidación, humillación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza o incitación a la violencia o cualquier forma de maltrato psicológico, verbal, físico o por medios electrónicos contra un niño, niña, o adolescente, por parte de un estudiante o*

9 Cfr. REMOLINA ANGARITA, Nelson. 2013. Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012. 1 ed. Bogotá: Legis Editores. Pág 172

10 Sanz, J., 2020. Sé Legal En Internet. Agencia Española para la Protección de Datos.

varios de sus pares con quienes mantiene una relación de poder asimétrica, que se presenta de forma reiterada o a lo largo de un tiempo determinado."[11] . Igualmente, se establece que **Ciberbullying o ciberacoso escolar** es una *"forma de intimidación con uso deliberado de tecnologías de información (internet, redes sociales virtuales, telefonía móvil y videojuegos online) para ejercer maltrato psicológico y continuado."*[12]

El Ciberbullying causa daño a otras personas. Los NNA pueden ser víctimas o autores de esta conducta. Por eso, es importante que comprendan que el acoso, la discriminación, la violencia y el odio son conductas que maltratan a los seres humanos y atentan contra su dignidad humana. También es fundamental que los NNA protejan sus derechos y respeten los derechos de los demás tanto en sus actividades virtuales como reales o presenciales.
En este sentido, es pertinente que los NNA no sólo conozcan sus derechos y exijan la protección de los mismos sino que como ciudadanos también tengan presente que deben cumplir algunos deberes. En línea con lo anterior,el artículo 95 de la Constitución establece, entre otras, lo siguiente:

> *"La calidad de colombiano enaltece a todos los miembros de la comunidad nacional. Todos están en el deber de engrandecerla y dignificarla.* **El ejercicio de los derechos y libertades reconocidos en esta Constitución implica responsabilidades.**
>
> *Toda persona está obligada a cumplir la Constitución y las leyes.*
>
> *Son deberes de la persona y del ciudadano:*
>
> *1.* **Respetar los derechos ajenos y no abusar de los propios;**
>
> *2.* **Obrar conforme al principio de solidaridad social,** *respondiendo con acciones humanitarias ante situaciones que pongan en peligro la vida o la salud de las personas;*
>
> *3. Respetar y apoyar a las autoridades democráticas legítimamente constituidas para mantener la independencia y la integridad nacionales.*
>
> *4.* **Defender y difundir los derechos humanos como fundamento de la convivencia pacífica;**
>
> *5. Participar en la vida política, cívica y comunitaria del país;*
>
> *6. Propender al logro y mantenimiento de la paz;*
>
> *7. Colaborar para el buen funcionamiento de la administración de la justicia;*
> *8. Proteger los recursos culturales y naturales del país y velar por la conservación de un ambiente sano;*
>
> *9. Contribuir al financiamiento de los gastos e inversiones del Estado dentro de conceptos de justicia y equidad."* (Destacamos)

Tambien es relevante que los NNA tengan presente que el Ciberbullying se puede generar de manera directa o indirecta. La primera es cuando una persona realiza alguna de las conductas señaladas dentro del concepto del citado artículo 2 de la Ley 1620 de 2003. La indirecta tiene lugar cuando, por ejemplo, se comparten imágenes, comentarios, o dando "me gusta" a ciertos contenidos publicados por terceros. En efecto, se puede contribuir a generar Ciberbullying al distribuir mensajes o imágenes que generen cualquiera de estos efectos: agresión, intimidación, humillación, ridiculización, difamación, coacción, amenaza o incitación a la violencia o cualquier forma de maltrato psicológico, verbal, físico o por medios electrónicos contra otra persona.

11 Cfr. Artículo 2 de la Ley 1620 de 2013"
12 Ibid

Dado lo anterior es importante que los NNA no compartan o den click automático a todo. Es prudente que lean, verifiquen, analicen antes de compartir en redes o dar un click a publicaciones de terceros. Adicionalmente, al observar comportamientos de este tipo, los menores de edad pueden hacer uso de los canales de denuncia de las plataformas para que estas procedan a retirar los contenidos.

Si los NNA son víctimas de ciberbullying deben buscar ayuda de una persona adulta en la que confíen, preferiblemente los padres, tutores legales o profesores, para que les orienten y trabajen sobre el tema. Es importante que los adultos creen espacios seguros para que los menores sientan la confianza de acudir a ellos cuando tengan problemas en redes sociales o páginas de internet. En efecto, los menores de edad deben contar con espacios para reflexionar y hacer ejercicios en el aula de clase con el fin de dimensionar los daños que lo anterior puede causar, y las personas a las que se puede acudir si se es víctima de ciber-bullying o conoce de un evento relacionado. Los padres y educadores deben estar atentos para detectar cambios en el comportamiento que puedan ser producto de este tipo de acoso. Cambios en el estado de ánimo, el rendimiento académico y las conductas de los niños, pueden ser indicadores del ciberbullying.

