UTPL | Vinculación con la Sociedad

MANUAL DE BUENAS PRÁCTICAS Y PREVENCIÓN DEL CIBERACOSO

GRUPO DE INVESTIGACIÓN:
DERECHOS DIGITALES Y PROTECCIÓN DE DATOS PERSONALES

2024

UTPL | Vinculación con la Sociedad

MANUAL DE BUENAS PRÁCTICAS Y PREVENCIÓN DEL CIBERACOSO

GRUPO DE INVESTIGACIÓN:
DERECHOS DIGITALES Y PROTECCIÓN DE DATOS PERSONALES

COMPILADORES:
PhD. Luis O. Ordoñez Pineda
Mtra. Patricia Pacheco Montoya
Mtra. Maritza E. Ochoa Ochoa

2024

Grupo de Investigación Derechos Digitales y Protección de Datos personales (DIGILAW)

PhD. Luis Oswaldo Ordoñez Pineda
Coordinador

Miembros del Grupo de Investigación DIGILAW

Mgtr. Andrea Catalina Aguirre Bermeo
Mgtr. Sara Auxiliadora Cabrera Jiménez
Mgtr. Denisse Elizabeth Condolo Pardo
Mgtr. Jorge Luis Cueva Flores
Mgtr. María Augusta Herrera Vásquez
Mgtr. Juan Andrés Jaramillo Valdivieso
Mgtr. Carlos Rubén Mogrovejo Riofrío
Mgtr. Paúl Javier Moreno Quizhpe
Mtra. Maritza Elizabeth Ochoa Ochoa
PhD. Luis Oswaldo Ordoñez Pineda
Mtra. Emma Patricia Pacheco Montoya
PhD. Lucia Puertas Bravo
Mgtr. Santiago Israel Puertas Monteros
Mgtr. María Carolina Sacoto Romo

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

ISBN físico: 978-9942-26-364-3
ISBN digital: 978-9942-47-226-7

Diagramación:
EDILOJA Cía. Ltda.
Telefax: 073701444 ext. 3062
San Cayetano Alto s/n
www.ediloja.com
edilojainfo@ediloja.com.ec

Loja-Ecuador
Noviembre, 2024

Introducción

En la actualidad, el ciberacoso representa uno de los desafíos más alarmantes dentro del entorno digital, especialmente, en las comunidades de aprendizaje o instituciones educativas. A medida que las tecnologías de la información y comunicación (TIC) se integra cada vez más en la vida diaria de las personas, también surgen nuevas formas de violencia que pueden afectar, profundamente, su desarrollo de la personalidad. Así, en el caso de estudiantes, podrían existir, además, afectaciones a su desarrollo personal y académico, a partir de las reglas y normas convivencia dentro de las comunidades de aprendizaje, tal como lo ha destacado la Corte Constitucional de Ecuador en la Sentencia 456-20-JP /21, sobre justicia restaurativa y el derecho al debido proceso en contextos educativos /*sexting*.

Al parecer, el uso de dispositivos electrónicos y plataformas digitales ha proporcionado a niños, niñas y adolescentes herramientas transformadoras para la comunicación, pero también los ha expuesto a riesgos significativos, entre ellos el acoso *online*. En este marco, desde la perspectiva académica, el ciberacoso o *cyberbullying* no debería considerarse como una simple extensión de la intimidación tradicional, por cuanto, presenta características propias que lo convierte en mucho más dañino. Por ejemplo, la capacidad de los agresores para acosar a sus víctimas de forma anónima (*Anonymous Online Harassment*) y la velocidad a la que se puede propagar el contenido dañino y la dificultad de escapar del acoso, dado que el entorno digital está presente en casi todos los aspectos de la vida moderna (*Harmful Content*), son factores que exacerban el impacto de esta tipología de violencia.

Según investigaciones recientes, el ciberacoso puede dejar cicatrices emocionales profundas, afectando el bienestar psicológico y la autoestima de los estudiantes, naturalmente, con consecuencias que pudieran perdurar por toda la vida. Por ello, es fundamental que las instituciones educativas, de cualquier instancia, no solo reconozcan la gravedad de este fenómeno, sino que también promuevan investigaciones para comprender sus dinámicas y elaborar mecanismos de prevención y sistemas de alerta temprana. Desde luego, como advierte la Carta Iberoamericana de Principios y Derechos en Entornos Digitales y otros instrumentos internacionales, particular protección deberán tener los niños, niñas y adolescentes en el espacio digital.

Desde esta perspectiva, el "Manual de buenas prácticas y de prevención del ciberacoso" constituye una respuesta aproximada a los peligros que se desprenden del fenómeno de violencia digital. Surge en el marco del proyecto integrador "Ciberacoso en las comunidades de aprendizaje", ejecutado por el Grupo de Investigación "Derechos Digitales y Protección de Datos Personales" y financiado por la Universidad Técnica Particular de Loja. Los temas que se desarrollan tienen relación con: a) Los principios y derechos en los entornos digitales en Iberoamérica; b) La Sentencia 456-20-JP/21 de la Corte Constitucional de Ecuador: La justicia restaurativa y el derecho al debido proceso en contextos educativos / *Sexting*; c) La política pública por una Internet segura para niños, niñas y adolescentes; d) Acciones y estrategias para la prevención del ciberacoso; y, e) Sistematización de buenas prácticas enfocadas a la prevención del Ciberacoso, desde la Universidad Técnica Particular de Loja. Dichos escenarios han permitido investigar e identificar la importancia de códigos de convivencia, políticas públicas y modelos educativos que no solo protejan a sectores vulnerables, particularmente, mujeres y menores de

edad, sino que también promuevan una cultura digital responsable. Por tanto, consideramos que abordar el ciberacoso desde la investigación es también un paso necesario para construir sociedades más seguras y justas en el ámbito digital.

Así las cosas, el Grupo de Investigación "Derechos Digitales y Protección de Datos Personales" de la Universidad Técnica Particular de Loja entiende que es imperativo fortalecer el conocimiento sobre esta problemática, para que las medidas adoptadas por las instituciones educativas no solo sean correctivas, sino preventivas y proactivas. Enfatizamos que, solo, a través, de un esfuerzo conjunto entre investigadores, educadores y legisladores se podrá garantizar un entorno digital más seguro. Lógicamente, un modelo de cultura digital responsable debe tener un enfoque integral, el cual combine la sensibilización sobre el uso responsable de TIC, la formación de los docentes y la implementación de programas restaurativos que permitan una resolución efectiva de los conflictos que surjan, particularmente, en el entorno educativo.

Luis Ordóñez Pineda

1. Los principios y derechos en los entornos digitales en Iberoamérica

Mgtr. María Carolina Sacoto
Mgtr. Carlos Mogrovejo
Mgtr. Denisse Condolo

Iberoamérica, al igual que otras regiones, se ha comprometido a salvaguardar valores fundamentales, inherentes a la dignidad humana, que deben ser defendidos con firmeza, en la búsqueda de sociedades digitales inclusivas, justas, y seguras. Este asunto, que ha sido objeto de repetidos pronunciamientos por diferentes autoridades de la región, ha llevado a consensuar sobre propósitos y principios para que, los derechos que rigen en el mundo físico también sean aplicados y protegidos en el ciberespacio.

Así, estas preocupaciones se han plasmado en iniciativas concretas con carácter declarativo, que tienen el propósito de ser tomadas en cuenta por los Estados Iberoamericanos cuando se trate de implementar o ajustar las leyes nacionales y de poner en práctica políticas públicas relacionadas con la salvaguardia de los derechos y el cumplimiento de las obligaciones en espacios digitales.

Consecuentemente, y por su relevancia, es indispensable abordar la Carta Iberoamericana de principios y derechos en entornos digitales[1], instrumento del cual fueron partícipes 22 países, mismos que en esta era digital, afrontan retos similares a los de Ecuador, con énfasis en la urgente necesidad de proteger a los niños y adolescentes. De este importante

[1] Véase https://www.segib.org/wp-content/uploads/Carta_iberoamericana_derechos_digitales_ESP_web.pdf

documento se destacan las siguientes disposiciones pertinentes para la construcción del presente manual de buenas prácticas y prevención del ciberacoso: 1) La centralidad de la persona. Derechos y deberes en entornos digitales; 2) Privacidad, Seguridad y Confianza; y 3) Especial atención a niñas, niños y adolescentes.

1.1. La centralidad de la persona. Derechos y deberes en entornos digitales

Uno de los principales términos para comprender la presente temática es entender brevemente que es el antropocentrismo, al respecto Anzoátegui (2020) expresa que: (…) el ser humano (…) es el centro y punto de referencia de todas las cosas. (…) Es decir, el mundo es pensado al servicio del hombre, y exclusivamente en función de él cobraría sentido. Por tanto, la Teoría Antropocéntrica pone al ser humano en el centro de esta revolución digital; es decir, todo debe girar alrededor de la persona de sus derechos y de sus obligaciones en el mundo digital

En este sentido, es necesario destacar los derechos fundamentales de los niños, niñas y adolescentes establecidos en la Convención sobre los Derechos del Niño en la resolución 44/25 de 20 de noviembre de 1989, que fueron creados con el propósito de establecer principios elementales que aseguran el bienestar y desarrollo de los menores, especialmente la protección especial que deben tener debido a su condición de personas en desarrollo. Entre los principales destacan: 1) el derecho que tienen los niños, niñas y adolescentes a la igualdad, sin distinción de raza, religión o nacionalidad. 2) Derecho a una protección especial para que puedan crecer física, mental y socialmente sanos y libres. 3) Derecho a educación. 4) Derecho a atención y ayuda preferentes en caso de peligro.

[2] Estos derechos deberán ser las bases, y servir como principios rectores, para garantizar una protección efectiva de los menores en los entornos digitales.

Ahora bien, es preciso mencionar a los derechos digitales más relevantes de los niños, niñas y adolescentes, los que están orientados a igualar los derechos de la ciudadanía en los mundos analógico y digital para reforzarlos y aumentar la confianza de cara al uso de las tecnologías de la información y comunicación. Así, tenemos derechos como el acceso universal e igualitario a internet, protección de datos de los menores en internet, al olvido, ciberseguridad, no discriminación en el mundo y educación digitales que serán analizados a continuación.

El acceso a la internet no solo es un derecho, sino también un medio para ejercer otros derechos reconocidos al ser humano; Commatteo, (2021) expresa que el acceso universal e igualitario a internet:

También se conoce como el derecho a la banda ancha o a conectarse, no solo implica que mediante la conexión se puede lograr la concreción del acceso a la información, sino que involucra la realización de muchos otros derechos. Para esto es fundamental trabajar en el cierre de la brecha digital (…) dado que al universalizar el acceso a Internet estaríamos promoviendo el desarrollo y progreso de la sociedad en su conjunto (p. 398-39).

Las personas necesitan navegar por la web sin importar su condición personal, social, económica o geográfica. La urgencia de esta inclusión digital universal, asequible, de calidad y no discriminatorio

[2] Véase https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/crc_SP.pdf

para toda la población es urgente como equivalente a otras necesidades básicas, como: agua limpia, electricidad y educación. En tales circunstancias, aquellos que están atrasados digitalmente están consecuentemente también excluidos de servicios esenciales como la salud y la educación.

Además, el derecho al acceso universal a Internet (…) promueve el desarrollo sostenible, propicia el crecimiento de la economía digital, también fortalece las capacidades gubernamentales, mientras que su expansión es sustancial para promover la participación ciudadana. Es indudable que permite una gran cooperación entre los gobiernos, y sobre todo frente a una crisis como una pandemia, viabiliza espacios de cooperación virtuales ante el cese de todo tipo de reuniones (Commatteo, 2021, p. 407).

Especialmente con la pandemia de Covid-19 que ha supuesto una acelerada digitalización, el acceso universal e igualitario a internet, garantiza el derecho a intercambiar y compartir conocimientos, ideas, creaciones y de participar en la vida social y política, fortaleciendo el desarrollo de la persona en cuanto al conocimiento y la comunicación al proporcionar, desarrollar y facilitar nuevos mecanismos de intercambio de datos y de información.

Por otro lado, tenemos al derecho de protección de datos. En la Constitución de 2008, se sitúa dentro de los denominados “derechos de libertad” Dotú (2013) expresa que: La libertad se erige como uno de los valores superiores del ordenamiento jurídico y, a su vez, junto con el derecho a la vida y a la integridad física, como uno de los bienes más preciados del individuo (p. 117).

Incluso en el artículo 66 numeral 19 del mismo cuerpo normativo, determina que: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley".

En el sistema ecuatoriano la Constitución de la República del Ecuador (2008) reconoce a las niñas, niños y adolescentes como parte de los grupos vulnerables de atención prioritaria, donde el Estado, la sociedad y la familia, son garantes de la salvaguarda de sus derechos; por tanto, tiene la obligación de protegerlos. Para garantizar su efectividad en el caso de menores a continuación revisaremos los derechos a ser informado, de acceso y de oposición.

Respecto al derecho a ser informado, para Azurmendi (2018)

> Se debería prestar atención a que la información que se ofrece a los menores o a sus representantes legales se diera de forma dosificada mediante avisos, que a su vez fueran simples, concisos y escritos con un lenguaje pedagógico. La información (…) debería situarse siempre en el lugar de la pantalla más visible y durante el tiempo necesario. Al mismo tiempo debería garantizarse que llega siempre a los padres y responsables legales simultáneamente al menor (p. 31).

Es así como cualquier información dirigida específicamente a un niño, niña y adolescente se debe facilitar de forma breve, clara y de fácil acceso, con un lenguaje claro y sencillo, que evite causar confusión o que éstos lleguen a interpretar equivocadamente los hechos informados.

De forma habitual quienes ejercen este derecho en representación de los menores son sus padres o tutores, y deben hacerlo con base a el interés superior del menor. Es por ello que, el Código de la Niñez y Adolescencia, en el artículo 11 menciona que: "El interés superior del niño. - (…) está orientado a satisfacer el ejercicio efectivo del conjunto de los derechos de los niños, niñas y adolescentes; e impone a todas las autoridades administrativas y judiciales y a las instituciones públicas y privadas, el deber de ajustar sus decisiones y acciones para su cumplimiento" (CNA).

Dicho lo anterior, Azurmendi (2018) señala que: En función de la madurez del menor debería considerarse una variedad de opciones para que el menor pudiera ejercitar el derecho de acceso solo, junto con los padres o tutores, o en su caso, mediante la representación de sus padres o tutores. (…) Se debe buscar el equilibrio entre las opciones posibles desde el criterio del interés superior del menor, (…) considerar no sólo la edad del menor sino también de qué datos se trata y la forma en la que han sido obtenidos. Aquí evidenciamos que, aunque el derecho de acceso tiene valor por sí mismo, su alcance es mayor en la medida en que hace posible el ejercicio de derechos como el de rectificación, borrado o bloqueo, para aquellos datos erróneos o inadecuados.

Los centros educativos, personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, con el consentimiento del menor o sus representantes legales, en la publicación o difusión de sus datos personales a través de servicios de redes sociales o afines.

Por otra parte, tenemos el derecho de oposición, es cual tiene el titular de los datos, con mayor razón en el caso de menores, de solicitar que no se lleve a cabo un tratamiento de datos determinado. A diferencia del derecho de cancelación, tal como lo plantea Bordachar (2022): "El ejercicio de este derecho no significa necesariamente la eliminación de los datos del titular. Esto es relevante, ya que en muchos casos el titular no querrá que sus datos sean eliminados, sino únicamente que no se lleve a cabo un determinado tratamiento" (p. 404).

En estos términos, la Reyes Valenzuela (2013) señala que: "este derecho no solamente debe regular en un sentido estricto, en cuanto se refiere a oponerse al tratamiento de todos los datos, sino también en un sentido más amplio, es decir, oponerse al tratamiento de algunos datos personales"(en Pérez, 2020)En este sentido, si el titular de los datos hubiere dado su consentimiento, tiene derecho a oponerse al tratamiento de sus datos personales, si acredita motivos fundados y legítimos con respecto a una situación específica personal que justifiquen el ejercicio de este derecho.

Muñoz (2020), en su trabajo: El derecho al olvido digital, realiza la siguiente reflexión en torno al derecho al olvido:

> (…) conceptuado como el derecho del interesado a la supresión, por parte del responsable del tratamiento, de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando ya no sean necesarios para los fines para los que fueron tomados, cuando el interesado revoque su consentimiento, se oponga al tratamiento o los datos fueran recabados de forma ilícita, entre otras circunstancias (RGPD, 2016).

Es trascendental que toda persona tenga la posibilidad de que eliminen de las listas de resultados, que se obtuvieran tras una búsqueda efectuada en internet a partir de su nombre, los enlaces publicados que contienen información relativa a esa persona; y además, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales o su equivalentes cuando dicha información, en ambos casos, fuese inadecuada, inexacta, no pertinente, no actualizada, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información ya que, esto está vinculado a su derecho a la intimidad.

La ciberseguridad es también considerada como un Derecho digital. Moisés Barrio 2024, en su artículo La ciberseguridad en el Derecho digital europeo novedades de la Directiva NIS2 expresa que:

> La ciberseguridad es el conjunto de técnicas y procesos dirigidos a garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información. (…) busca garantizar el acceso a tecnologías digitales seguras y que protejan la privacidad (es decir, cubre productos y servicios digitales). Y tiene como complemento, por una parte, medidas para aumentar la resistencia de las tecnologías y los productos digitales y, por otra, normas para exigir responsabilidades a quienes traten de socavar la seguridad en línea y la integridad del entorno digital (p. 530).

Considerando que los usuarios domésticos de tecnologías de la información y la comunicación suelen ser blanco de ataques en línea debido a la creciente dependencia de los sistemas de información. Al mismo tiempo, las familias con niñas, niños o adolescentes se encuentran en una posición particularmente difícil ya que, los padres son responsables no solo de su propia seguridad digital, sino también de

la de sus hijos. Por ésta y otras razones es importante que el Estado debe garantizar la seguridad digital para evitar que los datos personales de los usuarios habituales queden expuestos a diversos riesgos como: el robo de identidad y el fraude financiero por mencionar algunos.

Los niños, niñas y adolescentes ya no aprenden como lo hacían antes, sus formas de adquirir conocimiento están cambiando radicalmente por la era o sociedad digital en la que nos encontramos. En palabras de Álvarez (2019):

El mejor instrumento para afrontar este desafío es la educación, que tiene que responder a las necesidades de un mercado laboral en constante transformación. Debe incorporar las competencias digitales y la formación para las nuevas profesiones, sumando los avances tecnológicos a los procesos de aprendizaje (…) que cubran la demanda de empleo en carreras digitales (p. 5).

Del mismo modo que, para lograr dicho objetivo en lo que se refiere al derecho a la educación digital, el artículo 83 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales menciona que:

> (…) El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. (…) deberán incluir (…) situaciones de riesgo

derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red (…).

La implementación y utilización de nuevas herramientas digitales generará responsabilidades no solo para docentes y alumnos sino también para los padres de familia o tutores de niños, niñas y adolescentes para que velen porque los menores de edad hagan uso equilibrado en el entorno digital y se garantice el adecuado desarrollo de su personalidad y preserven su dignidad, reconociendo que su alfabetización digital es esencial en la transformación del intercambio de conocimiento.

Los derechos digitales antes indicados son una muestra de una sólida propuesta de la importancia de promover en los espacios respectivos acciones que culminen con la materialización de leyes acordes con la realidad de la era digital en la que convivimos para reconocer y proteger a los usuarios y sus derechos tanto en Internet como con el uso de las tecnologías digitales.