• Ciberbaiting

El ciberbaiting es el acoso por parte de los menores de edad a un profesor. Esta es una conducta que aparece cuando alguno o algunos de los alumnos acosan a un profesor publicando su información en redes sociales, como por ejemplo fotos o videos del profesor que afectan su honra; imagen; buen nombre; privacidad, entre otros[13].

Como ya se mencionó, toda persona tiene derecho a su buen nombre, intimidad y honra. Por lo que, causar daños de este tipo a cualquier persona constituye una violación a sus derechos. Los menores de edad pueden pensar que se trata de un chiste y no comprender las consecuencias que este tipo de actuaciones tiene, tanto para la persona como en el plano legal. Es importante que se abra el diálogo en torno a estos comporta-mientos en línea, ya que es crucial que los NNA comprendan que es una falta contra los derechos de los educadores.

Como ya se mencionó, toda persona tiene derecho a su buen nombre, intimidad y honra. Por lo que, causar daños de este tipo a cualquier persona constituye una violación a sus derechos. Los menores de edad pueden pensar que se trata de un chiste y no comprender las consecuencias que este tipo de actuaciones tiene, tanto para la persona como en el plano legal. Es importante que se abra el diálogo en torno a estos comportamientos en línea, ya que es crucial que los NNA comprendan que es una falta contra los derechos de los educadores.

13 Sanz, J., 2020. Sé Legal En Internet. Agencia Española para la Protección de Datos.

• Grooming

El grooming es uno de los principales peligros a los que se exponen los NNA en internet, este ocurre principalmente en las redes sociales. Se refiere a todas las acciones que realiza un adulto para ganar la confianza de un NNA para acosarlo o abusar sexualmente de este[14]. Los adultos crean perfiles falsos y ganan la confianza de los menores de edad a través de mensajes. Los adultos se hacen pasar por otros niños, niñas o jóvenes y engañan a los menores de edad. También se da a través de los juegos en línea. Muchas páginas de juegos en internet requieren que los NNA creen un perfil. Los adultos se inscriben en estos juegos para interactuar con los menores de edad y engañarles.

En plataformas digitales es muy fácil crear perfiles o identidades falsas para engañar y acceder a la información de los menores. Los adultos utilizan seudónimos para no ser reconocidos o pueden utilizar la información de otras personas para que los menores no los identifiquen como desconocidos. Es por esto que, se debe enseñar a los menores de edad a que no deben hablar con personas que no conocen a pesar de tener la foto de un joven o un niño o niña en su perfil, pues, realmente no se puede tener certeza de quién es de la persona con la que están interactuando. Los adultos utilizan estas técnicas para pedir videos o fotografías a los niños. Igualmente puede haber acercamientos de tipo físico posteriormente.

Los NNA confían más en los amigos que conocen en línea porque desconocen los riesgos de hablar con desconocidos en internet. Además, al entregar Datos a extraños, pueden ser víctimas de chantaje. Si el menor de edad es víctima de chantaje por compartir sus fotos o se siente inseguro hablando con un desconocido, tiene que saber que los mensajes de extraños deben ser informados a los padres, tutores o adultos de confianza. Igualmente, se debe informar a los NNA que los servicios de mensajería y las redes sociales permiten bloquear y reportar a las cuentas desconocidas. En todo caso, existen canales de denuncia creados por la Policía Nacional de Colombia para denunciar chantajes y extorsiones a menores de edad.

• Sexting

El sexting es el envío de fotografías o videos íntimos que hace una persona de sí misma con contenido sexual. Es una práctica común entre los adultos, pero realizada por muchos adolescentes[15]. Se considera una práctica riesgosa, ya que la mayoría de las veces quien manda un contenido de este tipo confía que la persona que lo reciba no lo compartirá con nadie más.

14 Ibidem
15 Sanz, J., 2020. Sé Legal En Internet. Agencia Española para la Protección de Datos.

Sin embargo, en ocasiones lo que sucede es que el contenido termina en manos de un tercero o en publicaciones en línea. Estos contenidos se pueden utilizar para extorsionar o chantajear a las personas y sacar un beneficio propio, esto se conoce como sextorsión. Los menores pueden conocer personas a través de internet que pueden pedir fotografías y videos con contenidos sexuales para luego atentar contra su dignidad y su honra. Estas publicaciones pueden terminar en páginas en internet de contenido sexual, lo cual constituye un delito ya que esto se consideraría pornografía intantil.

Si los NNA están siendo chantajeados por alguien deben buscar ayuda para detener estos comportamientos. Lo ideal es no compartir contenido de este tipo con nadie y enseñar a los NNA que no se deben enviar videos o fotografías de contenido sexual, ni a parejas ni amigos porque estos pueden hacer un uso inadecuado, vulnerando su dignidad. Si alguien recibe este tipo de contenidos debe saber que al compartirlos con terceros o en las redes sociales vulnera los derechos de los demás.

• Suplantación de Identidad

Suplantar significa, entre otras, *"ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba"*[16] ; *"sustituir ilegalmente a una persona u ocupar su lugar para obtener algún beneficio"*[17] ; La suplantación de identidad consiste en hacerse pasar por otra persona para diversos propósitos: engañar a terceros, obtener bienes y servicios con cargo a la persona suplantada, incurrir en fraudes y otro de conductas ilícitas.

Mediante la suplantación de identidad los impostores engañan a terceros, obtienen créditos, adquieren productos o servicios en nombre de la persona suplantada y ésta última es la afectada porque, en muchos casos, le toca asumir el pago de dichas obligaciones.

La suplantación, se puede dar entre pares o por parte de un adulto a un menor de edad. Es probable que, tratándose de menores de edad, el hurto de identidad se dé en las redes sociales. Los NNA pueden hacerse pasar por sus amigos y compañeros creando perfiles con sus nombres y fotos a modo de broma o a modo de bullying o troleo. En este sentido, es preciso recalcar que los Datos no se deben usar en nombre de nadie y sin su Autorización o consentimiento.

Por otro lado, se puede dar la suplantación cuando un adulto hurta la identidad de un menor de edad y se hace pasar por este para obtener información personal de él o con a el fin de acosar a otros NNA. Cuando el menor de edad le entrega sus Datos a desconocidos en internet, o no es cauteloso con el manejo de su información, queda expuesto a que la persona que la adquiera, le suplante y la usepe con fines ilícitos como el acoso, chantaje o extorsión.

Es más común que la suplantación se dé entre adultos, pero, es igualmente importante que los NNA comprendan que entregando sus Datos a extraños abren la puerta a que se utilice su información de manera indiscriminada e inadecuada, lo cual pone en grave riesgo su privacidad y la de sus familiares.

16 Cfr. Diccionario de la lengua española. Actualización 2017. http://dle.rae.es/?id=YlZNKd0
17 Cfr. WordReference.com: http://www.wordreference.com/definicion/suplantar

BLOQUEO Y REPORTE DE CONTENIDOS.

Los NNA tiene la opción en las redes sociales y las plataformas digitales de bloquear y reportar contenidos, cuentas o usuarios que amenacen su seguridad. Existen muchas maneras de bloquear contenidos inadecuados. Los principales prestadores de servicios de internet cuentan con herramientas de apoyo como el control parental, el cual puede ser activado por los técnicos que trabajan en dichas compañías, o incluso por el mismo usuario del servicio.

De igual forma, las redes sociales brindan la posibilidad de bloquear usuarios y contenidos, estas permiten denunciar y reportar cualquier tipo de acoso. A través de los links de ayuda de las redes en cuestión se puede obtener toda la información de bloqueo y denuncia.

Para otras redes sociales o páginas de internet, bastará con poner en el buscador el nombre de la página o red social en la cual se desea hacer un bloqueo, reportar o denunciar contenidos inadecuados o que perjudican a los menores de edad, para que aparezcan los pasos a seguir o los canales para bloquear personas o contenidos inadecuados para los menores de edad.

LA SEGURIDAD ES CLAVE

La creación de contraseñas seguras es una de las principales recomendaciones de seguridad para proteger los Datos de NNA. Es importante enseñarles que una contraseña segura es una herramienta de protección de sus Datos en línea. Dichas contraseñas no deben contener sus nombres, apellidos o nombres de familiares ya que estos son fáciles de adivinar. Se recomienda que las contraseñas contenga letras mayúsculas y minúsculas, números y caracteres especiales como por ejemplo: @, # o $.

Además, es importante que los menores no compartan sus contraseñas con nadie diferente a sus padres. Muchas veces los NNA comparten sus contraseñas con amigos(as), novios(as) o personas que consideran de confianza y esto puede poner en riesgo su información y su privacidad ya que otras personas pueden hacer uso de sus perfiles de maneras que los pueden afectar tanto física como sicológicamente.

De igual manera, cambiar las contraseñas frecuentemente es una manera de prevenir que las cuentas sean hackeadas. Adicionalmente, se recomienda tener contraseñas diferentes para cada una de las cuentas que se tengan a fin de evitar que fácilmente un tercero pueda acceder a ellas. Tampoco es prudente compartir la ubicación al subir fotos o videos a redes sociales. Se sugiere desactivar la geolocalización de aplicaciones.

Igualmente, se les debe aclarar a los NNA que nadie los puede obligar a realizar retos en línea, ni a compartir sus fotos, videos o información. Es clave leer las políticas de privacidad y seguridad de las aplicaciones que usan los NNA y utilizar únicamente aplicaciones aptas para su rango de edad.

Importante:

• Educar a los NNA para que activen todas las configuraciones de privacidad en sus redes sociales, perfiles en línea y plataformas web.

• Enseñar a los menores de edad que no deben aceptar invitaciones físicas ni virtuales a personas que no conocen.

• Explicar por qué no deben intercambiar mensaje ni información personal en internet, especialmente con desconocidos.