1.2. Privacidad, Seguridad y Confianza de los espacios virtuales

Los niños y adolescentes cada vez están más expuestos a la tecnología y a la comunicación en línea, lo que plantea preocupaciones sobre su privacidad, seguridad y sobre la confianza en los entornos digitales. Subsecuente, el número de incidentes relaciones con el cometimiento de delitos empleando entornos digitales ha aumentado significativamente en los últimos años. Los menores se están viendo afectados considerablemente, al estar expuestos a contenido inapropiado, puesto que, es fácil encontrar material para adultos, violento o inapropiado. Pero ese no es la principal preocupación, más

bien, es por el uso secundario que pueden hacer ciertas personas con la información proveniente de los datos personales de este grupo prioritario, en consecuencia, su privacidad cada vez está más expuesta en los espacios virtuales. Todo esto puede resultar muy perturbador y perjudicial para su libre desarrollo.

El primer desafío, la privacidad, que plantea algunas consideraciones por el riesgo actual a que los menores sean víctimas de múltiples afectaciones a sus derechos en los entornos digitales, ya sea por su mal uso o por el aprovechamiento de estos espacios por parte de personas inescrupulosas. [3] La privacidad en estos espacios digitales se refiere a la protección de la información personal y la intimidad de los menores en línea, pues, en un mundo cada vez más digital, es esencial garantizar la privacidad en línea para proteger a los niños, niñas y adolescentes de la recopilación no autorizada de datos, la intrusión en su vida personal y otras amenazas. Esto requiere que los niños, niñas y adolescentes tengan una protección especifica y exclusiva, que no sólo garantice su privacidad en los entornos digitales, sino, que se salvaguarde su intimidad, para garantizar el desarrollo de su personalidad y el respeto a su dignidad. (Rodríguez, 2024)

Uno de ellos es la violación de su privacidad en las redes sociales que mantienen, el compartir demasiada información personal en las redes sociales puede llevar a la exposición no deseada de datos personales, especialmente de fotografías, lo que puede ser utilizado por personas oportunistas que, mediante la suplantación de su identidad, fingen ser ellos y perpetran acciones perjudiciales en su nombre. (Herrera de las Heras & Paños, 2022). Es importante recalcar que también se puede producir una violación de la privacidad por parte de

[3] Véase: https://www.aepd.es/documento/la-guia-que-no-viene-con-el-movil.pdf

las empresas, éstas a menudo recopilan datos de los usuarios, incluidos de los menores, lo que plantea preocupaciones sobre la privacidad y la seguridad de esos datos, sobre todo, el qué hacen con esos datos.

Existe un alto riesgo también en ser víctimas de acoso cibernético o en línea, que incluye insultos, amenazas y difamación a través de mensajes de texto, redes sociales y otras plataformas digitales hacia adolescentes, representan una de las principales incidencias que ocurren en los entornos digitales. O el "*grooming*" es otra práctica habitual, utilizada por los depredadores en línea, que mediante tácticas de manipulación se ganan la confianza de los menores, a menudo haciéndose pasar por amigos o personas de confianza, con el objetivo de obtener información personal o persuadir a los menores para que compartan contenido inapropiado. (Zysman, 2022). Y por el *"sexting",* en donde los menores pueden son tentados a enviar imágenes o mensajes de naturaleza sexual a través de mensajes de texto o aplicaciones de mensajería. Esto puede llevar a la distribución no deseada de imágenes y al chantaje en la mayoría de las ocasiones. (Ochoa & Aranda, 2019).

El segundo desafío, la seguridad, es de suma importancia, pues se debe garantizar que los niños y adolescentes estén protegidos mientras navegan por internet y utilizan dispositivos electrónicos. Esto incluye, que a los menores se les debe garantizar un espacio de tranquilidad en los entornos virtuales, que les permita el libre ejercicio de sus derechos individuales; en especial, que perciban seguridad, no sólo de sus datos, de toda la actividad –que han, están y realizarán– en estos espacios digitales.

Razón por la cual, todos los actores que tienen participación –directa o indirectamente–en estos espacios virtuales, de modo

imperativo, deberán promover la educación en seguridad; es fundamental enseñar a los menores sobre los riesgos en línea, y cómo protegerse, puesto que, deben ser conscientes de las amenazas que existen, que no se debe compartir información personal en línea y que solo divulguen información con personas de confianza. (Garmendia, 2011). Es necesario que aprendan a realizar una configuración de privacidad, establecer adecuadamente las opciones de privacidad en sus cuentas en redes sociales, aplicaciones y dispositivos.

Tomando en cuenta que el uso de entornos digitales por parte de menores es alto, es esencial que los padres realicen un control, deben supervisar el uso que sus hijos hacen del internet y de la tecnología, en qué emplean su tiempo y para qué utilizan los entornos digitales, deben limitar el acceso de los menores a sitios web y aplicaciones no apropiadas para su edad. O instalar un *software* de seguridad en los dispositivos que los menores utilizan para protegerlos contra virus, *"malware"* y sitios web maliciosos.[4]

En último lugar, el desafío de la confianza, que va de la mano, con la seguridad, permitirá a los niñas, niños y adolescentes, fiarse de los espacios digitales, que son lugares inmancables; y que si, por cualquier razón, se les llega a vulnerar sus derechos, tengan la certeza que se les protegerá de manera inmediata. Ergo, los proveedores de la información juegan un rol principal, pues, éstos son los que, –en un primer lugar– tienen la obligación de garantizar la reserva, invulnerabilidad, previsibilidad y mitigación de los posibles riesgos del uso de sus espacios.

Esto es esencial para el funcionamiento efectivo y seguro de los entornos digitales, permitiendo generar creencia en la integridad,

4 Véase https://www.aepd.es/guias/guia-privacidad-y-seguridad-en-internet.pdf

protección y confiabilidad de las tecnologías y servicios en línea; así como en la manera en que los menores y organizaciones interactúan en el mundo digital. La seguridad cibernética permitirá alcanzar la confianza en entornos digitales, esto implica la protección de sistemas, datos y redes contra amenazas cibernéticas y otros ataques. Las medidas de seguridad servirán para proteger a los menores, y a sus datos. Por ende, la confianza es un aspecto crítico de la sociedad en línea actual, el promover la seguridad, la privacidad y la integridad en línea es primordial para construir y mantener esta confianza en un mundo cada vez más conectado y dependiente de la tecnología. Promover la seguridad en línea y la confianza en un mundo digital es fundamental para garantizar un entorno en línea seguro y enriquecedor para los niños y adolescentes. (González-Meneses, 2023).

De la mano, se requiere salvaguardar la privacidad de los datos personales, mediante leyes y regulaciones, deben establecerse estándares para la recopilación y el uso de datos personales, lo que es fundamental para la confianza en línea. Para ello, la transparencia de las empresas y organizaciones, deben ser diáfanas sobre cómo recopilan, utilizan y comparten los datos de los usuarios. Esto incluye proporcionar políticas de privacidad claras y comprensibles, y brindar a los usuarios la posibilidad de controlar sus datos. Así mismo, deben promover métodos de identificación y autenticación seguras, para asegurarse de que las personas que acceden a servicios en línea sean quienes dicen ser. De igual manera, las organizaciones deben cumplir con regulaciones y estándares de seguridad cibernética aplicables para garantizar la confianza de los usuarios y la protección de sus datos.

En la misma línea, es importante destacar la estrategia española, específicamente de la Agencia Española de Protección de Datos

(AEPD), que ha estado y está cumpliendo un rol fundamental en la concientización de los riesgos que afrontan los menores en internet. Promoviendo un conjunto de campañas que aminoren y minimicen el impacto del uso de las tecnologías a los derechos de los niños, niñas y adolescentes. De igual manera, ha promulgado una decena de guías, que permitan conocer, al menor y a sus padres, del peligro y las amenazas que podrán encontrarse en los entornos digitales, incluso de las posibles acciones y herramientas que tienen para mitigar el riesgo. De hecho, la AEPD habilitó un canal prioritario para que los menores puedan contactarlos en circunstancias especialmente delicadas, como cuando se difunden contenidos de carácter sexual o que muestran actos de agresión, y se ponen en grave riesgo los derechos, que. tanto la persona afectada como cualquier individuo que tenga conocimiento sobre la difusión de estos contenidos puede utilizar este canal.

En suma, las niñas, niños y adolescentes están constantemente expuestos a los entornos digitales, por lo que sus derechos podrán ser comprometidos en cualquier momento, al ser un grupo sumamente vulnerable, su comportamiento en entornos digitales, debido a ingenuidad, no les permite graduar de forma adecuada las consecuencias de sus publicaciones. Por tanto, y tomando en cuenta los derechos fundamentales, y en particular, el interés superior, que es un principio elemental, se convierte en obligación para todos los actores directos e indirectos, el garantizar una protección singular, que asegure un espacio seguro. Además, es crucial implementar políticas públicas que salvaguarden la integridad, privacidad y bienestar físico y mental de los niños y adolescentes en cualquier entorno digital. Por otro lado, es esencial hacer hincapié en la educación y la adquisición de habilidades digitales que permitan a los niños y adolescentes aprovechar los beneficios de la transformación digital y la potestad de ejercer sus derechos.

En este sentido, es necesario destacar los derechos fundamentales de los niños, niñas y adolescentes establecidos en la Convención sobre los Derechos del Niño en la resolución 44/25 de 20 de noviembre de 1989, que fueron creados con el propósito de establecer principios elementales que aseguran el bienestar y desarrollo de los menores, especialmente la protección especial que deben tener debido a su condición de personas en desarrollo. Entre los principales destacan, el derecho que tienen los niños, niñas y adolescentes a la igualdad, sin distinción de raza, religión o nacionalidad. El derecho a una protección especial para que puedan crecer física, mental y socialmente sanos y libres. Así como, el derecho a educación, y el derecho a atención y ayuda preferentes en caso de peligro. [5] Estos derechos deberán ser las bases, y servir como principios rectores, para garantizar una protección efectiva de los menores en los entornos digitales.

Finalmente, y no menos importante, es imprescindible contar con políticas públicas que ayuden a disminuir el impacto y garanticen la privacidad, seguridad y confianza de los entornos digitales, por ejemplo, el Plan de Confianza en el Ámbito Digital en España de 2013[6] que ha permitido contribuir al desarrollo de la economía y la sociedad digital, disponer de un ciberespacio abierto, seguro y protegido, garantizar un uso seguro de las redes y los sistemas de información, y responder además a los compromisos internacionales en materia de ciberseguridad. También, la Agenda Digital para España[7]. Así como la propuesta actual de Pacto de Estado 'Protegiendo a la infancia y adolescencia en el entorno digital'[8] una iniciativa que fue promovida por la Asociación

[5] Véase https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/crc_SP.pdf

[6] Véase https://plantl.mineco.gob.es/planes-actuaciones/Bibliotecaconfianza/Detalle%20del%20Plan/Plan-ADpE-5_Confianza.pdf

[7] Véase https://www.lamoncloa.gob.es/documents/agendadigital150213.pdf

[8] Véase https://digitalforeurope.eu/pacto-menores-online

Europea para la Transición Digital, que tiene como punto de partida la preocupación por los riesgos que afrontan los y las menores en los entornos digitales al utilizar mayoritariamente servicios que han sido diseñados para adulto.

Estos tres desafíos, son retos que serán abordados en el presente Manual de Buenas Prácticas y de Prevención del Ciberacoso, pero se debe considerar que, para proteger a los menores en entornos digitales, es fundamental que los padres, tutores y educadores estén al tanto de estos riesgos, eduquen a los menores sobre la seguridad en línea y supervisen sus actividades en línea de manera adecuada. También es importante fomentar una comunicación abierta para que los menores se sientan cómodos compartiendo sus preocupaciones y experiencias en línea con adultos de confianza. La privacidad y la seguridad en línea son asuntos críticos para garantizar un entorno digital seguro para los menores. Los padres y tutores deben educar a los menores sobre la importancia de proteger su privacidad en línea. Esto incluye enseñarles sobre la importancia de no compartir información personal, como nombres completos, direcciones, números de teléfono, y fotos comprometedoras con personas desconocidas en línea.[9]

1.3. Especial atención a niñas, niños y adolescentes.

La Carta Iberoamericana de principios y derechos en entornos digitales, en su principio quinto, reconoce expresamente que, en la actualidad, el uso de entornos digitales se ha convertido en una parte fundamental de la vida cotidiana de niñas, niños y adolescentes quienes han adoptado de manera natural y activa dispositivos conectados a internet como herramientas versátiles en diversos aspectos de sus vidas (Djeffal, 2022).

[9] Véase https://www.aepd.es/preguntas-frecuentes/10-menores-y-educacion

En el ámbito educativo, el aprendizaje en línea y el acceso a recursos educativos a través de la web han ampliado las oportunidades de aprendizaje, permitiendo a estudiantes de todas las edades explorar nuevos temas, participar en clases virtuales y acceder a una vasta cantidad de información de manera instantánea (Li, Odhiambo & Ocansey, 2023). Esta digitalización de la educación ha demostrado ser especialmente relevante durante situaciones de crisis, como la pandemia de COVID-19, en donde esta modalidad se convirtió en una necesidad, se desarrolló en las instituciones de educación y ha permanecido a través del tiempo para integrarse como una herramienta más al servicio de la educación (Tinjić & Nordén, 2024).

Fuera ya del ámbito educación, y en cuanto a actividades de esparcimiento, es innegable que las plataformas digitales ofrecen opciones de entretenimiento bastante llamativas para niños, niñas y adolescentes que van desde videojuegos hasta contenido audiovisual en "*streaming*". Así, la tecnología permite que niños y adolescentes puedan conectarse con amigos y compañeros de todo el mundo en juegos en línea, mientras que las plataformas de transmisión de video les brindan acceso a películas, series y contenido creado por internautas. Esto, sin lugar a duda, también ha transformado la manera en la que se experimenta el entretenimiento, ofreciendo una diversidad de opciones y experiencias personalizadas, ajustadas a los gustos e intereses de los menores (Alanko, 2023).

Igualmente, la socialización también ha experimentado un cambio significativo. Las redes sociales y las aplicaciones de mensajería instantánea permiten a niñas, niños y adolescentes mantenerse en contacto con amigos y familiares, compartir sus experiencias y expresar sus opiniones. Estas plataformas permiten construir identidades en línea

y participar en comunidades con intereses similares (Winstone, Mars, Haworth, et al., 2021).

Ahora bien, es cierto que estos entornos ofrecen oportunidades significativas, pero también plantean desafíos que deben ser abordados para garantizar que los niños, niñas y adolescentes puedan beneficiarse de manera segura y saludable de la era digital. La seguridad en línea, la privacidad y la salud psíquica, son algunos aspectos que deben tratarse de manera adecuada por la especial exposición y vulnerabilidad de niños, niñas y adolescentes en los entornos virtuales. Algunos de los retos más destacados que surgen de la interacción de estos grupos en espacios digitales se mencionan a continuación (Jang & Ko, 2023).

Al estar en contacto con personas desconocidas mediante las diferentes aplicaciones móviles o web, los niños y adolescentes son víctimas frecuentes de ciberacoso, que bien puede tomar la forma de acoso verbal, exclusión social o amenazas en línea. La facilidad de comunicación digital permite que el acoso persista fuera del entorno escolar y continúe en espacios privados, lo que puede tener un impacto devastador en su bienestar emocional y psicológico (Zhu, Huang, Evans, & Zhang, 2021).

En ese contexto, se han identificado predadores en línea, quienes aprovechando los entornos digitales utilizan plataformas de redes sociales y mensajería instantánea para tomar contacto con grupos vulnerables, ganarse la confianza de los menores y manipularlos para obtener información íntima y personal, lo cual puede exponerlos a riesgos como el robo de identidad, el uso no autorizado de sus datos personales y prácticas como *"revenge porn"* (Dombrowski, LeMasney, Ahia, & Dickson, 2004). Así, el *sexting*, el envío de mensajes, fotos o

videos sexualmente explícitos a través de dispositivos móviles, resulta un problema creciente, sobre todo entre los adolescentes. Esta tendencia preocupante presenta una serie de desafíos y riesgos que igualmente, deben abordarse de manera integral para proteger a los menores (Mori, Park, Temple, & Madigan, 2022).

A esto, se suma la desinformación y contenido inapropiado, los menores, a menudo tienen dificultades para discernir entre información verídica y desinformación en línea, situación que los lleva a consumir contenido falso e inapropiado, a malinterpretar o tergiversar la información que encuentran en línea, lo cual puede tener consecuencias negativas en su comprensión del mundo y sus valores, en su desarrollo emocional y social. Además, pueden estar expuestos a contenido violento, sexual o perjudicial, riesgo constante que merece una atención especial, para evitar que se vean influenciados por el contenido que consumen en línea, y desemboque en imitación de comportamientos inapropiados o peligrosos y adicciones digitales. Igualmente, la exposición a contenido sexual puede hacer que los menores sean más susceptibles a ser víctimas de acoso sexual o explotación en línea, pues los depredadores pueden aprovecharse de su curiosidad o falta de experiencia para involucrarlos en situaciones peligrosas (Álvarez-Guerrero, Fry, Lu, & Gaitis, 2024).

Estos problemas afectan negativamente el rendimiento académico, las relaciones familiares y la salud psíquica de niños, niñas y adolescentes, y resaltan la necesidad de proteger los derechos fundamentales de este grupo de menores entre ellos, su derecho al bienestar físico y mental, no discriminación, desarrollo, educación, identidad; privacidad, descanso y juego, entre otros. Así lo afirma la Carta Iberoamericana de principios y derechos en entornos digitales, al destacar que el interés superior de niñas, niños y adolescentes debe ser una preocupación central en esta

sociedad de la información. Uno de los aspectos más importantes sería entonces, procurar un acceso seguro y responsable a la tecnología y la información en línea. Esto significa no solo protegerlos de contenido perjudicial o inapropiado, sino también brindarles oportunidades para acceder a contenido educativo y enriquecedor que fomente su desarrollo cognitivo y emocional.

Considerando eso, la prevención del ciberacoso es una parte crucial para salvaguardar el interés superior de los niños y adolescentes en línea, por lo que es fundamental tomar medidas efectivas para prevenirlo y abordarlo cuando ocurra. Es latente la necesidad de implementar medidas para identificar, denunciar y combatir el ciberacoso, así como el accionar destructivo al que se encuentran expuestos niñas, niños y adolescentes (Hendry, Hellsten, & McIntyre, 2023).

Para este fin, es imprescindible educar a menores sobre el uso seguro y responsable de la tecnología y promover una mayor supervisión por parte de los padres y tutores (Office of Educational Technology, 2023). La importancia de la colaboración entre gobiernos, empresas tecnológicas, organizaciones no gubernamentales y la sociedad en general no puede subestimarse. Estas partes interesadas deben trabajar juntas para desarrollar políticas, herramientas y recursos que promuevan el respeto y protección de los menores abordando este desafío de manera efectiva.

Existen ya iniciativas importantes que ayudan a combatir estos desafías. UNICEF, ha desarrollado campañas de educación para prevenir el ciberacoso[10]. UNESCO[11] también se centra en la educación

[10] Véase https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

[11] Véase https://www.unesco.org/es/health-education/safe-learning-environments

y la sensibilización para empoderar a las niñas, niños y adolescentes, así como en la promoción de políticas y estándares internacionales para combatir el ciberacoso. Igualmente, existen organizaciones que ponen a disposición canales de ayuda, como Child Helpline Internacional[12] para atención a menores en riesgo. Incluso autoridades de protección de datos personales se han preocupado por formular estrategias para luchar contra la violencia digital en Iberoamérica[13].