• Inculcar en los NNA que deben informar a los padres, tutores, profesores o un adulto de confianza si reciben mensajes extraños o si se sienten en peligro.

• Evitar que los NNA faciliten su información por medio de las redes sociales, publiquen información como su ubicación; número de teléfono; correo electrónico; la dirección de su vivienda; entre otros.

• Conocer que es posible bloquear o denunciar comentarios y notificaciones indeseadas así como perfiles de desconocidos.

• Recomendar a los NNA que al jugar en línea, no se deben proporcionar Datos como nombre, apellido, ubicación o edad. Asimismo que deben mantener la cámara apagada.

• Permitir descargas de aplicaciones de sitios oficiales únicamente.

• Navegar en páginas web que implementen medidas de seguridad pertinentes para evitar el robo de Datos.

• Informarse en sitios oficiales. En internet se publican muchas noticas falsas e información que no es cierta.

¿DE QUÉ MANERA LA SIC PUEDE AYUDAR A NIÑOS, NIÑAS Y ADOLESCENTES RESPECTO DE SUS DATOS PERSONALES?

La Organización para la Cooperación y el Desarrollo Económico (OCDE) estableció los *"principios para un entorno digital seguro y beneficioso para los niños"*[18] en donde pone de presente que , entre otras, las organizaciones públicas y privadas que desempeñan un papel activo en el establecimiento de políticas y prácticas o en la prestación de servicios para los niños en el entorno digital, deben:

a) Defender el interés superior del niño como consideración primordial; e
b) identificar cómo se pueden proteger y respetar los derechos de los niños en el entorno digital y tomar las medidas adecuadas para hacerlo.

Adicionalmente, señala la OCDE que se deben tomar medidas para ayudar a los niños a darse cuenta de los beneficios y disfrutar de aquellos en el entorno digital al:

• Apoyar a los padres, tutores y cuidadores en su papel fundamental de evaluar y minimizar los riesgos a daños y optimizar los beneficios para sus hijos tanto en línea como fuera de línea;

• Asegurar que los niños y sus padres, tutores y cuidadores sean conscientes de sus derechos en el entorno digital y establecer mecanismos accesibles para hacer cumplir dichos derechos, incluidos los mecanismos de denuncia u otros recursos legales;

• Apoyar a los niños y a sus padres, tutores y cuidadores para que comprendan:

-los derechos de los niños como Titulares de información; y

18 Cfr. OECD (2021). Recommendation of the Council on Children in the Digital Environment. En: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-038919 Cfr. Artículo

- la forma en que se recopilan, tratan, comparten y utilizan los Datos personales de los niños;

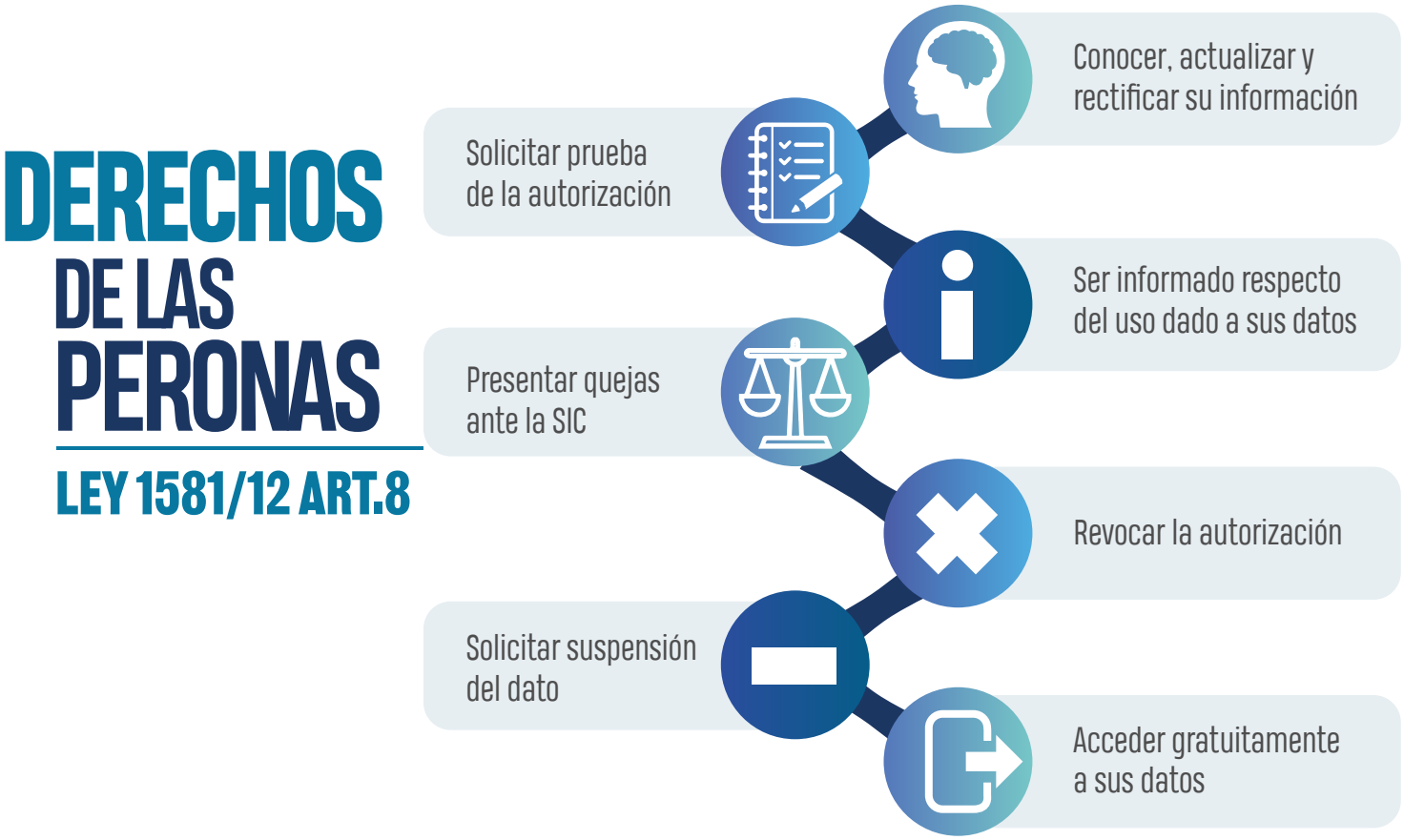
• Defender y respetar el derecho de los niños a expresar libremente sus opiniones y su capacidad, según corresponda teniendo en cuenta su edad y madurez, para participar en los asuntos que les afecten en el entorno digital;