De otro lado, las redes sociales también han puesto a disposición ciertas herramientas que apoyan este objetivo. La aplicación "Snapchat", por ejemplo, cuenta con la iniciativa *"Here for you"*[14] para usuarios en riesgo. Tik Tok, cuenta igualmente con un espacio destinado a la prevención del acoso[15], una guía de bienestar y un portal de denuncias[16]. Por su parte el grupo Meta, en Facebook e Instagram ha implementado espacios para denunciar cuentas de forma anónima, ponen a disposición un centro de ayuda a las familias[17] para proteger a los menores, así como un centro de seguridad[18] que contiene herramientas para combatir situaciones de afección a menores, Instagram cuenta con una guía para padres e indicaciones para procurar un uso seguro de esta plataforma[19]. Asimismo, Twitter cuenta con un centro de ayuda[20] que podría ser útil para este fin.

12 Véase https://childhelplineinternational.org/
13 Véase https://eurosocial.eu/seminarios-web/estrategias-de-las-autoridades-de-proteccion-de-datos-para-erradicar-la-violencia-digital-en-iberoamerica-con-perspectiva-de-genero/
14 Véase https://www.tiktok.com/safety/es-es/bullying-prevention/
15 Véase https://www.tiktok.com/safety/es-es/well-being-guide/
16 Véase https://support.tiktok.com/es/safety-hc/report-a-problem/report-a-video
17 Véase https://familycenter.meta.com/
18 Véase https://about.meta.com/actions/safety/topics/bullying-harassment
19 Véase https://about.instagram.com/es-la/safety
20 Véase https://help.twitter.com/en

Existen también aportes de empresas tecnológicas como la iniciativa "*Safe Zone*", del grupo de telecomunicaciones Orange contra el ciberacoso en los videojuegos y web 3.0, quienes han dado cifras sobre esta problemática, indicando que más de un 20% de *gamers* sufren acoso digital y que la mayor parte de ellos son niños y adolescentes. Así, se ha puesto a disposición de los internautas la llamada *Droid Area* y *Quiz Area*, con las que prestan consejos, recomendaciones y oportunidades de aprendizaje para prevenir y combatir el ciberacoso. Además, cuentan con un botón denominado "*Jump to get Help*" con el que los usuarios en situación de riesgo serán redirigidos a una línea de ayuda[21] (Reason Why, 2023).

Todas estas iniciativas dan cuenta de la relevancia de este asunto y exigen tomar acciones concretas –lo antes posible–, en el marco de los derechos reconocidos en la Convención sobre los Derechos del Niño, que procuren la protección de menores en el uso seguro de las tecnologías digitales. Hay que ser conscientes de esta realidad, y que muchos de los peligros que enfrentan los niños, niñas y adolescentes pueden ser prevenidos, pero la falta de educación digital promueve un uso irresponsable y descuidado de los espacios digitales. Por ello, la mejor manera de garantizar sus derechos es a través de acciones preventivas que fomenten su formación y concienciación, las mismas que se reflejarán en el presente manual.

[21] Grupo Orange. *Orange lanza la iniciativa «Safe Zone» para combatir el ciberacoso en los videojuegos, 14 de noviembre 2022, disponible en* https://www.orange.es/metaverso/noticias/actualidad/orange-lanza-la-iniciativa-safe-zone-para-combatir-el-ciberacoso-en-los-videojuegos *, accedido el 06 de octubre 2023.*

Referencias

Alanko, D. (2023). The Health Effects of Video Games in Children and Adolescents. *Pediatrics in Review*, 44(1), 23-32. https://doi.org/10.1542/pir.2022-005666

Álvarez-Guerrero, G., Fry, D., Lu, M., & Gaitis, K. K. (2024). Online Child Sexual Exploitation and Abuse of Children and Adolescente with Disabilities: A Sistemática Review. *Disabilities*, 4(2), 264-276. https://doi.org/10.3390/disabilities4020017

Álvarez, J. (2019). La educación en la era digital. *Telos: Cuadernos de comunicación e innovación*, Nº. Extra 110, 2019. Recuperado el 25 de septiembre de 2024, de https://telos.fundaciontelefonica.com/wp-content/uploads/2019/04/telos-110-enlighted-editoriales-jose-maria-alvarez-pallete-cesar-alierta.pdf

Asamblea Constituyente del Ecuador. (2008, 20 de octubre). Constitución de la República del Ecuador. *Registro Oficial 449.*

Anzoátegui, M. (2020). Antropocentrismo. Interinsular: Ciencia, Derecho, Filosofía y Animales. En Memoria Académica. Disponible en: http://www.memoria.fahce.unlp.edu.ar/art_revistas/pr.12068/pr.12068.pdf

Azurmendi, A. (2018). "Derechos digitales de los menores y datos masivos. Reglamento europeo de protección de datos de 2016 y la Coppa de Estados Unidos". *El profesional de la información*, v. 27, n. 1, pp. 27-35. http://dx.doi.org/10.3145/epi.2018.ene.03

Barrio, M. (2024). La ciberseguridad en el Derecho digital europeo novedades de la Directiva NIS2 *Indret: Revista para el Análisis del Derecho*, Nº. 1. https://raco.cat/index.php/InDret/article/view/425695/520231

Bordachar, M. (2022). Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO. *Revista chilena de derecho y tecnología*, 11(1), 397-414. https://doi.org/10.5354/0719-2584.2022.67205

Congreso Nacional del Ecuador. (2003, 3 de enero). Código de la Niñez y Adolescencia. *Registro Oficial 737.*

Commatteo, G. (2021) El rol de los parlamentos en garantizar el acceso universal a internet como derecho humano. *Revista Internacional de Derechos Humanos* Vol. 11, Nº. *2, 2021.* https://dialnet.unirioja.es/servlet/articulo?codigo=8515707

Djeffal, C. (2022). Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment. *Laws*, 11(6), 84. https://doi.org/10.3390/laws11060084

Dombrowski, S. C., LeMasney, J. W., Ahia, C. E., & Dickson, S. A. (2004). Protecting Children From Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations. *Professional Psychology: Research and Practice*, 35(1), 65–73. https://doi.org/10.1037/0735-7028.35.1.65

Dotú I Guri, M. D. M. (2013). Los derechos fundamentales: derecho a la libertad frente a las medidas cautelares penales: (ed.). Barcelona, Spain: J.M. BOSCH EDITOR. Recuperado de https://elibro.net/es/ereader/bibliotecautpl/59797?page=117

Garmendia Larrañaga, M. (2011). *Riesgos y seguridad en internet : los menores españoles en el contexto europeo*. Universidad del País Vasco.

Grupo Orange. (2022, 14 de noviembre). Orange lanza la iniciativa «Safe Zone» para combatir el ciberacoso en los videojuegos. Recuperado el 6 de octubre de 2023, de https://www.orange.es/metaverso/noticias/actualidad/orange-lanza-la-iniciativa-safe-zone-para-combatir-el-ciberacoso-en-los-videojuegos

Hendry, B. P., Hellsten, L. M., & McIntyre, L. J. (2023). Recommendations for cyberbullying prevention and intervention: A Western Canadian perspective from key stakeholders. *Frontiers in Psychology*, 14, 1067484. https://doi.org/10.3389/fpsyg.2023.1067484

Herrera de las Heras, R., & Paños Pérez, A. (2022). *La Privacidad de los menores en redes sociales : especial consideración al fenómeno influencer*. Atelier Libros Jurídicos.

Jang, Y., & Ko, B. (2023). Online Safety for Children and Youth under the 4Cs Framework—A Focus on Digital Policies in Australia, Canada, and the UK. *Children*, 10(8), 1415. https://doi.org/10.3390/children10081415

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Li, X., Odhiambo, F. A., & Ocansey, D. K. W. (2023). The effect of students' online learning experience on their satisfaction during the COVID-19 pandemic: The mediating role of preference. *Frontiers in Psychology*, 14, 1095073. https://doi.org/10.3389/fpsyg.2023.1095073

Machado, J. (2020). El Derecho al Olvido Digital. *Docta Complutense.* https://hdl.handle.net/20.500.14352/11314

Mori, C., Park, J., Temple, J. R., & Madigan, S. (2022). Are Youth *Sexting* Rates Still on the Rise? A Meta-analytic Update. *Journal of Adolescent Health*, 70(4), 531-539. https://doi.org/10.1016/j.jadohealth.2021.10.026

Ochoa Pineda, A. C., & Aranda Torres, C. J. (2019). *Sexting: signo de identidad juvenil en la sociedad digital*. Editorial Universidad de Almería.

Office of Educational Technology. (2023). Parent and Family Digital Learning Guide. U.S. Department of Education. Recuperado de https://tech.ed.gov/publications/digital-learning-guide/parent-family/

Pérez, M. R. (2020). Protección de datos personales y derecho a la autodeterminación informativa: Régimen jurídico. *Revista De Derecho*, (28), 107–138. https://doi.org/10.5377/derecho.v0i28.10146

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Rodríguez Prieto, R. (2024). Menores, privacidad y derechos humanos en la escuela. El caso de Google workplace for education en España. *DERECHOS Y LIBERTADES: Revista de Filosofía Del Derecho y Derechos Humanos*, *50*, 199–224. https://doi.org/10.20318/dyl.2024.8240.

Tinjić, D., & Nordén, A. (2024). Crisis-driven digitalization and academic success across disciplines. *PLoS ONE*, 19(2), e0293588. https://doi.org/10.1371/journal.pone.0293588

Winstone, L., Mars, B., Haworth, C.M.A. et al. (2021). Social media use and social connectedness among adolescents in the United Kingdom: a qualitative exploration of displacement and stimulation. *BMC Public Health*, 21, 1736. https://doi.org/10.1186/s12889-021-11802-9

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures. *Frontiers in Public Health*, 9, 634909. https://doi.org/10.3389/fpubh.2021.634909

Zysman, M. (2022). *Grooming*: cómo enseñar a los chicos a cuidarse en la web. Bonum. https://elibro-net.sire.ub.edu/es/lc/craiub/titulos/2195012.

2. Sentencia 456-20-JP /21 de la Corte Constitucional de Ecuador: La justicia restaurativa y el derecho al debido proceso en contextos educativos /*Sexting*

Mtra. Patricia Pacheco
Mgtr. Paúl Moreno
Mgtr. María Augusta Herrera

Introducción

Ante las nuevas formas de violentar la integridad de los niños, niñas y adolescentes el Comité de los Derechos del Niño ha emitido la Observación General No. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital.

En este sentido, los entornos digitales están en constante evolución y expansión, y abarca las tecnologías de la información y las comunicaciones, incluidas las redes, los contenidos, los servicios y las aplicaciones digitales, los dispositivos y entornos conectados, la realidad virtual y aumentada, la inteligencia artificial, la robótica.

De esta forma, el entorno digital reviste una creciente importancia para casi todos los aspectos de la vida de los niños y de la población en general ya que las funciones sociales, como la educación, los servicios gubernamentales y el comercio, dependen cada vez más de las tecnologías digitales, ofreciendo de esta manera nuevas oportunidades para hacer efectivos los derechos de los niños, pero también bosqueja riesgos relacionados con su violación o abuso.

Por otro, lado el Comité de Derechos del Niño refiere que el entorno digital puede abrir nuevas vías para ejercer violencia contra los niños al facilitar situaciones en que estos estén expuestos a la violencia o puedan verse influidos a hacerse daño a sí mismos o a otros, así mismo indica que los delincuentes sexuales pueden utilizar las tecnologías digitales para abordar a los niños con fines sexuales y para participar en abusos sexuales de niños en línea, por ejemplo mediante la emisión de vídeos en directo, la producción y distribución de material visual de abusos sexuales de niños y la extorsión sexual (Organización de las Naciones Unidas, 2021).

Ante ello, los estados parte deben reforzar las políticas públicas con relación a los entornos digitales y protegerlos a los niños, niñas y adolescentes de cualquier acto de violencia contra su integridad personal, tal es así que en nuestra legislación máximo órgano de control, interpretación y administración de justicia como es la Corte Constitucional con la Sentencia No. 456-20-JP/21 (La justicia restaurativa y el derecho al debido proceso en contextos educativos) analiza esta figura del *sexting* por ser grave y novedosa y que tiene relación con el *sexting, sextorsión y grooming.*

Finalmente, la sentencia de jurisprudencia vinculante No. 456-20-JP/21 de la Corte Constitucional del Ecuador, analiza y conmina a que los conflictos en el ámbito educativo apliquen la justicia restaurativa o sanadora a fin de que el ofensor se responsabilice y repare a la víctima, y de esta manera utilicen los diferentes programas restaurativos y no se recurra a la caduca forma retributiva o sancionatoria, garantizando con ello el interés superior del niño, niña o adolescente cuando hay cometido una conducta delictiva.

2.1 Contexto del *sexting*

En una era marcada por la llegada de la Revolución Digital, la cual ha transformado la cotidianidad de las personas, aparecen nuevos conceptos y teorías que buscan explicar los cambios por los que atraviesa nuestra sociedad. La revolución tecnológica ha redimensionado la dinámica de las relaciones interpersonales y de los procesos incorporados a los distintos ámbitos de la sociedad.

> El incremento de uso de las Tecnologías de la Información y la Comunicación ha permitido afianzar el enlace entre el entorno social, personal, empresarial y académico. Este fenómeno ha sido renombrado por algunos investigadores como "sociedad de la información". La aparición de Internet marca un antes y un después en la forma de compartir información como elemento básico para que la sociedad funcione de forma versátil. (Moreira et al., 2019, p. 87)

Las TIC han abierto nuevos horizontes de interacción social que logran la exposición de múltiples vulnerabilidades digitales, pudiendo ser la interacción con extraños o víctimas de acoso cibernético. El delito más común que ha aprovechado este avance es el *Sexting*. (Moreira et al., 2019, p. 91)

Las definiciones dadas por Lounsbury, Mitchell y Finkelhor; Marrufo; Menjívar; Wolak y Finkelhor citados por Mercado, Pedraza y Martínez señalan que:

> El término "*sexting*" originalmente hace referencia a la combinación de sexo (*sex*) y enviar textos por teléfono móvil (*texting*), sin embargo, con el avance de la tecnología ya no es

> posible delimitarlo al uso de teléfonos móviles, sino que se ha permeado en aquellos mensajes con imágenes como fotografías o videos sexualmente sugestivas enviados a través de algún espacio virtual. (2016, p. 4)

El *sexting* ha irrumpido en la vida de muchas personas, influyendo en la forma en que expresamos nuestra sexualidad y establecemos conexiones en la era digital.

Para Moreira, Maldonado y García:

> El *sexting* es una nueva tendencia de conversaciones, el deseo natural de explorar la sexualidad ha llevado a los jóvenes a interesarse por este fenómeno que consiste en compartir contenido sexual (fotos, videos) de manera interna y que a su vez son publicados abiertamente por alguno de los dos al momento de su ruptura o mínima discusión, provocando así un chantaje, destrucción de personalidad o venganza estimada. (2019, p. 92)

El *sexting* conlleva todas las acciones que tienen por objeto exhibir por redes sociales fotografías, videos o similares de las personas con contenido sexual (Peris y Maganto, 2018, p. 52).

Según (Ojeda et al., 2020), el *sexting* tiene mayor relevancia entre la población adolescente en quienes se presenta incluso de forma común y con naturalidad entre sus conversaciones a través de dispositivos móviles. No obstante, no deja de ser un acto en el que se exponen riesgos muy difíciles de contrarrestar.

Mercado, Pedraza y Martínez (2016) destacan que uno de los aspectos más estudiados en relación con este fenómeno son las causas

que diversos autores identifican como factores de riesgo, los cuales actúan como antecedentes de la práctica del *sexting*. Entre estos factores se encuentran:

> La exploración de la sexualidad, la diversión y excitación que genera (Baumgartner, Sumter, Peter, Valkenburg y Livingstone 2014; Marrufo, 2012), la falta de atención y supervisión, y la falta de presiones normativas y sanciones legales (Agustina, 2010; Cuesta y Gaspar, 2013); fracaso académico, vulnerabilidad de la dignidad, daños psicológicos, ansiedad, aislamiento, depresión, levantamiento de cargos legales por pornografía infantil e incluso suicidio de la persona expuesta (Farber et al., 2012; Marrufo, 2012), así como también se ha mencionado tanto como causa y consecuencia el uso del alcohol y de sustancias ilegales, así como ser una plataforma para llevar a la realidad dichas relaciones (Benotsch, Snipes, Martin y Bull, 2013, p. 5)

Así mismo, para los autores Fajardo, Gordillo y Regalado (2013) existen numerosos aspectos que agravan la práctica del *sexting* en adolescentes, dentro de ellos se pueden destacar:

1. Inconsciencia de riesgo potencial: "Ellos no siente el peligro de las nuevas tecnologías porque nacieron con ellas y se imitan a través de éstas" En este sentido, la culpa no radica en los recursos que ofrece Internet, sino la propia percepción de los adolescentes, los cuales "no perciben la diferencia entre lo que es público y lo que es privado". (De Domini, 2009; citado por Menjívar, 2010)

2. Brecha generacional: hace alusión a la falta de comprensión de la **generación** de migrantes tecnológicos (Menjívar, 2010)

3. Sexualidad precoz de la infancia: este concepto se refiere a la tendencia que se está dando en los últimos años de adelantar la adolescencia a edades cada vez más tempranas, manifestándose sobre todo en las niñas e implicando el desarrollo de las características propias de la edad, entre ellas la definición sexual. (Pérez et al., 2011)

4. Inmediatez de las comunicaciones: el acceso a las nuevas tecnologías brinda cada día una mayor disponibilidad, facilidad, portabilidad y economía, lo que implica que los impulsos pueden hacerse realidad sin posibilidad de vuelta atrás. (2013, pp. 523-524)

Por su parte, la Corte Constitucional del Ecuador (CCE, 2021) en sentencia Nro. 2064-14-EP/21, de fecha 27 de enero de 2021 señala que las fotografías íntimas son datos personales sensibles que "pertenecen a la esfera más íntima del individuo dado que esta constituye una manifestación del ejercicio de su sexualidad" (párr. 152)

En relación con la indicada sentencia el Juez Constitucional Enrique Herrería Bonnet, en la fundamentación del Voto Salvado en la sentencia Nro. 456-20-JP/21, de fecha 10 de noviembre de 2021, establece:

> En la prenombrada sentencia, se indicó que el uso indebido de esta información podría acarrear graves consecuencias para el titular del dato, pues su uso no autorizado tiene la potencialidad de vulnerar los derechos a la protección de datos personales, a la autodeterminación informativa, a la honra, al buen nombre, al manejo de la propia imagen y a la intimidad. Estos escenarios son más alarmantes en contextos educativos donde niños, niñas

y adolescentes son víctimas de la difusión no autorizada de datos sensibles. (p. 35)

Ante ello el jurista ya expresa que el no consentimiento de divulgar fotos vulnera la integridad y más aún si se trata de este grupo de atención prioritaria como son los niños, niñas y adolescentes, que no miden las consecuencias en este tipo de actos.

La Observación General No. 25 del Comité de los Derechos del Niño relativa a los derechos de los niños en relación con el entorno digital, señala que el entorno digital proporciona nuevas oportunidades para la perpetración de violencia contra menores. Las formas de violencia, explotación y abuso sexual pueden abarcar comportamientos en línea como ciberacoso, que involucra intimidación y amenazas que afectan la reputación de la víctima, así como la creación o intercambio de textos o imágenes de carácter sexual sin consentimiento, incluyendo contenido generado por la víctima bajo coerción o presión. (Organización de las Naciones Unidas, 2021)

Los Estados deben adoptar todas las medidas apropiadas para proteger a los niños frente a todo lo que constituya una amenaza para su derecho a la vida, la supervivencia y el desarrollo; con enfoques de enfoques de prevención, salvaguardia y justicia restaurativa respecto de los niños afectados.

La Constitución de la República del Ecuador (2008) partiendo del principio de interés superior del menor, consagra un ámbito protectorio que establece un conjunto de medidas de seguridad destinadas a prevenir situaciones que puedan amenazar la integridad sexual de los niños, niñas y adolescentes, resguardando su dignidad y abordando

los posibles impactos negativos derivados del uso inapropiado de la tecnología en su desarrollo integral. (Arts. 35 y 46)

En Ecuador el "*sexting*" no se encuentra incorporado al catálogo de delitos contenido en el Código Orgánico Integral Penal (2014), el tratamiento que ha dado el Ministerio de Educación, mediante los Protocolos y Rutas de Actuación frente a hechos de violencia y/o violencia sexual detectados o cometidos en establecimientos del sistema educativo nacional, encasilla a este tipo de actos en el delito de pornografía con utilización de niñas, niños o adolescentes contenido en el artículo 103 de la norma punitiva, al definir al *sexting* como:

> Una forma de tener sexo a través de internet, mediante el envío de videos o imágenes íntimas o teniendo relaciones sexuales. Estas imágenes pueden ser compartidas a través de las redes con otras personas, volviéndose un caso de pornografía infantil en el caso de niños, niñas y adolescentes (MINEDUC, 2014, p. 32).

La Corte Constitucional por su parte considera que el *sexting* entre adolescentes y en comunidades educativas, como otros fenómenos relacionados con el uso de la tecnología, no puede ser pensando siempre y exclusivamente desde la perspectiva de la violencia y de la legislación penal. De ahí la necesidad de adoptar, adecuar y utilizar las regulaciones existentes para afrontar el *sexting* desde el enfoque de una comunidad de aprendizaje y desde la justicia dialógica, participativa y restauradora (CCE, sentencia Nro. 456-20-JP/21, 2021, párr. 102).

El *sexting,* es un fenómeno complejo que ha transformado la forma en que las personas se relacionan en la era digital. Esta práctica, conlleva riesgos y preocupaciones importantes. La exposición no deseada, la pérdida de privacidad y las implicaciones legales son amenazas que

requieren una consideración seria. Además, el *sexting* plantea desafíos éticos relacionados con el consentimiento y la responsabilidad personal, así como la responsabilidad del Estado de velar por la protección de los derechos de los ciudadanos, con especial énfasis en niños, niñas y adolescentes.

2.2 Las comunidades de aprendizaje

Los estudios referentes a los cambios que debe tener la educación del futuro insisten en la necesidad de generar comunidades educativas o comunidades de aprendizaje, entendiendo que son las que están conformadas por la escuela, la familia y la sociedad, en la que estos actores colaboran para optimizar la educación y el aprendizaje, como lo indican Hampson, Patton y Shanks, citados por Scott (2015).

Las comunidades de aprendizaje fundamentan su accionar en el aprendizaje dialógico, concepción que fue desarrollada por la *Community on Research of Excrellence for All* (CREA) "Comunidad de Investigación para la Excelencia de Todos" quienes a su vez se basaron en las ideas desarrolladas en los estudios de Vygotsky, Bruner, Mead, Bakhtin y Habermas[22], en las cuales se manifiesta que para mejorar el aprendizaje se debe contar con el diálogo igualitario como uno de sus elementos centrales (CIPPEC, s/f).

[22] Diversos autores se han referido a la naturaleza dialógica del lenguaje y de la condición humana (Bakhtin, 1981; Mead, 1990; Vygotsky, 1986) así como del diálogo como un requisito indispensable para la convivencia entre personas (Habermas, 1987; Freire, 1997). La perspectiva dialógica en el aprendizaje se puede definir a través de la interacción social entre personas, mediada por el lenguaje. A través del diálogo las personas intercambian ideas, aprenden conjuntamente y producen conocimiento, encontrando y creando nuevos significados que transforman el lenguaje y el contenido de sus vidas. Valls, R.; Soler, M. y Flecha, R. (2008).

Para la ONG Grupo Faro, las comunidades de aprendizaje se forman con la participación comprometida de sus integrantes lo que permite a través del aprendizaje dialógico la mejora significativa de los procesos educativos y de la convivencia escolar. Este aprendizaje dialógico se basa en "7 principios: diálogo igualitario, inteligencia cultural, transformación, creación de sentido, solidaridad, dimensión instrumental e igualdad de diferencias" (2022). Por lo cual estas comunidades de aprendizaje pasan de ser un mero enunciado a prácticas de mejora del sistema educativo de nuestro país.

En la sentencia del caso No. 456-20-JP la Corte Constitucional también se refiere a las comunidades de aprendizaje e indica que estas no pueden ser consideradas como "otra forma de asociación o de reunión de personas", sino que son espacios para "satisfacer el derecho a la educación" y justamente este es el rol de los centros educativos, dentro de los que encontramos a las escuelas y colegios que son en sí las comunidades de aprendizaje. (Sentencia No. 456-20-JP, párrafo 46). Las cuales deben actuar observando lo establecido en el artículo 27 de la Constitución del Ecuador en donde se indica los fines[23], principios[24] y objetivos[25] de la educación.

[23] Los fines de la educación son: La educación es indispensable para el conocimiento, el ejercicio de los derechos y la construcción de un país soberano, y constituye un eje estratégico para el desarrollo nacional. Cfr. Art. 7 Constitución de la República del Ecuador.

[24] Los principios de la educación establecidos en la Constitución son: La educación se centrará en el ser humano y garantizará su desarrollo holístico, en el marco del respeto a los derechos humanos, al medio ambiente sustentable y a la democracia. Cfr. Art. 7 Constitución de la República del Ecuador.

[25] La Constitución ecuatoriana establece como objetivos de la educación a los siguientes: será participativa, obligatoria, intercultural, democrática, incluyente y diversa, de calidad y calidez; impulsará la equidad de género, la justicia, la solidaridad y la paz; estimulará el sentido crítico, el arte y la cultura física, la iniciativa individual y comunitaria, y el desarrollo de competencias y capacidades para crear y trabajar. Cfr. Art. 7 Constitución de la República del Ecuador.

Es necesario recalcar que en la sentencia se utiliza indistintamente tanto el término comunidades de aprendizaje como el de comunidades educativas, entendiendo que más allá del nombre, cuando se habla de comunidades en el contexto educativo se refiere a aquellas en las que participan alumnos, maestros, personal administrativo y padres de familia para garantizar y cumplir con el derecho a la educación, para lo cual es importante y necesario que cada institución educativa tenga un código de convivencia que será el instrumento que permita la resolución de conflictos que se pudieran presentar; conflictos que son inevitables y que deben ser aprovechados para su análisis y para buscar estrategias para prevenir casos similares, lo cual fortalece la convivencia de los entornos educativos.

Así en el caso en análisis, el hecho de la difusión de las fotografías (*sexting* pasivo) no es considerado como un hecho personal o de afectación limitada entre las dos adolescentes (la adolescente fotografiada y la adolescente que difundió las imágenes), si no que al ser realizado por miembros de una comunidad de aprendizaje, es toda esta comunidad la que se ve afectada, más cuando son varias las adolescentes que compartieron las imágenes, y que a la larga involucró a docentes, directivos de la institución y padres de familia. Por ello es necesario que, para solucionar este conflicto con base a lo establecido en el código de convivencia institucional, se hayan aplicado herramientas de diálogo, de tal forma que, a partir de la implementación de una pedagogía dialógica, llegar a una justicia dialógica (justicia restaurativa), todo en beneficio de los integrantes de la comunidad de aprendizaje.

Para ello era necesario y fundamental que la institución educativa garantice el debido proceso[26] y la participación plena de la comunidad educativa, (de la comunidad de aprendizaje), al permitir que las partes involucradas, alumnas, padres de familia, profesores, puedan intervenir, libremente y sin presiones de ninguna clase; y que las instancias o reuniones que se establezcan al interno de las instituciones educativas, para tratar las presuntas faltas cometidas, sean llevadas en espacios de diálogo y en cumplimiento de lo establecido en el código de convivencia institucional y de la normativa nacional de educación. (Art. 58 Ley Orgánica de Educación Intercultural [LOEI], 2011; Art. 331 Reglamento LOEI, 2023)

No se debe pasar por alto que si el hecho fue realizado en la comunidad de aprendizaje, es toda la comunidad la afectada, y por lo tanto también es la comunidad en su conjunto la que es considerada al momento de la sentencia, así, aunque es el colegio el más afectado por la decisión al considerar que vulneró el debido proceso al que tenía derecho la adolescente que difundió las fotografías y es quién tiene que reparar el daño cometido, el difundir la sentencia y observar los procedimientos incluye a toda la comunidad.

[26] Ley Orgánica de Educación Intercultural (LOEI), artículo 58, "Son deberes y obligaciones de las instituciones particulares: (…) literal e): Garantizar el debido proceso en todo procedimiento orientado a establecer sanciones a los miembros de la comunidad educativa, docentes, trabajadoras y trabajadores, padres, madres de familia o representantes legales y estudiantes". Lo cual guarda relación con lo establecido en el artículo 331 del Reglamento a la LOEI que dice: "las faltas leves y las faltas graves deben ser conocidas y resueltas dentro de la institución educativa mediante el mecanismo previsto en su Código de Convivencia, otorgándoles al estudiante y a su representante legal el derecho a la defensa"60 y agrega que "En los procesos sancionatorios o disciplinarios previstos en la Ley Orgánica de Educación Intercultural y en este reglamento, se debe dar estricto cumplimiento a lo dispuesto en su artículo 136 y en el 76 de la Constitución de la República".

Es importante recalcar que en este caso no se analiza si la conducta realizada por la adolescente es o no *sexting*, sino que lo que se considera es si el colegio aplicó correctamente su proceso sancionatorio; y es justamente en lo cual disiente el Juez Constitucional Enrique Herrería y en su voto salvado indica en primer lugar que, a su criterio, no existió violación al debido proceso, ni se han vulnerado derechos de la menor infractora, por lo que considera que esta sentencia no debía ser una sentencia *inter partes* y más bien era necesario analizar jurídicamente el hecho que ocasionó la sanción del colegio y crear precedentes *erga omnes* respecto a la "imposición de sanciones en el contexto de la difusión no consentida de imágenes privadas de niños, niñas y adolescentes" (párrafo 21), y cuidando siempre que cualquier procedimiento que se adopte no produzca una revictimización de la afectada; considerando además que la justicia restaurativa no puede ser aplicada en todos los casos, como por ejemplo en casos de acoso escolar o de *sexting*.

2.3. La justicia restaurativa y los códigos de convivencia

El creador de la justicia restaurativa expresa que este nuevo modelo aporta un verdadero cambio de paradigma, del modelo retributivo (castigo) al restaurador (sanador), tomando como eje central los daños y las necesidades tanto de la víctima como el delincuente (ofensor) y la comunidad; por lo tanto, es solidaria y cooperativa en los procedimientos en los que estarán involucrados. Todo esto con el fin de corregir los caminos que nacieron mal (Zehr, 2007).

En el Manual sobre programas de Justicia Restaurativa de la Oficina de Naciones Unidas contra la droga y el delito (2006) a la justicia restaurativa se la describe de las siguientes formas:

> "justicia comunitaria", "hacer reparaciones", "justicia positiva", "justicia relacional", "justicia reparadora", y "justicia restauradora", todo programa que utilice procesos restaurativos e intente lograr resultados restaurativos". (…) El énfasis en esta definición está claramente presente en los procesos participativos diseñados para alcanzar resultados deseados. Un "proceso restaurativo" se define como "todo proceso en que la víctima, el delincuente y, cuando proceda, cualesquiera otras personas o miembros de la comunidad afectados por un delito participen conjuntamente de forma activa en la resolución de las cuestiones derivadas del delito, por lo general con la ayuda de un facilitador. (pp. 6-7)

Con la justicia restaurativa lo que se propone es un cambio de paradigma, es decir la reparación y no en el castigo; mediante el establecimiento de programas que se centren en la solución del conflicto, desde las partes que lo originaron y no en el *ius puniendi* del Estado; mediante el diálogo y los diferentes procesos que la regulan, en especial con enfoque en justicia juvenil, pero para alcanzar ese cambio hay que llegar al reconocimiento de que el delito es un hecho humano concreto y que, por lo tanto, afecta a las víctimas, ofensor y comunidad; por lo que, se debe promover la búsqueda de la reconciliación, pero sin olvidar la reparación del daño o la restitución.

Ante ello, la Corte Constitucional en la sentencia nro. 456-20-JP/21 (La justicia restaurativa y el derecho al debido proceso en contextos educativos) indica que el proceso fue sancionatorio y no restaurador, a más de ello la sanción lejos de ser educativa y reparadora afectó a la víctima ya la ofensora ya que optaron por desertar del colegio.

Por otro lado, no se garantizó un debido proceso, es decir no se tomó en cuenta su opinión tal como refiere Convención de Derechos

del Niño (1989) en su artículo 12, pues no se garantizó este derecho ser consultado que lo ampara también el Art. 60 del Código de la Niñez y Adolescencia, en concordancia con la Observación General nro. 12 (2009) sobre "El derecho del niño a ser escuchado" del Comité de Derechos del Niño, vulnerándose de esta manera el interés superior del niño consagrado en el Art. 3 de la CDN, Art. 11 del CONA, que expresa que es un "principio que está orientado a satisfacer el ejercicio efectivo del conjunto de los derechos de los niños, niñas y adolescentes; e impone a todas las autoridades administrativas y judiciales y a las instituciones públicas y privadas, el deber de ajustar sus decisiones y acciones para su cumplimiento" (Art. 11).

Sin duda alguna al no escucharse a la adolescente sancionada se vulneró su interés superior no habiendo un debido proceso, pues en el ámbito educativo primero se debe agotar la justicia restaurativa a través de sus diferentes programas que ofrece este nuevo paradigma de solución de conflictos.

En este sentido el ya referido Manual sobre programas de Justicia Restaurativa de la Oficina de Naciones Unidas contra la droga y el delito (2006), señala:

a. Apoyar a las víctimas, darles una voz, motivarlas a expresar sus necesidades, permitirles participar en el proceso de resolución y ofrecerles ayuda.

b. Reparar las relaciones dañadas por el crimen, en parte llegando a un consenso sobre cómo responder mejor al mismo.

c. Denunciar el comportamiento criminal como inaceptable y reafirmar los valores de la comunidad.

d. Motivar la responsabilidad de todas las partes relacionadas, especialmente de los delincuentes.

e. Identificar resultados restaurativos y directos. En lugar de enfatizar las reglas que se han roto y el castigo que debe ser impuesto, tienden a enfocarse principalmente en las personas dañadas. La justicia restaurativa se basa en las relaciones y se esfuerza en conseguir resultados que satisfagan a un grupo amplio.

f. Reducir la reincidencia motivando el cambio en los delincuentes particulares y facilitando su reintegración a la comunidad.

g. Identificar los factores que causan el delito e informar a las autoridades responsables para que implementen estrategias de reducción del delito (pp. 10-11).

Con todos estos enunciados lo que pretende este nuevo paradigma restaurativo es reparar el daño causado entre víctima, ofensor y la comunidad, pese a que, en la legislación de Ecuador, en el Código de la Niñez y Adolescencia no se regule la justicia restaurativa en el Protocolo de actuación frente a situaciones de violencia detectadas o cometidas en el sistema educativo.

Ante lo indicado en el Manual de Justicia Restaurativa emitido por el Ministerio de Educación se regulan las prácticas de justicia restaurativa informal (la escucha, las declaraciones afectivas, la comunicación no violenta, las preguntas restaurativas en caso de conflicto; y las pequeñas reuniones restaurativas espontaneas) así como también las prácticas restaurativas fórmales (círculos restaurativos, la mediación escolar y la

reunión restaurativa) que es donde se reúnen las personas participantes (víctimas, ofensores, comunidad y las personas de apoyo más próxima) en formas de círculo, con ello lo que se pretende es reparar a la víctima y a la comunidad por el daño causado. Sin embargo, esto no fue posible, en el caso analizado, puesto que la entidad educativa no agotó primero la justicia restaurativa sino más bien directamente sancionó a la estudiante, no habiéndose garantizado un debido proceso.

Con ello cuando existen este tipo de conflictos en una institución educativa lo que se debe pretender es aplicar los tres pilares de la justicia restaurativa que son: los daños y necesidades; las obligaciones y la participación (Zher, 2007), estos tres pilares son fundamentales para reparar el daño.

En el caso en concreto no se aplicó justicia restaurativa para cumplir con los tres pilares, que como fin tienen reparar el daño causado por la reproducción de las fotos sin el consentimiento de la víctima; y pedir las disculpas del caso, ya que de esta manera se evitaba que las víctimas primarias y secundarias, deserten de su formación académica y no dejen de asistir a clases. Por ello la importancia de que los establecimientos educativos en sus instalaciones tengan facilitadores y promuevan este tipo de justicia y resuelvan de mejor manera los conflictos suscitados en las comunidades de aprendizaje.

Para una buena convivencia educativa el código de convivencia debe cumplir con lo determinado en el Art. 64 de la Ley Orgánica de Educación Intercultural, ya que en él se plasman los acuerdos y compromisos que constituirán las directrices destinadas a regir a la comunidad educativa para garantizar los derechos de los estudiantes y la consolidación de un entorno seguro, saludable, de convivencia armónica, así como la cultura de paz propicia para el desarrollo integral.

Al ser un documento que forma parte del plan educativo institucional y contener directrices que rigen a la comunidad educativa, tiene una temporalidad específica de cuatro (4) años (MINEDU, 2020).

Este código de convivencia entre sus objetivos establece: Garantizar que la dinámica institucional se desarrolle en el marco del respeto de los derechos humanos de toda la comunidad educativa. • Promover la participación y corresponsabilidad de la población estudiantil, las familias, los profesionales de la educación y personal administrativo en la construcción de la convivencia armónica en cada una de las instituciones educativas. • Establecer medidas para la resolución alternativa de conflictos escolares, que respondan a la realidad de cada contexto. • Fortalecer el reconocimiento de que niños, niñas y adolescentes como sujetos de derechos y como agentes clave en la toma de decisiones sobre las situaciones que les afecta (MINEDU, 2020).

Este código debe realizarse cada 4 años como ya se lo indicó y siempre bajo la guía del gobierno escolar en articulación con los demás miembros del comité central colmena. Este organismo debe garantizar que en su construcción participen inspectores o la autoridad similar (dependiendo de la designación de autoridades con la que cuente la institución) y, de contar con el departamento de consejería estudiantil, que participe al menos un delegado de este organismo.

Con ello se colige que un debido proceso en armonía con el *corpus juris* de derechos de niñez y adolescencia y, enfocado en la justicia restaurativa juvenil evita someter a los adolescentes a procesos judiciales.

Finalmente, las instituciones educativas deben asegurar que los docentes asignados estén calificados para aplicar este tipo de procesos y programas dirigidos a restaurar el tejido social y resolver y mitigar los efectos negativos del crimen, con la participación de las partes en conflicto y las comunidades locales. Los procesos de justicia restaurativa se basan en la idea de que los crímenes y delitos no sólo violan la ley, sino que también dañan a las víctimas y a las comunidades, por lo tanto, el proceso de justicia restaurativa enfatiza la reconciliación, la identificación, el control, la reparación mutua y, por tanto, la reparación de las relaciones dañadas mediante el diálogo entre todas las partes en disputa.