• Dar a conocer a los niños, así como a sus padres, tutores y cuidadores, los servicios legales, psicosociales o terapéuticos disponibles para los niños que requieran asistencia como resultado de actividades o acciones en el entorno digital, y facilitar el acceso a estos y,

• Desarrollar mecanismos para generar consciencia a los niños, padres, tutores y cuidadores de las prácticas comerciales en línea que puedan causar daños a los niños.

En línea con lo anterior, y dentro del marco de sus competencias legales como autoridad de protección de datos, la Superintendencia de Industria y Comercio (SIC) está facultada para ejercer *"la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley"* [19]

Cabe recordar que los NNA son titulares de los siguientes derechos consagrados en el artículo 8 de la Ley Estatuaria 1581 de 2012:



19 de la Ley Estatutaria 1581 de 2012

En el desarrollo, interpretación y aplicación de la presente ley se aplicarán, de manera armónica e integral , los siguietes principios:

Los NNA o su representante legal pueden interponer una queja ante la SIC si los datos personales de un NNA son recolectados ilícitamente (sin autorización), usados para fines no autorizados o permitidos por la ley, enviados o circulados a terceros ilegítimamente o si, en general, se realiza cualquier actividad con datos personales al margen de la ley.

La SIC ha creado varias herramientas o canales para garantizar estos derechos, a saber:

A. Servicios y canales de asesoría de la SIC

La orientación sobre el procedimiento para realizar un queja realacionada con datos personales, se realiza a través de los canales de atención presencial, telefónico o virtual disponibles en el enlace de trámites y servicios de la página web. La atención a las consultas se brinda de manera gratuita.

La SIC cuenta con varios servicios de atención ciudada, a saber:

- Redes sociales

A través del dinámico canal de atención virtual de las redes sociales Twitter y Facebook, la SIC orienta a los ciudadanos acerca de los diferentes trámites que se pueden adelantar en la entidad, y atiende las consultas e inquietudes mediante las cuentas @sicresponde y @sicsuper.

- Vídeo llamada

La SIC cuenta con un práctico canal de atención en línea donde los ciudadanos tienen la oportunidad de hacer consultas sobre los trámites y servicios que se adelantan en la SIC, en tiempo real, ingresando a la sala de chat a través de la página web www.sic.gov.co, donde se encuentra el botón de enlace en vivo y en directo con uno

de los asesores de servicio. Allí se encuentra la información especializada: **Para trámites e información general**

• **Chat de asesoría en línea**

Se puede entrar al chat en el siguiente link: **https://www.sic.gov.co/asesoria-en-linea**

• **Atención telefónica.**

Los siguientes son los números de contacto:

- Teléfono Conmutador: +57 (1) 587 00 00 - Bogotá - Línea Gratuita Nacional: 01 8000 910165
- Contact center +57 (1) 592 0400

B. Para presentar una queja por indebido tratamiento de datos personales

Antes de presentar una queja ante la SIC hay que radicar una consulta o reclamo ante la empresa o entidad que presuntamente está vulnerando los derechos. Hay que tener presente que la Ley 1581 de 2012 consagra los procesos de consultas y reclamos para que los NNA ejerzan sus derechos. El trámite previo de consultas o reclamos es un requisito legal de procedibilidad para presentar quejas ante la SIC.