Conclusiones

De lo analizado se colige que si bien es cierto las sociedades han ido evolucionando con las tecnologías de la información y la comunicación, también los niños, niñas y adolescentes son más propensos a que se violente su integridad personal y que sean víctimas del *sexting*, *grooming* y *sextorsión* por parte de sus pares o personas adultas (pederastas), debiendo los estados parte precautelar su integridad personal a través de políticas públicas.

Se concluye que las comunidades de aprendizaje y códigos de convivencia en los establecimientos educativos sirven para que de manera tripartita (alumnos, profesores y padres de familia) puedan coexistir de manera pacífica y armónica en distintos espacios, ya que concibe a la convivencia como el bienestar de la comunidad educativa que se expresa en un ambiente sano, equitativo, inclusivo, respetuoso y diverso; que favorece el ejercicio pleno de los derechos humanos individuales y colectivos.

En el presente análisis la Corte Constitucional en la Sentencia No. 456-20-JP/21 sobre la justicia restaurativa y el derecho al debido proceso en contextos educativos, insta a que en los planteles educativos primero se agote la justicia restaurativa a través de sus diferentes programas restaurativos, que como fin tienen reparar el daño causado y reconstruir el tejido social, a más de ello se evita la vulneración del interés superior del niño, debiendo siempre en todos los procesos administrativos y judiciales escuchar y tomar en cuenta la opinión del NNA, pues de esta manera se cumple con los estándares internaciones de protección de la niñez y adolescencia.

Referencias

Asamblea Constituyente del Ecuador. (2008, 20 de octubre). Constitución de la República del Ecuador. *Registro Oficial 449.*

Asamblea Nacional del Ecuador. (2011, 31 de marzo). Ley Orgánica de Educación Intercultural [LOEI]. *Registro Oficial 2S - 417.*

Asamblea Nacional del Ecuador. (2014, 10 de febrero). Código Orgánico Integral Penal. *Registro Oficial Suplemento 180.*

Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento [CIPPEC]. (s/f). *Comunidades de Aprendizaje*. https://www.cippec.org/proyecto/comunidades-de-aprendizaje/

Congreso Nacional del Ecuador. (2003, 3 de enero). Código de la Niñez y Adolescencia. *Registro Oficial 737.*

Corte Constitucional del Ecuador [CCE]. (2021, 10 de noviembre). *Sentencia N° 456-20-JP/21. Sobre La justicia restaurativa y el derecho al debido proceso en contextos educativos*. https://www.corteconstitucional.gob.ec/sentencia-456-20-jp-21/

Corte Constitucional del Ecuador [CCE]. (2021, 27 de enero). *Sentencia No. 2064-14-EP/21* sobre la acción de hábeas data planteada en contra de una persona natural que poseía fotografías íntimas y personales de la actora. https://www.corteconstitucional.gob.ec/sentencia-2064-14-ep-21/

Grupo Faro. (2022). Comunidades de aprendizaje. https://grupofaro.org/areas-de-trabajo/comunidades-de-aprendizaje/

Fajardo, M., Gordillo, M. y Regalado, A. (2013). *Sexting*: Nuevos Usos de la Tecnología y la Sexualidad en Adolescentes. *International Journal of Developmental and Educational Psychology*, 1(1), 521-534, ISSN 0214-9877.

Luna Scott, C. (2015, diciembre). *El futuro del aprendizaje 3. ¿Qué tipo de pedagogías se necesitan para el siglo XXI? Investigación y prospectiva en educación. Documentos de trabajo.* Organización de las Naciones Unidas para la Educación la Ciencia y la Cultura. https://n9.cl/mj2bh

Menjívar Ochoa, M. (2010). El *sexting* y l@s nativ@s neo-tecnológic@s: apuntes para una contextualización al inicio del siglo XXI. *Revista Electrónica del Instituto de Investigación en Educación de la Universidad de Costa Rica,* 10(2), 1-23, ISSN 1409-4703

Mercado, C., Pedraza, F. y Martínez, K. (2016). *Sexting*: su definición, factores de riesgo y consecuencias. *Revista sobre la infancia y la adolescencia.* 10(1), 1-18. http://dx.doi.org/10.4995/reinad.2016.3934

Ministerio de Educación (2014*) Protocolos de actuación frente a situaciones de violencia detectadas o cometidas en el sistema educativo*. https://educacion.gob.ec/wp-content/uploads/downloads/2017/03/Protocolos_violencia_web.pdf

Ministerio de Educación. (2020) *Manual de Prácticas Restaurativas en el ámbito educativo*. https://ecuador.vvob.org/sites/ecuador/files/2020_ecuador_eftp_manual_practicas_restaurativas.pdf

Ministerio de Educación (2022). *Construcción del Código de Convivencia.* https://educacion.gob.ec/wp-content/uploads/downloads/2022/10/4-Colmena-Codigo-de-Convivencia.pdf

Moreira, M., Maldonado, W. y García, A. (2019). Vulnerabilidades en el Uso de las Tecnologías de la Información: *Sexting* y *Grooming* en Adolescentes. *Revista Inclusiones*, 6 (núm. esp.), 85-98, ISSN 0719-4706

Ojeda, M., Del-Rey, R., Walrave, M., & Vandebosch, H. (06 de enero, 2020). *Sexting en adolescentes: Prevalencia y comportamientos*. Revista Comunicar, N° 64, 9-19. https://doi.org/10.3916/C64-2020-01

Organización de Naciones Unidas - Comité de los Derechos del Niño. (2009). *Observación general núm. 12. El derecho del niño a ser escuchado.*https://www.acnur.org/fileadmin/Documentos/BDL/2011/7532.pdf

Organización de Naciones Unidas - Comité de los Derechos del Niño. (2021). *Observación general núm. 25. Relativa a los derechos de los niños en relación con el entorno digital.* https://www.ohchr.org/es/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Oficina de Naciones Unidas contra la droga y el delito. (2006). *Manual sobre programas de Justicia Restaurativa.* https://www.unodc.org/documents/justice-and-prison-reform/Manual_sobre_programas_de_justicia_restaurativa.pdf

Pérez, P., Flores, J., de la Fuente, S., Álvarez, E., García, L., y Gutiérrez, C. (2011) Guía sobre adolescencia y *sexting*: qué es y cómo prevenirlo. *Observatorio de la Seguridad de la Información de INTECO y Pantallas Amigas.*

Peris Hernández, M., y Maganto Mateo, C. (2018). *Sexting, sextorsión y grooming: Identificación y prevención. Pirámide*

Presidencia de la República del Ecuador. (2023, 22 de febrero). Reglamento General a la Ley Orgánica de Educación Intercultural. *Registro Oficial 2S - 254.* https://www.derechopenalenlared.com/libros/sexting-sextorsion-y-grooming.pdf

Valls, R; Soler, M; y Flecha, R. (Enero – Abril- 2008). Lectura dialógica: interacciones que mejoran y aceleran la lectura. *Revista Iberoamericana de Educación. Nro. 46. OEI.* https://rieoei.org/historico/documentos/rie46a04.htm

Zehr, H (2007). *El pequeño libro de la Justicia Restaurativa*. Good Books - Intercourse https://www.icbf.gov.co/sites/default/files/el_pequeno_libro_de_las_justicia_restaurativa.pdf

3. La política pública por una Internet segura para niños, niñas y adolescentes

Mgtr. Andrea Aguirre
Mgtr. Jorge Luis Cueva
Mgtr. Sara Cabrera

3.1. Protección de datos personales y prevención de delitos

La Política pública por una internet segura para niños, niñas y adolescentes (2020) surge dentro de un marco de voluntad institucional como compromiso por parte del Estado ecuatoriano y con el objetivo de proteger a las niños, niñas y adolescentes, erradicando las distintas formas de violación de sus derechos en la Internet.

En su proceso de formación participaron la sociedad civil, empresas y organizaciones no gubernamentales; siendo responsables y corresponsables de la implementación de la misma dentro del marco de sus competencias y adecuándola a la realidad territorial y a los planes de desarrollo existentes. Adicional, se tomó en consideración las principales recomendaciones y observaciones del Informe del Comité de los Derechos del Niño emitido por las Naciones Unidas en el año 2017 y otros instrumentos e indicadores internacionales.

Al referirnos a los derechos de niños, niñas y adolescentes en el mundo digital, es importante señalar que se busca construir una sociedad de la información integradora y orientada al desarrollo, enfocada a crear, consultar y compartir la información y el conocimiento, tomando

como base los propósitos y principios de la Carta de Naciones Unidas y respetando y defendiendo la Declaración Universal de Derechos Humanos. (Consejo Nacional para la Igualdad Intergeneracional en el marco del Grupo de Trabajo Ampliado para la Protección Integral de Niñez y Adolescencia, 2020, p. 25).

Diversos estudios de Cepal, Fundación Telefónica y otros, establecen que en la región 4 de cada 10 niños, niñas y adolescentes utilizan la internet sin la compañía de un adulto (Pavez, 2014); es decir, no cuentan con un criterio formado ni control parental que podría disminuir el peligro y la vulnerabilidad de usuarios en la red.

Al referirse a este mismo aspecto, Víctor Giorgi, Director General del Instituto Interamericano del Niño, la Niña y Adolescentes (INN-OEA) establece que, en el caso de los niños, niñas y adolescentes, la Internet se convierte en un instrumento para el ejercicio de múltiples derechos; entre ellos, libertad de expresión y acceso a la información (INN-OEA y WVRD, 2018). Sin embargo, coexisten con riesgos y amenazas, enfrentándose a violencia digital a través de varios tipos de contenidos asociados con la explotación sexual comercial y no comercial.

Los niños, niñas y adolescentes tienen conocimiento de cierto tipo de delitos; entre ellos, los más conocidos son el ciberbullying y el sexting; sin embargo, existen otras conductas que se han trasladado al mundo virtual como: ciberacoso, *grooming,* pornografía infantil, *sextortion*, etc., e identificarlas resulta muy importante para poder enfrentarlas.

De acuerdo con la Organización de Estados Americanos los niños, niñas y adolescentes se enfrentan a las siguientes amenazas digitales:

Abuso sexual de niños, niñas y adolescentes en línea: hace referencia a todas las formas de abuso sexual facilitadas por las tecnologías de la información y/o difundidas por medios en línea, de conformidad a ECPAT - *End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes*. (ECPAT, 2016).

***Ciberbullying*/Ciberacoso:** acoso y agresión que se produce entre pares con la utilización de la internet, celular u otra tecnología y que tiene como intención propagar mensajes o imágenes crueles y que estos sean visualizados por varias personas (ECPAT, 2016).

Ciberadicción o Abuso del uso de la Internet / Tecnologías de la Información y las Comunicaciones (TIC): comportamiento compulsivo y excesivo relacionado con el uso de la Internet y las TIC´s, manifestándose de diversas maneras, que incluye la adicción a las redes sociales, los videojuegos en línea, la pornografía y el uso excesivo de dispositivos móviles que degeneran en una adicción con graves consecuencias físicas y psicológicas.

Chantaje sexual a niños, niñas y adolescentes/*Sextorsion:* consiste en amenazar con la difusión de imágenes o videos sexuales autogenerados por estos, con la intención de mantener relaciones sexuales o continuar con la explotación sexual (ECPAT, 2016).

Exposición a contenidos nocivos: se refiere al acceso o exposición de forma intencional o accidental, a contenido violento sexualizado o generador de odio que perjudica el desarrollo de estos (ECPAT, 2016).

Explotación sexual de niños, niñas y adolescentes en línea: incluye el uso de las TIC´s e Internet con la intención de producir,

difundir, comprar y vender imágenes o materiales que documentan la explotación sexual de niños, niñas y adolescentes (ECPAT, 2016).

***Flaming**:* envío de mensajes utilizando las diferentes redes sociales con lenguaje vulgar o violento y que tienen como finalidad humillar e intimidar (ECPAT, 2016).

Grooming es realizado por un adulto que busca estrategias con el objetivo de ganarse la confianza de un niño, niña o adolescente, utilizando las diferentes comunidades virtuales con el propósito de explotarlo sexualmente.

Es importante señalar que dependiendo de la forma en cómo se realiza existen dos tipos de *grooming*: 1.- El acosador busca ganarse la confianza del niño, niña o adolescente generando un vínculo personal con el propósito de lograr que los mismos, de forma voluntaria, entreguen material sexual para luego volverlo objeto de chantaje, amenazas, etc. 2.- No existe esta etapa previa de contacto que genere confianza, ni un vínculo personal entre el acosador con el niño, niña o adolescente; y, el adulto o acosador logra obtener fotos o videos sexuales con el objetivo de extorsionarlos con difundir este material a cambio de acceder a un encuentro personal.

Hipersexualización infantil: tendencia de sexualizar a los niños, niñas y adolescentes a través de actitudes, expresiones, códigos de vestimenta, etc, enfatizándose en el rol sexual del cuerpo a través de fotos o videos, generalmente publicados en las diferentes redes sociales o medios de comunicación. Como consecuencia, estas acciones provocan impacto en la autoimagen, problemas de salud mental, vulnerabilidad sexual y deterioro de la infancia.

Materiales de abuso sexual, de niños, niñas y adolescentes generados de forma digital: consiste en la producción de todo tipo de material digital que representa a niños, niñas y adolescentes participando en actividades sexuales creadas artificialmente aparentando que son reales (ECPAT, 2016).

Outing: revelar o hacer pública la homosexualidad de una persona sin su consentimiento, difundiendo o publicando mensajes o correos íntimos que podrían avergonzar a un niño, niña o adolescente.

Paliza Feliz: es una forma de ciberbullying que consiste en grabar con una cámara cuando una persona o grupo de personas golpean a la víctima, para posteriormente difundirlo en las redes sociales burlándose o ridiculizando.

Pornografía infantil: el Código Orgánico Integral Penal (2014) menciona que:

> La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años. (Art. 103)

Como circunstancia constitutiva del tipo penal la pena se agrava si la persona infractora se encuentra comprendida dentro de una categoría especial descrita en el mismo cuerpo normativo como: el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo

de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima.

Publicación de información privada: los niños, niñas y adolescentes publican información personal, por ejemplo, la dirección de su domicilio, número de contacto, etc. sin medir el peligro de esta en las diferentes redes sociales y exponiéndose así, a violencia digital o acoso de menores a través de las diferentes plataformas digitales.

Sexteo o *Sexting* se lo define como autoproducción de imágenes sexuales y su intercambio a través de teléfonos e Internet. En el caso de niños, niñas y adolescentes pueden encontrarse presionados a enviar una foto o video a un amigo, compañero o novio, quienes después difunden el contenido digital, sin previo consentimiento.

Streaming trasmisión en vivo relacionada a una conducta nociva y criminal, refiriéndose a prácticas de abuso sexual contra niños, niñas y adolescentes a través de la prostitución, espectáculos pornográficos o elaboración de material de carácter pornográfico que son transmitidas en vivo (ECPAT, 2016).

En la actualidad, los niños, niñas y adolescentes no conocen un mundo sin la Internet y tecnologías en línea; de allí la necesidad de promover y proteger sus derechos en los entornos virtuales y digitales.

De conformidad a lo dispuesto en la Coalición Dinámica por los Derechos y Principios de la Internet, en el 2015, los derechos humanos son aplicables y exigibles en el mundo digital con la misma fuerza e intensidad que el mundo real; y, esto obliga a los Estados a garantizar la protección contra los abusos a través de la Internet y las

nuevas tecnologías; por ello, a escala mundial se destacan como buenas prácticas tres elementos importantes en lo que se debe trabajar: 1) inclusión digital y acceso a la Internet, 2) programas y campañas que promuevan su acceso y uso; y, 3) la existencia y aplicación de normativa para protección de los derechos de niños, niñas y adolescentes.

Con base a lo expuesto, nuestro país fomenta un marco normativo y regulatorio a través de la Política pública por una internet segura para niños niñas y adolescentes que busca potenciar las oportunidades y habilidades que ofrecen las tecnologías digitales y promover el aprovechamiento de los usos y beneficios de las TIC, estableciendo conductas protectoras para prevenir factores de riesgos que pueden poner en peligro la vida e integridad de niños, niñas y adolescentes.

3.2 Ejes de la política pública por una internet segura para niños, niñas y adolescentes

La Internet es una herramienta tecnológica fundamental para el desarrollo de la sociedad, convirtiéndose en el medio generador de oportunidades de aprendizaje, trabajo, relaciones sociales, desarrollo industrial, etc, considerándose como un pilar fundamental para impulsar el ejercicio de derechos de las personas.

Al tiempo que la Internet otorga innumerables beneficios, existen usuarios que se han convertido en víctimas de usuarios de la web, y para nuestro análisis nos enfocaremos en el grupo vulnerable de niños, niñas y adolescentes, quienes en la actualidad mantienen una conexión con la web, con escaso o nulo control parental, convirtiéndose en una conexión libre y vulnerable.

Es ilógico pretender desconectar de la internet a los niños, niñas y adolescentes, pero su conexión debe guardar relación con medidas de control, como un método preventivo para evitar futuras afectaciones informáticas o digitales.

El Estado, principalmente, es el obligado a reconocer, precautelar y garantizar los derechos de los niños, niñas y adolescentes en un mundo virtual lleno de información positiva y negativa, sin dejar de lado la corresponsabilidad de la familia y sociedad para lograr extraer de la web los mayores beneficios para un óptimo desarrollo integral del ser humano y proteger su honra y dignidad.

Para prevenir, combatir y erradicar presentes y futuros riesgos digitales, la política pública contiene 5 ejes esenciales, tales como:

Eje 1: Medidas legales para garantizar los derechos digitales.

Su objetivo se encuentra enfocado en:

> Desarrollar normativa que promueva los derechos digitales y la dignidad e integridad física, psicológica, emocional y sexual de niñas, niños y adolescentes, estableciendo los mecanismos para el aprovechamiento de los beneficios de las tecnologías de la información y la comunicación, y atienda y mitigue los riesgos y delitos que pueden cometerse a través de ellas. (Consejo Nacional para la Igualdad Intergeneracional en el marco del Grupo de Trabajo Ampliado para la Protección Integral de Niñez y Adolescencia, 2020, p. 35).

El enfoque del primer eje se concentra en fortalecer el ordenamiento jurídico ecuatoriano con la finalidad de otorgar mayor protección a los niños, niñas y adolescentes frente a la conexión digital.

Siendo emergente una reforma al Código Orgánico de la Niñez y Adolescencia, para incluir norma regulatoria relacionada a derechos digitales, ciudadanía digital, medidas de protección y reparación. Posteriormente, se debe regular la tipificación y medidas sancionatorias frente al cometimiento de delitos informáticos que tengan como víctimas a niños, niñas y adolescentes.

Paralelamente, es necesario la regulación de prestación de servicios de internet, buscando la implementación de herramientas tecnológicas para un acceso sano, educativo y libre de violencia. Regulación que se extiende a los proveedores de servicio de internet y espacios que ofrecen acceso a internet.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) de Ecuador es el órgano rector encargado de desarrollar políticas y regulaciones en el ámbito de las telecomunicaciones y la sociedad de la información. Su objetivo es garantizar que los proveedores de servicios de telecomunicaciones ofrezcan herramientas que protejan los derechos de niños, niñas y adolescentes. Para lograr esto, el MINTEL trabajará en conjunto con otras entidades como el Ministerio de Inclusión Económica y Social, la Dirección Nacional de Registro de Datos Públicos y la Agencia de Regulación y Control de las Telecomunicaciones. Este esfuerzo colaborativo se enfoca en analizar e identificar necesidades de regulación, elaborar y proponer normativas, y realizar el seguimiento necesario para asegurar su correcta implementación.