• Consultas

Mediante este proceso se busca materializar el derecho de conocer por parte del NNA la información que sobre él/ella tiene una empresa o entidad pública. La respuesta a la consulta deberá comunicarse al solicitante en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al NNA expresando los motivos de la demora y señalando la fecha en que se atenderá la consulta, que en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

• Reclamos

Los reclamos tienen por objeto corregir, actualizar, o suprimir datos o elevar una queja por el presunto incumplimiento de cualquiera de los deberes contenidos en la ley 1581 de 2012.

El reclamo debe presentarse mediante solicitud dirigida al Responsable o Encargado del tratamiento que contenga la siguiente información: a) Nombre e identificación de la persona que presenta el reclamo; b) Descripción precisa y completa de los hechos que dan lugar al reclamo; c) Dirección física o electrónica para remitir la respuesta e informar sobre el estado del trámite y, d) Documentos y demás pruebas pertinentes que se quieran hacer valer.

El término máximo para atender el reclamo es de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se debe informar al NNA los motivos de la demora y la fecha en que se dará respuesta al reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Una vez presentada la consulta o el reclamo y si no es respondida o el NNA considera que la respuesta recibida no es correcta, podrá presentar queja ante la SIC.

Para el efecto, se puede acudir a las siguientes alternativas:

a) Utilizar la App QRFS de la Superintendencia de Industria y Comercio

Esta App fue diseñada para que se puedan presentar las quejas ante la SIC. Se descárga y se usa.

b) Presentar la queja a través de la página web de la SIC en donde se encuentra un formulario electrónico en : https://servicioslinea.sic.gov.co/servilinea/P-QRSF2/ . En el asunto del formulario escribir: "Violación de datos personales de menor de edad"

c) Enviar un correo electrónico a:
Señores
Superintendencia de Industria y Comercio
Delegatura para la Protección de Datos Personales
habeasdata@sic.gov.co,

(En el asunto del correo indicar el siguiente: "Violación de datos personales de menor de edad")
Allí se menciona brevemente lo siguiente:

- Nombre o el del representante legal (papá,mamá).
- Dirección electrónica de contacto.
- Nombre y datos de contacto de la empresa o entidad que no han tratado correctamente los datos personales.
- Descripción de los hechos que dan lugar a la queja.
- Pruebas que se tengan y se quieran hacer valer.

C. Solicitar el bloqueo temporal de datos

El bloqueo es una medida excepcional y temporal mientras se adopta una decisión definitiva sobre la queja que se presente ante esta superintendencia. Bloquear datos personales significa adoptar medidas para impedir o limitar el tratamiento[20] de los mismos. El bloqueo tiene como finalidad obstruir o dificultar el acceso, el uso, la circulación y cualquier otra actividad sobre datos personales.

La medida de bloqueo procede únicamente si se cumplen y prueban los supuestos que establece el literal c) del artículo 21 de la Ley Estatutaria 1581 de 2021. Dentro de esos requisitos se encuentran: (i) la existencia de una solicitud por parte del Titular del dato; (ii) que se identifique un riesgo cierto de vulneración de los derechos fundamentales, y (iii) que dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.

Es importante resaltar que la violación de derechos fundamentales de los que trata la norma antes citada no solo comprende el derecho a la protección de datos personales, sino cualquier otro derecho fundamental que pueda resultar afectado, como el derecho a la vida, la intimidad y al buen nombre, entre otros.

Para facilitar el uso de este mecanismo, se puede utilizar el siguiente modelo de solicitud de bloqueo temporal:

20 El término Tratamiento se refiere a "cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión" (Literal g del artículo 3 de la ley 1581 de 2012.

Señores
Superintendencia de Industria y Comercio
Delegatura para la Protección de Datos Personales
habeasdata@sic.gov.co,
contactenos@sic.gov.co,

Ref. Solicitud de bloqueo temporal

Respetados señores:

De conformidad con el literal c) del artículo 21 de la Ley Estatutaria 1581 de 2012 y el numeral 4 del artículo 16 del Decreto 4886 de 2011, solicito que se ordene el bloqueo temporal teniendo en cuenta lo siguiente:

I. INFORMACIÓN DE IDENTIFICACIÓN Y DE CONTACTO DE LA PERSONA NATURAL QUE SOLICITA EL BLOQUEO TEMPORAL:

- Nombre del titular del dato personal:
- Número de identificación:
- Dirección de correo electrónico para notificaciones:
- Dirección postal para notificaciones:
- Ciudad:
- País:

II. INFORMACIÓN DE CONTACTO E IDENTIFICACIÓN DE LA EMPRESA, PERSONA O ENTIDAD QUE PRESUNTAMENTE HA INCURRIDO EN UN ACTO ILEGAL RESPECTO DE DATOS PERSONALES Y QUE HA GENERADO UN RIESGO CIERTO DE VULNERACIÓN DE DERECHOS FUNDAMENTALES:

- Nombre de la entidad que está poniendo en riesgo mis derechos:
- Número de identificación:
- Dirección de correo electrónico para notificaciones:
- Dirección postal para notificaciones:
- Ciudad:
- País:
- Sitio web:
- Otros datos contacto:

III. INFORMACIÓN PRECISA Y COMPLETA DE LA BASE DE DATOS O PÁGINA WEB RESPECTO DE LA CUAL SE SOLICITA EL BLOQUEO TEMPORAL:

Esto es, el sitio exacto en donde se encuentra ubicada o publicada la base de datos que solicito bloquear temporalmente:

IV. HECHOS RELEVANTES Y DATOS PERSONALES TRATADOS INDEBIDAMENTE

Mi petición de bloqueo se fundamenta en los siguientes hechos: (Enuncie los hechos relevantes y mencione los datos personales que se están recolectando o usando de manera ilegal -fotos, videos, datos de contacto, etc.)

V. EXISTENCIA DE RIESGO CIERTO DE VULNERACIÓN DE MIS DERECHOS FUNDAMENTALES Y NECESIDAD DE EMITIR ORDEN DE BLOQUEO PARA PROTEGERLOS.

Pongo de presente que existe una amenaza real de que se viole, infrinja, quebrante o lesione mis derechos fundamentales por lo siguiente: (Explicar por qué razón considera que se pueden afectar de manera inminente sus derechos fundamentales -vida, intimidad, buen nombre, etc- y por qué es necesario que se emita la orden de bloqueo)

VI. PRUEBAS

Anexo las siguientes pruebas:

Cordialmente,

Nombre completo y firma del solicitante
Identificación

REFLEXIONES FINALES

Sin perjuicio de todo lo anterior, queremos reiterar o dejar planteado lo siguiente:

La realidad socio tecnológica del siglo XXI genera oportunidades y retos a los NNA, quienes cada día conviven en escenarios "virtuales". Las redes sociales digitales (RSD) , por ejemplo, son una realidad cotidiana para analizar en la cual crece significativamente el número de usuarios, muchos de los cuales son NNA. ¿Saben los padres que imágenes y contenidos publican diariamente sus hijos en las RSD?. ¿Conocen qué tipos de contenidos ven o leen sus hijos diariamente a través de las RSD?, ¿Tienen idea del perfil de las personas con quienes ellos se contactan diariamente a través de las RSD?; ¿En los colegios están educando y formando adecuadamente a los NNA para convivir de manera civilizada y segura en las RSD?, ¿En casa hemos conversado con nuestros NNA sobre estos temas?; ¿Las madres y padres de familia tienen claro los riesgos a que se exponen sus hijos por interactuar en una RSD?, ¿Sabemos cómo guiar a nuestros NNA para que su convivencia virtual en las RSD sea sana y segura?.

Esta realidad incide en el presente y futuro de los NNA. Abordar debidamente esta situación no es tarea de poca monta. Buena parte de la protección de nuestros derechos depende de la educación que recibamos. La formación académica, humana, social y ética que se imparte en las escuelas y en casa es muy importante . Es fundamental enfocar esfuerzos que los NNA ellos no sólo sean respetuosos de los derechos de los demás sino que se conviertan en sujetos activos y principales guardianes de ssus datos personales.

El artículo 7 de la Ley Estatutaria 1581 de 2012 ordena educar los NNA para que vivan adecuadamente bajo el contexto de la sociedad de la información. En ese sentido, es crucial que los NNA conozcan los *"eventuales riesgos a los que se enfrentan (…) respecto del Tratamiento indebido de sus datos personales" y sean capaces de realizar un "uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás"*

Este es un reto de todos. Si los NNA no son conscientes del tema e ignoran los riesgos negativos sobre el tratamiento indebido de sus datos pues continuarán siendo víctimas de, entre otras, los delincuentes, los abusos, etc. La familia, el Estado y los establecimientos educativos deben contribuir a formar ciudadanos para una sociedad llena de tecnología y de información.

Internet ha creado nuevos espacios que permiten la interacción, el aprendizaje, la cultura y muchas otras cosas. Sin embargo, es importante construir una ciudadanía digital que permita una mejor convivencia en estos espacios.

Es clave que los menores de edad protejan sus Datos personales toda vez que estos hacen parte de su identidad y un uso inadecuado puede causar daños en la intimidad, honra y buen nombre, no solo de ellos mismo sino de otras personas. El menor de edad debe reflexionar sobre su seguridad y comprender que es el encargado de proteger su identidad digital y de preservar el buen nombre de los otros en línea.

En internet se puede proteger a los menores si se toman las precauciones necesarias y las medidas preventivas como la educación en temas de riesgo y seguridad para los NNA. Los educadores y padres de familia cumplen un rol crucial en la educación de los menores y en su acompañamiento en redes. Es importante crear espacios de diálogo y reflexión para que los NNA comprendan lo importantes y valiosos que son sus Datos, que estos les pertenecen y que deben ser cuidadosos con la información que suministran y a quién se la entregan.

CUIDA TU IDENTIDAD DIGITAL

GLOSARIO

• **Autorización:** consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

• **Acoso escolar o bullying:** "Conducta negativa, intencional metódica y sistemática de agresión, intimidación, humillación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza o incitación a la violencia o cualquier forma de maltrato psicológico, verbal, físico o por medios electrónicos contra un niño, niña, o adolescente, por parte de un estudiante o varios de sus pares con quienes mantiene una relación de poder asimétrica, que se presenta de forma reiterada o a lo largo de un tiempo determinado."

• **Ciberbullying o ciberacoso escolar:** "Forma de intimidación con uso deliberado de tecnologías de información (internet, redes sociales virtuales, telefonía móvil y videojuegos online) para ejercer maltrato psicológico y continuado."

• **Consentimiento:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que una persona autoriza el tratamiento de sus datos personales.

• **Dato personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

• **Huella digital:** son los registros que dejan todas las actuaciones de los usuarios en internet. Comentarios, registros de información, fotos, gustos, preferencias y demás interacciones construyen la huella digital.

• **Titular:** persona natural cuyos datos personales sean objeto de tratamiento.

• **Tratamiento de Datos:** es cualquier operación o conjunto de operaciones sobre los datos personales, tales como la recolección, almacenamiento, uso, circulación y suspensión.

---

21 Tomado de la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
22 Cfr. Artículo 2 de la Ley 1620 de 2013 "por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar"
23 Cfr. Artículo 2 de la Ley 1620 de 2013 "por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar"
24 Tomado de Glosario Página web Sé Legal en Internet. Disponible en: https://www.tudecideseninternet.es/aepd/para-saber-mas/glosario.html
25 Tomado de la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
26 Tomado de Internet Society. Disponible en: https://www.internetsociety.org/es/tutorials/digital-footprint-matters/module-1-digital-footprint
27 Tomado de la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
28 Ibidem

REFERENCIAS

- Convención sobre los *derechos del Niño*, 1989, Serie de Tratados de las Naciones Unidas, disponible en: **https://www.unicef.es/sites/unicef.es/files/comunicacion/ConvencionsobrelosDerechosdelNino.pdf**

- Constitución política de Colombia (1991).
- González Fuster, G. and Kloza, D., 2016. *The European Handbook For Teaching Privacy And Data Protection At Schools.* [online] Arcades-project.eu. Disponible en: **http://arcades-project.eu/images/pdf/arcades_teaching_handbook_final_EN.pdf**
- Gregorio, C. and Ornelas, L., 2011. Protección De Datos Personales En Las Redes Sociales Digitales: **En Particular De Niños Y Adolescentes.** Memorándum De Montevideo. México, D.F.: Instituto de Investigación para la Justicia.

- OECD, 2021. *Recommendation of the Council on Children in the Digital Environment.* [online]. OECD. Disponible en: **https://www.oecd.org/digital/ieconomy/protecting-children-online.htm**
https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389

- OECD, 2021. *Children in the digital environment revised typology of risks oecd digital economy papers January 2021 No. 302.* En:
https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1623292179&id=id&accname=guest&checksum=9AC7B897CADEB18BCD05055409C5ADFA

- OECD Innovation Blog, 2021. *Innovation Blog.* [online]. OECD. Disponible en:
https://oecd-innovation-blog.com/2021/06/01/oecd-recommendation-children-digital-environment-online-safety-risks/

- REMOLINA ANGARITA, Nelson. 2013. Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012. 1 ed. Bogotá: Legis Editores.

- SANZ, J., 2020. *Sé Legal En Internet.* [online] Tudecideseninternet.es. Disponible en:
http://tudecideseninternet.es/aepd/guias/se-legal-en-internet.html

- UNICEF, 2020. *Niños En Un Mundo Digital.* [online] Fondo de las Naciones Unidas para la infancia. Disponible en: **https://www.unicef.org/media/48611/file**

- Varios Autores. *Código de Buenas Prácticas para Orientar el Tratamiento en Línea de Datos Personales de Niñas, Niños y Adolescentes. Disponible* en:
https://home.inai.org.mx/wpcontent/documentos/pdpdoctosguias/-codigobuenaspracticasnna.pdf

Algunos sitios de ayuda

A continuación algunos recursos que pueden ser de ayuda para los docentes y padres de familia en la educación de Datos Personales. Pueden encontrar recursos adicionales en:

En TIC Confío:
https://www.enticconfio.gov.co/

Internet Segura 4 Kids:
https://www.is4k.es/educadores

Pantallas Amigas:
https://www.pantallasamigas.net/

Sé Legal en Internet:
https://www.tudecideseninternet.es/aepd/guias/se-legal-en-internet.html