Aún con la aplicación de medidas preventivas, los delitos informáticos seguirán existiendo, por tanto, es importante que existan procesos para acceder a las estadísticas de este tipo de delitos, protegiendo la identidad de las víctimas, lo que permitirá la futura toma de decisiones, correctivos y posibles regulaciones normativas. Para lograr este objetivo, el Consejo de la Judicatura es la entidad pública que actúa como líder para la implementación de procesos que permitan el cruce de información entre las instituciones que forman parte de la Función Judicial, para el levantamiento de estadísticas relacionadas a causas de delitos cibernéticos que afectan a niños, niñas y adolescentes. Po tanto, la formación de base de datos deberá ser anonimizada para garantizar la protección de datos personales de las víctimas.

Eje 2: Medidas técnicas y procedimentales:

El presente eje tiene como objetivo, "Promover el acceso, uso e interacción adecuada, responsable, sana, segura y constructiva de las tecnologías de la información y las comunicaciones que impulse el desarrollo integral y el pleno ejercicio de los derechos de niñas, niños y adolescentes." (Consejo Nacional para la Igualdad Intergeneracional en el marco del Grupo de Trabajo Ampliado para la Protección Integral de Niñez y Adolescencia, 2020, p. 36).

Al tratarse de un objetivo amplio, requiere de la división de lineamientos con sus acciones específicas.

El primer lineamiento busca promover el acceso a las tecnologías de la información y comunicación, de una forma segura, evitando que los niños, niñas y adolescentes tengan contacto con información calificada como nociva y que pueda atentar contra su integridad y dignidad. Para el cumplimiento del primer lineamiento se propone la creación

e implementación de diversas acciones, como la creación de políticas públicas desde las instituciones estatales, conducentes a garantizar el acceso a las tecnologías de una forma segura y en beneficio de los usuarios; de la misma forma, las políticas públicas se deben impulsar desde los Gobiernos Autónomos Descentralizados las cuales buscan el similar ámbito de protección, pero, especialmente debe regular los requerimientos que debe cumplir un local comercial de acceso a las tecnologías (información y comunicación), previo a la emisión de las autorizaciones para su funcionamiento. Por otro lado, es fundamental la implementación de lineamientos y procedimientos para regular el acceso a contenido que atente contra los derechos de los niños, niñas y adolescentes; y, con la finalidad de registrar precedentes judiciales, es importante la creación de un medio para denunciar los contenidos ilegales, lo cual servirá para que la instancia correspondiente realice la investigación pertinente hasta obtener la aplicación de una sanción y eliminación de contenido digital perjudicial.

El segundo lineamiento, se concentra en convertir a las instituciones públicas, privadas y comunitarias en actores clave para la protección de los niños, niñas y adolescentes frente a contenido virtual que atente a los derechos fundamentales del ser humano. Fortaleciendo las instituciones, para combatir el contenido digital ilegal, mediante la aplicación de protocolos que permitan ejecutar una denuncia efectiva, con un seguimiento eficaz hasta la aplicación de una sanción.

El trabajo importante es prevenir y no llegar hasta un proceso judicial, por tanto, el lineamiento pretende la creación de un portal web en el cual se refleje información, herramientas, vídeos, tutoriales, manuales, etc., para que los usuarios de la web conozcan anticipadamente, la forma de actuar para prevenir ser víctima de contenidos nocivos o

usuarios que actúan fuera del margen de la ley. Finalmente, el segundo lineamiento a más de fortalecer a las instituciones, también se concentra en convertir a los niños, niñas y adolescentes en actores clave para la toma de decisiones y evaluación de las acciones implementadas.

Eje 3: Construcción de estructuras organizacionales de seguimiento y control / Cooperación internacional.

El tercer eje se plantea dos objetivos, el primero enfocado en "Coordinar, dar seguimiento, monitorear y evaluar el cumplimiento de lo estipulado en el plan de política pública por el uso seguro de internet." (Consejo Nacional para la Igualdad Intergeneracional en el marco del Grupo de Trabajo Ampliado para la Protección Integral de Niñez y Adolescencia, 2020, p. 38).

Para el cumplimiento de este objetivo, la evaluación de acciones ejecutadas debe ser analizada mediante la implementación de una mesa técnica interinstitucional, lo cual beneficiará para verificar si las decisiones adoptadas han sido eficaces o requieren de una modificación, para obtener un mayor impacto de protección. Además, los resultados de la evaluación deberán ser comunicados a las entidades gubernamentales, la sociedad e instancias internacionales, permitiendo obtener el apoyo de nuevos aliados y estrategias que pueden fortalecer la política pública para una internet segura.

El segundo objetivo del tercer eje se enfoca en "Establecer acuerdos, tratados o convenios internacionales multilaterales jurídicamente vinculantes u oficiosos de cooperación técnica y económica en materia de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia." (Consejo Nacional para la Igualdad Intergeneracional en

el marco del Grupo de Trabajo Ampliado para la Protección Integral de Niñez y Adolescencia, 2020, p. 38).

La información digital no es un tema que afecte solamente a un determinado país, por tanto, la internet es una herramienta transfronteriza que puede atentar contra los derechos humanos a nivel mundial, por ello, la promoción de un proceso regional permitirá la regulación jurídica y acuerdos internacionales para la erradicación de la violencia digital. Además, el análisis de casuística internacional facilitará la toma de decisiones y regulación mediante políticas públicas.

Las acciones de mayor relevancia que requieren ejecución urgente es la adhesión del Estado Ecuatoriano al Convenio de Budapest sobre la ciberdelincuencia; y, la obtención de recursos económicos para el financiamiento de proyectos enfocados a la protección de los niños, niñas y adolescentes frente a una internet segura.

Eje 4: Construcción y fortalecimiento de capacidades.

El cuarto eje tiene como objetivo:

> Promover una cultura preventiva para el uso seguro de internet y tecnologías digitales que oriente a los miembros de la comunidad educativa acerca de los beneficios y riesgos, así como desarrolle competencias y habilidades digitales básicas que contribuyen a su desarrollo humano. (Consejo Nacional para la Igualdad Intergeneracional en el marco del Grupo de Trabajo Ampliado para la Protección Integral de Niñez y Adolescencia, 2020, p. 39).

Objetivo direccionado a fortalecer las capacidades del Sistema Nacional de Educación, mediante un diagnóstico sobre las actuales

medidas de protección con que cuentan los niños, niñas y adolescentes en su proceso educativo, en la interacción con la web, y, de conformidad a los resultados obtenidos se elaborará e implementará la Agenda Educativa Digital 2030. Además, se reconoce la importancia de mantener capacitaciones permanentes en beneficio de los docentes sobre el manejo de las tecnologías de la información y comunicación, para que sean el primer asesor y contacto de los niños, niñas y adolescentes víctimas del contenido digital.

Al mismo tiempo, este objetivo se plantea el reto de comunicar e informar en las comunidades educativas y en la sociedad en general, los derechos, obligaciones y responsabilidades existentes al momento de hacer uso de las tecnologías digitales. Los medios de comunicación que serán las herramientas para la difusión serán públicos y privados, con la finalidad de tener un mayor alcance e impacto en la sociedad. Una herramienta fundamental que se encuentra en funcionamiento es la página *web internetsegura*, su construcción ha sido impulsada por la Dirección Nacional de Registro de Datos Públicos con el apoyo de instituciones públicas y privadas, página que contiene información dirigida para niños, niñas y adolescentes, padres y madres de familia, y docentes, con la finalidad de formar a la sociedad sobre la prevención de los delitos informáticos.

La Dirección Nacional de Registro de Datos Públicos, con el apoyo de diversas instituciones públicas y privadas, ha desarrollado la página web www.internetsegura.gob.ec. Este sitio ofrece recursos y herramientas dirigidas a niñas, niños, adolescentes, padres, madres, y docentes, con el objetivo de garantizar los derechos digitales de los menores y promover el uso seguro de internet.

Eje 5: Construcción y fortalecimiento de capacidades.

El quinto eje tiene como objetivo, "Desarrollar una estrategia comunicacional para promover los derechos digitales y un uso seguro de la internet por parte de niñas, niños y adolescentes." (Consejo Nacional para la Igualdad Intergeneracional en el marco del Grupo de Trabajo Ampliado para la Protección Integral de Niñez y Adolescencia, 2020, p. 40).

Para el cumplimento del objetivo las acciones a desarrollarse son el promover una cultura de protección integral en el ámbito de la información digital, mediante el apoyo de diversas instituciones para la difusión de mensajes relacionados a la política pública para una internet segura. Además, para obtener una mayor difusión, las redes sociales funcionarán como un medio idóneo para conectarse con los niños, niñas y adolescentes, debido a que son la mayor parte de la comunidad que permanecen conectados a la web. Las campañas de difusión de mensajes preventivos y de contenido de la política antes mencionada, permitirá la erradicación de contenido digital nocivo y posteriormente se podrá realizar un análisis sobre el impacto provocado en diversos medios de comunicación digital, tales como tv, radio, redes sociales, entre otros de similar característica.

3.3 Manual de buenas prácticas y de prevención del ciberacoso

Códigos de Convivencia del Ministerio de Educación

El Ministerio de Educación del Ecuador, como parte de su misión, garantiza a los habitantes del territorio nacional el acceso y calidad de la educación en el área inicial, básica y bachillerato, a través de la

formación integral, holística e inclusiva para así fortalecer el desarrollo social, económico y cultural.

Bajo este contexto, esta Ministerio fomenta varias acciones en diversos aspectos de la educación, entre los cuales, se ubica el ámbito de la convivencia armónica y respetuosa dentro de una comunidad educativa; aspecto que constituye un elemento indispensable para el desarrollo integral de los individuos y progreso de la sociedad.

El Ministerio de Educación, mediate el Código de Convivencia (2022) expresa que, **la convivencia** representa el bienestar de la comunidad educativa, la misma que debe manifestarse en un ambiente sano, equitativo, inclusivo, respetuoso y diverso; a fin de favorecer el ejercicio pleno de los derechos humanos individuales y colectivos. (p. 4 - 5)

Con este fin, en el Ecuador se implementa en las instituciones educativas el código de convivencia, (vigente por cuatro años) de acuerdo con el artículo 89 del Reglamento General a la Ley Orgánica de Educación Intercultural (2023) se define como:

> el documento público construido por los actores que conforman la comunidad educativa. En este se deben detallar los principios, objetivos y políticas institucionales **que regulen las relaciones entre los miembros de la comunidad educativa;** para ello, se deben definir métodos y procedimientos dirigidos a producir, en el marco de un proceso democrático, las acciones indispensables para lograr los fines propios de cada institución.
>
> Participan en la construcción del Código de Convivencia los siguientes miembros de la comunidad educativa: 1. El Rector,

director o líder del establecimiento; 2. Las demás autoridades de la institución educativa, si las hubiere; 3. Tres (3) docentes delegados por la Junta General de Directivos y Docentes; 4. Dos (2) delegados de los Padres y Madres de Familia; y, 5. El presidente del Consejo Estudiantil.

La responsabilidad de la aplicación del Código de Convivencia le corresponde al equipo directivo en estricto respeto de la legislación vigente. Este documento debe entrar en vigor, una vez que haya sido ratificado por el Nivel Distrital, de conformidad con la normativa específica que para el efecto expida el Nivel Central de la Autoridad Educativa Nacional. (p. 30)

Se deduce entonces que el código de convivencia representa un instrumento que permite a los centros educativos orientar los procedimientos regulatorios que rigen la vida de la comunidad educativa. Su elaboración requiere la participación activa de todos sus integrantes: autoridades educativas, personal docente y administrativo, alumnos y padres de familia.

También es preciso manifestar que este instrumento evidencia la misión, visión y valores instituciones considerando los derechos de niños, niñas y adolescentes y del resto de miembros de la comunidad educativa.

¿Cuál es el objetivo de un código de convivencia?

Con base en la definición antes descrita y una breve contextualización de lo que representa un código de convivencia, seguro

se podrá identificar sus objetivos, por ello, se precisa citar lo mencionado por el Ministerio de Educación – Código de Convivencia (2022):

- Garantizar que la **dinámica institucional** se desarrolle en el marco del respeto de los derechos humanos de toda la comunidad educativa.
- **Promover la participación** y corresponsabilidad de la población estudiantil, las familias, los profesionales de la educación y personal administrativo en la construcción de la en cada una de las instituciones educativas.
- Establecer **medidas para la resolución alternativa de conflictos escolares** , que respondan a la realidad de cada contexto.
- Fortalecer el **reconocimiento** de que niños, niñas y adolescentes como sujetos de **derechos** y como agentes clave en la toma de decisiones sobre las situaciones que les afecta. (p.7)

¿Cuáles son las características del Código de Convivencia?

Tomando en consideración que este instrumento rige para todos quienes conforman la comunidad educativa, es necesario que este reúna ciertas características, tales como comprensible, de fácil acceso, pertinente, contextualizado, aplicable, consensuado, integrador, restaurativo, preventivo y flexible.

Es importante destacar la pertinencia, pues esta se relaciona con el contexto social para el cual rige el instrumento, es decir, mirar la realidad en la que se desenvuelve la comunidad educativa; para ello, se contempla el desarrollo de un diagnóstico institucional donde se identifica las necesidades referentes a los criterios de convivencia siguientes:

- Vida en comunidad,
- Relaciones con el entorno física y ambiental,
- Actuación en la dinámica educativa e institucional; y,
- Estilo de vida.

En relación con la flexibilidad, esta característica se refiere a los cambios y requerimientos por parte de la comunidad educativa y a los cuales debe ajustarse el código de convivencia; consensuado y de fácil acceso, por las partes educativas a través de diversas estrategias de socialización; preventivo, al establecer mecanismos para la gestión pacífica de desacuerdos; y, restaurativo, al aplicar metodologías que conlleven a la reparación y bienestar de la comunidad educativa.

Precisando un poco más sobre la característica de restaurativo, es necesario manifestar que la resolución de los conflictos surgidos en una comunidad de aprendizaje debe contar con la participación de todos sus miembros. Para ello, conviene aplicar una metodología denominada justicia restaurativa considerada también por otros autores como una filosofía, la misma que tiene como objetivo reparar los daños causados y mitigar sus consecuencias.

Por otra parte, cabe recalcar que el Ministerio de Educación y Cultura aplica el Manual de Prácticas Restaurativas en el ámbito educativo, con el propósito de brindar a los profesionales que se ven inmersos en la educación, una herramienta teórico-práctica que les permita promover e implementar de manera efectiva y continua su rol desde una filosofía restaurativa. En este manual se exponen varias definiciones de justicia restaurativa, una de ellas, cita lo expresado por las Naciones Unidas, en el año 2006:

> una metodología para solucionar problemas que involucra a la persona víctima, a la persona ofensora, a las redes sociales, las instituciones judiciales y la comunidad. La considera como un proceso para resolver el problema de la delincuencia enfocándose en la comprensión del daño a las víctimas, haciendo a las personas agresoras responsables de sus acciones. (Como se citó en VVOB educación para el desarrollo, 2020, p.21)

Sumado a ello, se ubica también el Acuerdo Ministerial 0434-12 del MINEDUC que establece:

Art. 3. Principio.- las alternativas de solución de conflictos y las acciones educativas disciplinarias, deben ser aplicadas como parte de la formación integral del estudiante, que contribuya al pleno desarrollo de su personalidad, capacidades y potencialidades, respetando sus derechos y libertades fundamentales y promoviendo las construcción de una cultura de paz y no violencia entre las personas y la convivencia pacífica y armónica entre los miembros de la comunidad educativa.

Art. 5. Prevención de conflictos.- Para prevenir la generación de situaciones conflictivas entre los estudiantes y de éstos con el resto de actores de la comunidad educativa, la institución educativa debe ejecutar las siguientes acciones:

a. Incorporar en el Proyecto Educativo Institucional, el enfoque transversal de la solución pacífica de conflictos.

b. Incluir en la planificación, como parte de la asignatura "Educación para la ciudadanía", horas pedagógicas y actividades fuera de clase en las que se promueva la prevención y solución pacífica de conflictos;

c. Difundir entre los miembros de la comunidad educativa el Código de Convivencia;

d. Capacitar a los docentes en la detección y manejo de conflictos;

e. Impartir charlas y conferencias, dirigidas a los representantes de los estudiantes; y,

f. Definir la intervención del departamento de Consejería Estudiantil. (2012, pp. 2-3)

¿Qué elementos debe considerarse para el desarrollo del código de convivencia?

El Reglamento General a la Ley Orgánica de Educación Intercultural (2023), Art. 90 manifiesta que el código de convivencia debe observar y cumplir obligatoriamente los siguientes preceptos:

- Desarrollo de valores éticos integrales y de respeto a la diferencia y a la identidad cultural de cada persona y colectivo, como fundamentos de una convivencia sana, solidaria, equitativa, justa, incluyente, participativa e integradora, para el desarrollo intercultural del tejido social;
- Respeto a la dignidad humana, a la honra y los derechos de las personas, a las libertades ciudadanas, a la igualdad de todos los seres humanos dentro de la diversidad, al libre desarrollo de la personalidad y al derecho de ser diferente;

- Promoción de la cultura de paz y de no agresión entre todos los miembros de la comunidad educativa y de la comunidad en general;
- Consolidación de una política institucional educativa de convivencia basada en derechos, valores, disciplina, razonabilidad, justicia, pluralismo, solidaridad y relación intercultural;
- Legitimación del quehacer educativo del plantel a través de un sistema de diálogo, discusión democrática y consensos; de reconocimiento y respeto a los disensos; y de participación activa de los miembros de su comunidad educativa;
- Integración, sin ningún tipo o forma de discriminación o inequidad, de todos los miembros de la comunidad de la institución educativa como factor clave para el mejoramiento continuo y progresivo de los procesos de enseñanza, aprendizaje e interaprendizaje;
- Legitimación de los procedimientos regulatorios internos del plantel a través de procesos participativos, equitativos e incluyentes;
- Precautela de la integridad de cada una de las personas que hacen parte de la institución y de la comunidad educativa, así como de los bienes, recursos, valores culturales y patrimoniales del plantel; y,
- Promoción de la resolución alternativa de conflictos. (p. 31)

Otros elementos que requieren considerarse al momento de diseñar un código de convivencia, son los principios y enfoques

establecidos en la Ley Orgánica de Educación Intercultural, los mismos que se ubican en los artículos 2.3 y 2.5 y que se aprecian a continuación:

Principio y enfoque	Imagen o audio	Descripción
Cultura de paz y solución de conflictos		El ejercicio del derecho a la educación debe orientarse a construir una sociedad justa, una cultura de paz y no violencia para la prevención, tratamiento y resolución pacífica de conflictos en todos los espacios de la vida personal, escolar, familiar y social. Se exceptúan todas aquellas acciones y omisiones sujetas a la normativa penal y a las materias no transigibles de conformidad con la Constitución.
Integridad		Reconoce y promueve la relación entre cognición, reflexión, emoción, valoración, actuación y el lugar fundamental del diálogo, el trabajo con los otros, la disensión y el acuerdo como espacios para el sano crecimiento en interacción de estas dimensiones.

Convivencia armónica		La educación tendrá como principio rector la formulación de acuerdos de convivencia armónica entre los actores de la comunidad educativa.
Igualdad de género		La educación debe garantizar la igualdad de condiciones, oportunidades y trato entre hombres y mujeres promoviendo una educación libre de violencias.
Derechos humanos		Pone como centro al ser humano, tanto en su dimensión individual como social. La educación es un derecho que permite desarrollar otros tipos de derechos para alcanzar una vida digna.
Intergeneracional		La educación a lo largo de la vida determina la necesidad de establecer un diálogo entre grupos de personas de diferentes edades pero que ejercen roles comunes.

Plurinacionalidad		Consiste en el reconocimiento de las formas tradicionales y costumbres de las comunas, comunidades, pueblos y nacionalidades en el Sistema Nacional de Educación.
Género		Considera las diferentes oportunidades que tienen los hombres y las mujeres, sin discriminación por razones de orientaciones sexual o identidad de género, las interrelaciones existentes entre ellos y los distintos papeles que socialmente se les asignan. Las relaciones de género desiguales derivan de los modos en que las culturas asignan las funciones y responsabilidades distintas a la mujer y el hombre. Ello a la vez determina diversas formas de acceder a los recursos materiales y no materiales. El enfoque de género permite analizar esas formas, con el fin de eliminar las barreras que limitan a las personas en razón de su identidad de género u orientación sexual.

Nota: Ley Orgánica de Educación Intercultural (artículos 2.3 y 2.5)

La ejecución y seguimiento de lo establecido a través del código de convivencia está a cargo de la comunidad educativa, ejerciendo la veeduría para que se cumplan los deberes y derechos de la población estudiantil.

En conclusión, en el Ecuador, la implementación efectiva de los códigos de convivencia en las instituciones educativas desempeña un papel crucial en la formación de ciudadanos comprometidos, éticos y socialmente responsables. Es así que los códigos de convivencia en la comunidad educativa ecuatoriana, destacan su rol en la promoción de valores, la prevención de conflictos y, la construcción de un ambiente propicio para el aprendizaje.

Referencias

Asamblea Nacional de Ecuador. (2011). Ley Orgánica de Educación Intercultural. *Registro Oficial del Gobierno del Ecuador* N° 417

Asamblea Nacional de Ecuador. (2023). Reglamento General a la Ley Orgánica de Educación Intercultural. *Registro Oficial del Gobierno del Ecuador* N° 254

Asamblea Nacional de Ecuador. (2014). Código Orgánico Integral Penal. *Registro Oficial del Gobierno del Ecuador* N° 80

Consejo Nacional para la Igualdad Intergeneracional. (2020). *Política Pública por una Internet Segura para Niños, Niñas y Adolescentes.* https://n9.cl/flodl

ECPAT. (2016). Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexual. ECPAT International.

IIN-OEA . WVRD. (2018). Red Intergeneracional para la Promoción del Uso Seguro de Internet - RIAMUSI. *Una mirada a la situación actual y una propuesta metodológica*. World Visión República Dominicana, Instituto Interamericano del Niño, la Niña y Adolescentes.

Schmitz, J. (s.f.). Manual de Prácticas Restaurativas en el ámbito educativo. *Ministerio de Educación.* https://ecuador.vvob.org/sites/ecuador/files/2020_ecuador_eftp_manual_practicas_restaurativas.pdf

Ministerio de Educación. (2022). Construcción del Código de Convivencia. *Ministerio de Educación*. https://educacion.gob.ec/wp-content/uploads/downloads/2022/10/4-Colmena-Codigo-de-Convivencia.pdf

Ministerio de Educación. (s.f.). Visión, Misión, Valores. *Ministerio de Educación.* https://educacion.gob.ec/valores-mision-vision/

Ministerio de Educación. (2012). Acuerdo Ministerial 0434-12. *Normativa sobre solución de conflictos en las instituciones educativas.* https://educacion.gob.ec/wp-content/uploads/downloads/2012/10/ACUERDO-434-12.pdf

Pavez, M. (2014). Los derechos de la infancia en la era de Internet: América Latina y las nuevas tecnologías. Naciones Unidas.

4. Acciones y estrategias para la prevención del ciberacoso

PhD. Luis Ordóñez
PhD. Lucia Puertas

En el marco del proyecto articulado "Ciberacoso en las comunidades de aprendizaje", el Grupo de Investigación "Derechos Digitales y Protección de Datos Personales" ha trazado que, desde la perspectiva de la investigación, un objetivo es articular un modelo de cultura digital para la protección de los menores; y, que, a partir de un enfoque de vinculación con la comunidad, otro objetivo trascendental es conocer las acciones de las instituciones educativas, frente al ciberacoso.

La construcción de una cultura digital en entornos digitales es primordial "para los fines de proteger el derecho a la autodeterminación informativa desde una perspectiva integral y global que, lógicamente, responda a los riesgos que plantean las Tics" (Ordóñez Pineda, 2018, p. 391). Lógicamente, este propósito tiene una especial connotación en las instituciones educativas, por cuanto, en éstas se podrían promover "mecanismos de control y prevención precisados en un modelo de cultura digital, respecto a los riesgos que representan sufrir amenazas, intimidación, extorsión y discriminación como resultado de la sobrexposición de información personal en entornos digitales" (Ordóñez Pineda, 2018, p. 390).

Esta propuesta que hemos desarrollado en otro momento se ha puesto de manifiesto en el ordenamiento jurídico ecuatoriano, mediante el reconocimiento del denominado derecho a la educación digital en

la Ley Orgánica de Protección de Datos Personales, el cual plantea la promoción de una cultura sensibilizada del derecho a la protección de datos personales, a través, de acciones y estrategias relacionadas con "el uso y manejo adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad" (LOPDE, 2021). En todo caso, también, desde el ámbito de las políticas públicas de Ecuador, este planteamiento trasciende en la Política Pública por una internet segura para niños, niñas y adolescentes, en donde se reconoce que se debe "promover una cultura preventiva para el uso seguro de la internet y las tecnologías digitales, así como el adecuado seguimiento y sanción en caso de vulneraciones de derechos" (CNII, 2021, p. 6).

Desde esta perspectiva, entendemos que la doctrina, legislación nacional e instrumentos internacionales –vinculantes o no– plantean una serie de presupuestos que, a la vez, se traducen en acciones y estrategias para la prevención del acoso de los menores, en el ámbito digital. Por tanto, a la luz de dichas prescripciones, pretendemos subrayar la importancia de "un deber preventivo (formación) y un deber reactivo (actuación en caso de ataques por parte de terceros). Ambos deberes han de estar en el justo equilibro en la balanza con los derechos de los menores de protección de datos" (Davara Fernández, 2017, p. 72).

Precisamente, un instrumento no vinculante que aclara este ámbito es el Memorándum de Montevideo (2009), el cual advierte que "es prioritaria la prevención, —sin dejar de lado un enfoque de políticas, normativo y judicial— para enfrentar los aspectos identificados como riesgosos de la Sociedad de la Información y Conocimiento, en especial del Internet y las redes sociales digitales". En efecto, un aspecto riesgoso,

especialmente, en Internet y plataformas digitales es el ciberacoso, el cual "suele tener lugar en entornos escolares —colegios, institutos, escuelas de formación profesional— y deja una huella psicológica en la víctima. En esta situación, hay un menor que actúa como víctima y uno —o varios— menores que actúan como verdugos" (Davara Fernández, 2017, p. 50).

Bajo estas consideraciones, a continuación, planteamos las siguientes acciones y estrategias, tendentes a identificar un modelo de prevención que haga frente el acoso en entornos digitales. Naturalmente, siguiendo las recomendaciones del Memorándum de Montevideo (2009), este propósito estará conectado con "la educación, considerando la participación activa de los propios niños, niñas y adolescentes, los progenitores u otras personas a cargo de su cuidado y los educadores, tomando en consideración como principio fundamental el interés superior de niñas, niños y adolescentes".

4.1. Acciones

La Agencia Española de Protección de Datos Personales (2022) define el ciberacoso como "la utilización de redes de comunicaciones (internet, telefonía móvil, videojuegos online, etc.) para humillar, vejar, difamar o acosar a otras personas. Se trata de un acoso entre iguales y, en general, reviste especial gravedad cuando se produce entre jóvenes y adolescentes, habiéndose llegado a dar casos de suicidio por esta causa". Frente a esta realidad que plantea el escenario de modernidad de las tecnologías, en principio, podría parecer complejo proponer medidas que, desde el Estado, la sociedad y la familia, se destinen a prevenir esta nueva forma de acoso.

Reconociendo que muchas conductas que se desprenden del ciberacoso tienen como punto partida el uso ilegítimo de los datos personales, es evidente la necesidad de buscar un equilibrio global, que garantice la protección integral de la información personal de los menores en el mundo digital, "desde un enfoque de derechos, especialmente en el derecho a la autodeterminación informativa, a la identidad y reputación digitales, así como a la responsabilidad de uso de redes sociales" (CNII, 2021, p. 33). En todo caso, subrayando que la responsabilidad de cuidar los propios datos personales es un presupuesto que, no solamente obliga a terceras personas sino también a los propios titulares de los datos; al parecer la clave de dichas medidas o acciones estaría en la instrucción y enseñanza (educación) sobre el valor y la importancia de proteger los datos personales. Por ello, agregamos que "los esfuerzos deben estar dirigidos a la sensibilización, capacitación y concientización sobre los peligros para la dignidad e integridad de nuestros niños y adolescentes" (CNII, 2021, p. 33).

En estos términos, el Memorándum de Montevideo (2009) describe una serie de acciones que las detallamos de la siguiente manera:

1. Los Estados y las entidades educativas deben **tener en cuenta el rol de los progenitores,** o cualquier otra persona que tenga bajo su responsabilidad el cuidado de las niñas, niños y adolescentes, en la formación personal de ellos, que incluye el uso responsable y seguro del Internet y las redes sociales digitales.

   Es tarea del Estado y las entidades educativas proveer información y fortalecer capacidades de los progenitores y personas responsables, sobre los eventuales riesgos a

los que se enfrentan las niñas, niños y adolescentes en los ambientes digitales.

2. Toda medida que implique **control de las comunicaciones tiene que respetar el principio de proporcionalidad.**

   Se debe determinar que la misma tiene como fin la protección y garantía de derechos que es adecuada al fin perseguido y que no existe otra medida que permite obtener los mismos resultados y sea menos restrictiva de los derechos.

3. Transmitir claramente a las niñas, niños y adolescentes que **Internet no es un espacio sin normas,** impune o sin responsabilidades.

   Deben alertarlos para no dejarse engañar con la aparente sensación de que allí todo vale dado que todas las acciones tienen consecuencias.
   Educación en el uso responsable y seguro de Internet y las redes sociales digitales. En particular:

3.1 La es posible en las redes sociales digitales. El proceso educativo debe reflexionar sobre los aspectos positivos del uso de pseudónimos como medio de protección y un uso responsable que —entre otras cosas— implica no utilizarlos para engañar o confundir a otros sobre su identidad real.

   Las niñas, niños y adolescentes deben ser advertidos sobre la posibilidad de que cuando creen estar comunicándose o compartiendo información con una persona determinada, en realidad puede tratarse de otra persona. Al mismo

tiempo es necesario advertir que la participación anónima o con un pseudónimo hace posible la suplantación de identidad.

3.2 En el proceso educativo es necesario **enfatizar el respeto a la vida privada, intimidad y buen nombre de terceras personas, entre otros temas.**

Es importante que las niñas, niños y adolescentes sepan que aquello que puedan divulgar puede vulnerar sus derechos y los de terceros.

3.3 Los niños, niñas y adolescentes deben **conocer que la distribución de contenidos prohibidos** por la regulación local y regional (en especial la pornografía infantil), el acoso (en especial el acoso sexual), la discriminación, la promoción del odio racial, la difamación, la violencia, entre otros, **son ilegales en Internet** y en las redes sociales digitales y están penados por la ley.

3.4 El proceso educativo debe proveer de **conocimiento acerca del uso responsable y seguro por parte de las niñas, niños y adolescentes** de las políticas de privacidad, seguridad y alertas con las que cuentan los instrumentos de acceso y aquellos sitios web en los que las niñas, niños y adolescentes son usuarios frecuentes como las redes sociales digitales.

3.5 Promover una **política educativa —expresada en términos acordes a la edad de las niñas, niños y adolescentes—** que incluya una estrategia informativa y formativa que los ayude a gestionar las potencialidades y

los riesgos derivados de la Sociedad de Información y el Conocimiento, en especial del uso de Internet y de las redes sociales digitales.

3.6 Informar sobre los **mecanismos de protección y las responsabilidades civiles, penales o administrativas** que existen cuando se vulneran derechos propios o de terceros en la red.

3.7 Advertir del **peligro que supone el llamado robo y/o suplantación de identidad** que se puede producir en los entornos digitales que inducen al engaño.

3.8 Explicar a las niñas, niños y adolescentes con un l**enguaje de fácil comprensión el espíritu de las leyes sobre protección de datos personales y protección de la vida privada** de modo tal que puedan captar la idea de la importancia del respeto a la privacidad de las informaciones personales de cada uno de ellos y de los demás.

3.9 **Educar para la incertidumbre** sobre la veracidad de los contenidos y la validación de las fuentes de información. Se debe enseñar a las niñas, niños y adolescentes a buscar y a discriminar las fuentes.

4. Promoción de una sostenida y completa **educación sobre la Sociedad de la Información y el Conocimiento,** en especial para el uso responsable y seguro del Internet y las redes sociales digitales, particularmente por medio de:

4.1 La inclusión en los **planes de estudios,** a todos los niveles educativos, de información básica sobre la importancia de la vida privada y de la protección de los datos personales, y demás aspectos indicados en numeral tres.

4.2 La producción de **material didáctico,** especialmente audiovisuales, páginas web y herramientas interactivas (tales como juegos online) en el que se presenten las potencialidades y los riesgos. Estos materiales deberán incluir información acerca de los mecanismos de protección de los derechos.

La naturaleza de estos temas y materiales exige de la participación y discusión de estos por parte de todos los actores involucrados y con ello responder a las particularidades locales y culturales.

4.3 Los **docentes deben ser capacitados** para facilitar la discusión y poner en contexto las ventajas y los riesgos de la Sociedad de la Información y el Conocimiento, y en especial de Internet y las redes sociales digitales.

Para ello, es fundamental contar con el apoyo de las autoridades de protección de los datos personales o de todas aquellas organizaciones que trabajen en este tema en los diferentes países.

4.4 **Las autoridades educativas**—con el apoyo de las autoridades de protección de datos (donde existan), el sector académico, las organizaciones de la sociedad civil, el sector privado y, cuando sea necesario, con la cooperación

internacional— **deben asistir a los docentes y apoyar el trabajo en las áreas descritas.**

5. Las autoridades competentes deben establecer **mecanismos para que los centros educativos resuelvan los conflictos**, que se generen como consecuencia del uso de Internet y las redes sociales digitales por parte de las niñas, niños y adolescentes, con un sentido didáctico, siempre considerando el interés superior de los mismos, sin vulnerar derechos y garantías, en particular el derecho a la educación.

5.2. Estrategias

Como hemos destacado, el ciberacoso constituye un problema social que puede afectar la salud y el bienestar de las personas, así como su seguridad, especialmente digital. Su prevención y abordaje son fundamentales para garantizar un entorno digital seguro y respetuoso para todos. Algunos organismos internacionales tales como UNICEF, UNESCO, recogen información y análisis sobre este tema. Por ejemplo, para la UNICEF (2022) "el ciberacoso deja una huella digital; es decir, un registro que puede servir de prueba para ayudar a detener el abuso". (s.f)

Muchos Estados han tomado acciones y estrategias para prevenir el ciberacoso, entre ellos Ecuador, a través, del Ministerio de Educación. Para este organismo, el acoso escolar se ha convertido especialmente en los últimos años en una de las formas de violencia escolar con indicadores preocupantes. Ecuador es el segundo país con mayor porcentaje de hostigamiento escolar después de Argentina. (Ministerio de Educación, 2016). Para este organismo el ciberacoso es una agresión,

"una humillación al otro, de manera repetida y que puede suceder cara a cara, pero también por celular o a través de las redes sociales". (p.7)

Las leyes de protección de datos personales, así como sus reglamentos, constituyen un elemento fundamental para hacer frente a los nuevos retos que plantea la sociedad de la información. Así, debido a la rápida evolución tecnológica y la globalización, se hace necesario que la ciudadanía cuente con mecanismos que ayuden a proteger su derecho a la intimidad. (Agencia Española de Protección de Datos, 2019). En el caso de Ecuador, la reciente creación de la Ley Orgánica de Protección de datos constituye un paso muy importante. Sin embargo, es necesario concientizar y educar a la sociedad, especialmente, a padres de familia, directivos, docentes y estudiantes de las escuelas y colegios.

En este orden de ideas, advertimos que el ciberacoso es un problema de gran importancia en la era digital por las siguientes razones:

a. Podría tener un impacto negativo en la salud mental y emocional de las víctimas.

b. Es necesario una seguridad en línea, para que las personas, especialmente los niños y adolescentes puedan aprovechar de sus beneficios sin temor a intimidación y acoso.

c. Puede dañar la reputación de las víctimas y tener consecuencias a largo plazo en su vida personal y profesional.

d. Puede interrumpir la convivencia en la sociedad y en el entorno escolar, afectando el bienestar de los estudiantes y su capacidad para aprender.

e. Algunas formas pueden convertirse en un delito, como la difamación, el acoso sexual y la incitación a la violencia.

f. Es necesario promover valores de empatía, respeto y ética en el uso de la tecnología.

En todo caso, subrayamos que el ciberacoso podría ser considerado de mayor gravedad y extenderse de forma más rápida. Su efecto es exponencial porque su difusión es más fácil de multiplicarse y muy difícil de bloquear y detener la información en la red. (Ministerio del Ecuador, 2016) Frente a esta realidad, se proponen las siguientes estrategias que podrían ayudar a evitar la proliferación del ciberacoso y especialmente evitar que aumente el número de víctimas. Para ello, a partir de las acciones planteadas desde el Memorándum de Montevideo, identificamos las siguientes estrategias:

1. Fortalecer la educación y concientización:

a. Identificar a quienes tienen bajo su responsabilidad el cuidado de los niños y adolescentes, tanto en el entorno familiar como escolar.

b. Impartir programas de educación digital para alumnos, padres y docentes que aborden el ciberacoso, su detección temprana, sus consecuencias y cómo prevenirlo.

c. Promover un ambiente de diálogo abierto sobre el ciberacoso y sus implicaciones en la comunidad escolar.

d. Transmitir claramente a los niños y adolescentes los riesgos que supone el internet y la responsabilidad que conlleva su uso inadecuado. Políticas de privacidad, seguridad y alertas,

es decir una educación completa sobre la sociedad dela Información y el Conocimiento.

e. Formar a los niños y adolescentes sobre la importancia de respetar la vida privada, la protección de datos personales y vulneración de información de terceros que puede atentar con la intimidad.

f. Informar sobre implicaciones legales sobre la protección de datos personales y protección a la vida privada.

g. Educar a los padres sobre el uso seguro de la tecnología y proporcionarles herramientas para supervisar las actividades en línea de sus hijos.

h. Fomentar la comunicación abierta entre padres e hijos sobre sus experiencias en línea.

Sobre este respecto, es importante señalar que la Asociación Profesional Española de Privacidad ha desarrollado la "Guía para padres y educadores sobre el uso de redes sociales e Internet por los menores"[27], que tiene por objeto exponer el papel de la familia, frente a desprotección de los menores en Internet. En todo caso, a partir del programa "Tú decides en Internet", la Agencia Española de Protección de Datos Personales, ha elaborado una Guía sobre "Protección de Datos y Prevención de Delitos[28], la cual pone de manifiesto varias conductas delictivas que tienen como base el uso ilegitimo de información de carácter personal. Así también, dicha entidad ha propuesto la Guía "Enséñales a ser legales en Internet"[29], para familiares y profesores,

27 Disponible en: Guía menores APEP 2015
28 Puede consultar en: guia-proteccion-datos-y-prevencion-de-delitos.pdf (aepd.es)
29 Disponible en: ensenales-ser-legales-en-internet.pdf (aepd.es)

destinada a ejercer actuaciones preventivas, mediante la información y sensibilización en materia de privacidad y protección de datos personales.

2. Promover campañas de prevención y apoyo en las escuelas y colegios:

a. Elaborar material que incluya información sobre el ciberacoso, como prevenirlo e identificarlo.

b. Se debe contar con material actualizado y constante que permita una continua capacitación a los estudiantes, docentes, directivos y personas responsables del cuidado de los niños y adolescentes.

c. Designar un punto de contacto de confianza al que los estudiantes puedan acudir en caso de ser víctimas de ciberacoso.

d. Fomentar prácticas de uso responsable de las redes sociales, como no compartir información personal, no acosar a otros y denunciar el ciberacoso.

e. Establecer un sistema de apoyo para las víctimas de ciberacoso, brindándoles asesoramiento orientativo y psicológico de ser necesario para afrontar la situación.

f. Asegurarse de que las denuncias se manejen de manera confidencial y con empatía.

g. Inculcar valores de empatía y tolerancia en el aula para prevenir la intolerancia y el ciberacoso.

h. Realizar actividades que promuevan la comprensión y la aceptación de la diversidad.

Sobre este punto, también, la Agencia Española de Protección de Datos Personales ha elaborado algunos documentos referenciales. Por ejemplo, la Guía para centros educativos[30], la cual contribuye al respeto de los derechos digitales de los menores en la sociedad de la información. Así también, reconociendo la importancia del derecho a la educación digital previsto en la Ley Orgánica de Protección de Datos de Ecuador, un documento que favorece la implantación de un modelo de cultura digital en las comunidades de aprendizaje es el "Modelo de contenidos para proporcionar a las administraciones educativas para los currículos relacionados con las tic"[31], el cual fue aprobado por la Conferencia Internacional de Autoridades de Protección de Datos en 2016.

3. Políticas y Reglamentaciones:

a. Establecer políticas y códigos de conducta escolar que incluyan sanciones por ciberacoso y delineen procedimientos para abordar denuncias.

b. Garantizar que los estudiantes y padres conozcan y comprendan estas políticas.

c. Regularmente evaluar la efectividad de las políticas y programas implementados y ajustarlos según sea necesario

30 Puede revisarla en: guia-centros-educativos.pdf (aepd.es)
31 Puede consultarla en: marco-conocimientos-privacidad-y-seguridad.pdf (aepd.es)

d. Trabajar en conjunto con las autoridades locales y las fuerzas del orden en casos graves de ciberacoso que puedan requerir medidas legales.

En relación con esto, además, la Agencia Española de Protección de Datos Personales ha elaborado el documento "La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD".[32] Ahora bien, en el marco de nuestro país, hay que considerar, tanto la " Política pública por una internet segura para niños, niñas y adolescentes"[33] del Consejo Nacional para la Igualdad Intergeneracional, como la "Guía para docentes tutores: Prevención de Riesgos Sociales"[34], para la prevención en familias del acoso escolar del Ministerio de Educación de Ecuador.

Desde esta perspectiva, es esencial que las escuelas y colegios tomen un enfoque integral para abordar el ciberacoso, involucrando a estudiantes, padres, docentes y personal escolar en la prevención y el apoyo a las víctimas. La educación y la promoción de un entorno en línea seguro son pasos importantes para combatir el ciberacoso.

32 Documento disponible en: recomendaciones-sobre-acoso-digital-aepd.pdf
33 Disponible en: política_publica_internet_segura.pdf (igualdad.gob.ec)
34 Puede consultarlo en: 2-Guia-Acoso-Escolar-tutores.pdf (educacion.gob.ec)

Referencias

Agencia Española de Protección de Datos. (2019). *La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD*.

Agencia Española de Protección de Datos; AEPD (2022). *Programa "Tú decides en Internet".* Recuperado de https://tinyurl.com/5ymnwf36

Asamblea Nacional del Ecuador; LOPDE (2021). *Ley Orgánica de Protección de Datos Personales de Ecuador*. Registro Oficial n.°459.

Consejo Nacional para la Igualdad Intergeneracional; CNII (2020). *Política Pública para una internet segura para niños, niñas y adolescentes*. Recuperado de https://tinyurl.com/y2fcv9el

Davara Fernández, L. (2017). *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. Madrid. Agencia Española de Protección de Datos.

Fondo de las Naciones Unidas para la Infancia [UNICEF] (2022). Ciberacoso: Que es y como detenerlo. Recuperado de https://tinyurl.com/27aec5m7

Ministerio de Educación. (2016). *Guía para docentes tutores, Prevención de riesgos Sociales.*

Ordóñez Pineda, L. (2018). La comunicación ante el ciudadano. En, Mañas Viniegra, Luis; Meléndez, Sendy y Estrella Martínez [coord.] *Protección de datos personales: precisiones para una cultura digital basada en la corresponsabilidad*, Barcelona, Gedisa.

Secretaria de Educación de Veracruz y Subsecretaria de educación básica. (2010). *Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes. Memorándum de Montevideo.* Recuperado de http://www.iijusticia.org/Memo.htm

5. Sistematización de buenas prácticas enfocadas a la prevención del Ciberacoso, desde la Universidad Técnica Particular de Loja

Mtra. Maritza Ochoa
Mgtr. Juan Jaramillo
Mgtr. Israel Puertas

Antecedentes

El uso de la tecnología tiene un impacto relevante dentro de la sociedad, según Linne (2014) "el fin del siglo 20 y los inicios del 21 están signados por la irrupción de las Tecnologías de Información y Comunicación (TIC)" p. 204. Es común que la juventud actual utilice dispositivos electrónicos y por ello se los reconoce como nativos digitales.

Los nativos digitales[35] son aquellos que tienen como habilidad innata el uso de la tecnología y la consideran esencial dentro del desarrollo sus actividades, con fines educativos, de diversión, para relaciones interpersonales, para efectuar compras y ventas, etc.

Tomando en cuenta la importancia del uso del internet y tecnologías, desde la Carrera de Derecho de la Universidad Técnica

[35] La expresión *Nativos Digitales* fue acuñada en 2001[1], por Marc Prensky, para referirse a las personas, estudiantes, nacidos en la era de la tecnología, producto de la expansión sorprendentemente marcada por dispositivos electrónicos, tales como: computadores (ordenadores), juegos de video, música digital, videos, teléfonos celulares y otros artefactos que hacen cada vez más amigable la navegación por INTERNET y la conformación de Redes Sociales del más variado tipo. (2010). Nativos Digitales: Desafió de la educación actual. *Paradígma*, *31*(2), 5-6. Recuperado en 20 de octubre de 2023, de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1011-22512010000200001&lng=es&tlng=es.

Particular de Loja, con base en una problemática identificada en la sociedad como es el desconocimiento de los derechos digitales en la sociedad de la información lo cual deriva en riesgos y amenazas que supone el uso ilegítimo de información de carácter personal, generando, en muchas ocasiones, la invasión de la intimidad de las personas, acoso mediante medios digitales, violencia, entre otras tipologías. Es por ello que se ha planteado proyectos de vinculación con la colectividad identificando como beneficiarios a los jóvenes[36] con la finalidad de afianzar el derecho a la educación digital previsto en la Ley Orgánica de Protección de datos personales, el cual tiene por objeto capacitar sobre el uso y manejo adecuado, seguro y responsable de las tecnologías de la información y la comunicación.

El proyecto de vinculación denominado "Garantía de los derechos digitales de los jóvenes en la sociedad de la información, aprobado por la Dirección de Vinculación de la UTPL, se desarrolló para efectuar el aprendizaje práctico experimental de las asignaturas Prácticum 2 prácticas preprofesionales y de vinculación con la Colectividad malla ECTS y Prácticum 1 Servicio Comunitario en la malla de rediseño, para cumplir con el art. 87, de la Ley Orgánica de Educación Superior (LOES), ya que los estudiantes deben acreditar servicios a la comunidad, a través de participación en programas de vinculación con la sociedad, prácticas o pasantías preprofesionales, con el acompañamiento pedagógico, acorde a cada especialidad. (LOES, 2020).

El objetivo del proyecto de vinculación fue el de "promover el respeto de los derechos digitales de los jóvenes en la sociedad de la información mediante talleres de capacitación." Para ello fue necesario aplicar una metodología participativa, de intervención y acción, en la

[36] Considerados como un grupo de atención prioritaria según el Art. 35 de la Constitución de la República del Ecuador.

cual convergen dos procesos, conocer y actuar, mediante la cual, como lo señala Abarca (2016), "visibiliza aspectos tradicionalmente ocultos como las interculturalidades, las cosmovisiones, la vida cotidiana, las subjetividades, las percepciones e intuiciones, los aprendizajes, la historiografía, la equidad, la diversidad entre las personas, entre otras". p. 95

Es así como los estudiantes de la carrera de Derecho, en primera instancia, efectuaron un análisis jurídico y doctrinario sobre los derechos digitales dentro de la sociedad de la información, para determinar, por una parte, la naturaleza de derechos relacionados con la intimidad, protección de datos personales, identidad digital, entre otros; y, por otra parte, identificar las problemáticas relacionadas con la vulneración de dichos derechos. En una segunda fase se desarrollaron diversos talleres de capacitación para instruir y formar a la colectividad sobre los derechos digitales.

El proyecto se ejecutó en modalidad a distancia en dos periodos académicos comprendidos desde el 1 de abril de 2022 al 31 de marzo de 2023, el alcance del proyecto fue nacional, se desarrolló en varias ciudades del Ecuador, esto dependía del lugar de residencia de los estudiantes de Derecho que aplicaron el proyecto. También se ejecutó en modalidad presencial durante el periodo abril – agosto 2023. Como resultados generales tenemos:

Tabla 1.

Beneficiarios del proyecto de vinculación

CATEGORÍA	VARIABLES	MODALIDAD A DISTANCIA		MODALIDAD PRESENCIAL
		# BENEFICIARIOS ATENDIDOS		# BENEFICIARIOS ATENDIDOS
		CICLO 1 ABRIL - AGOSTO 2022	CICLO 2 OCTUBRE 2022 - FEBRERO 2023	CICLO 1 ABRIL - AGOSTO 2023
SEXO	Femenino	**4471**	**8724**	**93**
	Masculino	**4304**	**7280**	**78**
	Bisexual	**54**	**27**	**3**
	Gay	**20**	**36**	**2**
	Intersexual	**10**	**86**	**0**
	Lesbiana	**20**	**5**	**1**
	Otra	**13**	**19**	**1**
EDAD	De 1 a 18 años	**1606**	**3182**	**53**
	De 19 a 65 años	**7199**	**12891**	**125**
	De 65 años en adelante	**87**	**125**	**0**
GRUPO ÉTNICO	Indígena	**398**	**14210**	**4**
	Mestizo	**7778**	**447**	**161**
	Blanco	**315**	**613**	**10**
	Afroecuatoriano	**180**	**420**	**3**
	Montubio	**189**	**426**	**0**
	Otros	**32**	**82**	**0**
DISCAPACIDAD	Sin discapacidad	**8707**	**15554**	**175**
	Con discapacidad	**185**	**644**	**3**
TOTAL GENERAL DE BENEFICIARIOS DIRECTOS		**8892**	**16198**	**178**

Elaboración: Ochoa M. (2023)

Entre los participantes indirectos del proyecto tenemos:

Tabla 2.

Participantes y ejecutores del proyecto de vinculación

	MODALIDAD A DISTANCIA		MODALIDAD PRESENCIAL
CATEGORÍA	**CICLO 1 ABRIL - AGOSTO 2022**	**CICLO 2 OCTUBRE 2022 - FEBRERO 2023**	**CICLO 1 ABRIL - AGOSTO 2023**
Total de estudiantes	**1207**	**3304**	**70**
Total de horas invertidas por estudiantes	**256**	**256**	**96**
Total de docentes, coordinadores y personal académico involucrado	**18**	**18**	**3**
Total de horas invertidas por todo el personal académico involucrado	**450**	**950**	**300**

Elaboración: Ochoa M. (2023)

Adicional, los beneficiarios del proyecto de vinculación manifestaron que dicho proyecto ha tenido muy buena acogida dentro de la colectividad; se debe destacar que este proyecto también tuvo incidencia en grupos de atención prioritaria, tales como jóvenes, mujeres embarazadas, personas con discapacidad, personas con enfermedades catastróficas y adultos mayores.

Finalmente, es necesario resaltar la importancia de la función sustantiva de vinculación como parte del quehacer de las Instituciones de Educación Superior por cuanto permiten a los estudiantes conocer la realidad de su entorno y ser protagonistas de un cambio, asimismo, se logra beneficiar a la colectividad aportando con la transferencia de conocimientos, por cuanto es un beneficio social en el conocimiento de derechos constitucionales y de aporte sociales.

En el periodo académico abril – agosto 2023, se desarrolló el proyecto articulado denominado "El ciberacoso en las comunidades de aprendizaje" con los estudiantes de la carrera de Derecho en Modalidad a distancia, cuyo objetivo fue el de "determinar la naturaleza y los efectos del ciberacoso en las comunidades de aprendizaje". En la fase de vinculación se emplearon metodologías participantes "intervención-acción" en la cual se levantó información, a través, de la aplicación de encuestas a estudiantes (edades comprendidas entre 16 a 29 años), con la información recabada y con el acompañamiento permanente de los docentes integrantes del proyecto se trabajó en la construcción de insumos y en talleres para la prevención del ciberacoso. Se han identificado algunas buenas prácticas puesto que, se ha trabajado con una diversidad de casos. La metodología aplicada se desarrolló con un enfoque de participación – acción, el rol del estudiante de Derecho fue protagónico y fungió como capacitador, exponiendo respecto a la normativa nacional acerca de los efectos y sanciones del ciberacoso, analizaron diversos cuerpos normativos vigentes y determinaron conclusiones relacionadas a las causas y efectos de la violencia digital existente en las comunidades de aprendizaje.

5.1. Buenas prácticas

Entre las buenas prácticas que se han desarrollado en el proyecto de vinculación destacamos las siguientes:

1. **Buena Práctica:** Aplicación de las actividades del proyecto realizadas en un Centro de Privación de Libertad

a. **Entorno educativo:** Centro de Privación de Libertad "Napo No. 1"

b. **Lugar de ejecución:**

- Provincia: NAPO
- Cantón: TENA
- Parroquia: TENA
- Barrio: LOS PINOS

c. **Beneficiarios:** Los beneficiarios directos del proyecto fueron personas privadas de la libertad, que fueron informados e involucrados en cada una de las actividades solicitadas y que pertenecían al proyecto de vinculación.

d. **Número de beneficiarios de ese caso:** 15 asistentes.

3. **Buena Práctica:** Aplicación de las actividades del proyecto realizadas en un Centros Educativos de la ciudad de Loja.

a. **Entorno educativo:** Unidad Educativa Bernardo Valdivieso / Unidad Educativa Teniente Coronel Lauro Guerrero

b. Lugar de ejecución:

- Provincia: LOJA
- Cantón: LOJA
- Parroquia: SAN SEBASTIAÓN / EL VALLE
- Barrio: LA PRADERA / EL VALLE

c. Beneficiarios: Los beneficiarios directos del proyecto fueron estudiantes de dos comunidades educativas de la ciudad de Loja, jóvenes comprendidos entre los 15 a 20 años que fueron informados e involucrados en cada una de las actividades solicitadas y que pertenecían al proyecto de vinculación.

d. Número de beneficiarios de ese caso: 178 asistentes.

3. Buena Práctica: Aplicación de las actividades del proyecto de vinculación en comunidad rural

a. Entorno educativo: Comunidad rural.

b. Lugar de ejecución:

- Provincia: CHIMBORAZO
- Cantón: RIOBAMBA
- Parroquia: LIZARZABURU

c. Beneficiarios: los beneficiarios directos del proyecto fueron residentes de una comunidad rural que fueron informados e involucrados en cada una de las actividades solicitadas y que pertenecían al proyecto de vinculación.

d. Número de beneficiarios de ese caso: 20 personas capacitadas.

Como podemos analizar con lo expuesto anteriormente, desde la Carrera de Derecho se han desarrollado proyectos de vinculación con la colectividad que han tenido un gran impacto en la sociedad y han servido como mecanismo para evidenciar la práctica profesional del estudiante.

En este sentido, vamos a exponer de forma general las definiciones básicas sobre ciberacoso, sus características, así como las diversas prácticas de ejercer ciberacoso y las formas de prevención identificadas.

5.2. Definición de Ciberacoso.

PK Smith y otros, quienes son citados por Rober Slonje, Peter K. Smith y Ann Frisen, en su artículo denominado La naturaleza del *Cyberbullying* y estrategias para su prevención, definen al ciberacoso como "un acto o comportamiento agresivo que se lleva a cabo utilizando medios electrónicos por un grupo o un individuo repetidamente y a lo largo del tiempo contra una víctima que no puede defenderse fácilmente" (Smith et. al. otros, 2008); y, a partir de ella, proporcionan una definición propia del mismo, indicando que "el ciberbullying es un abuso sistemático de poder que se produce mediante el uso de las tecnologías de la información y la comunicación (TIC)." (Slonje et al. otros, 2013).

Por tanto, no ha variado la naturaleza o esencia del acoso, aquella consistente la afectación de la víctima mediante la ejecución de actos lesivos o pronunciamiento de palabras hirientes, que provocan en la víctima efectos negativos que inciden en su personalidad y desarrollo integral. Pero concomitantemente a la evolución tecnológica que atravesamos, el acceso a redes sociales y la facilidad de transferencia de información (datos personales, fotografías, etc.) mediante dispositivos

tecnológicos, la práctica del acoso ha evolucionado también, adoptando mecanismos ajenos a los ya conocidos; siendo ejercido a través del ciber espacio, acortando distancias, superando límites físicos, violentando la seguridad proporcionada por el hogar y logrando su cometido.

Situación con la que concuerda Mateo y otros, quienes manifiestan que "el ciberacoso es entendido como el daño repetido e intencionado ocasionado a través de medios electrónicos como teléfonos móviles o internet (Patchin y Hinduja, 2006), realizado por un grupo o individuo contra el que la víctima no puede defenderse por sí misma. Debido a los diferentes formatos tecnológicos, los 'ciberacosadores' (adultos o menores), muchas veces anónimos (forma indirecta de acoso), realizan amenazas, vejaciones, fotografías intimidantes, hostigamientos, y/o menosprecios hacia sus compañeros/as de pupitre a través de diferentes mecanismos con base tecnológica" (Mateo et al. otros, 2010).

Resulta importante destacar la intencionalidad de los agresores, esto significa que, muy aparte de la decisión de compartir información ajena, tienen consciencia del daño que van a provocar y de la imposibilidad de resarcirlo.

5.3. Características del ciberacoso.

De la comparación del acoso tradicional y el ciber acoso, se pueden determinar, a partir de la modalidad de su práctica y efectos, ciertas particularidades propias de este último.

A decir de Slonje y Smith (2008), citados por Mateo y otros en su artículo El ciberacoso en la enseñanza obligatoria, "el ciberacoso se diferencia de las otras tipologías de acoso escolar fundamentalmente en tres aspectos: (a) las víctimas del acoso tradicional dejan de ser agredidas

una vez que se encuentran en su casa, mientras que las víctimas del ciberacoso no dejan de recibir mensajes difamatorios mientras están conectados; (b) el ciberacoso puede implicar a muchas personas, mientras que en el acoso tradicional suelen estar implicados pequeños grupos de iguales; (c) la invisibilidad de los agresores, no siendo consciente el agresor del daño real que propina a la víctima." (Mateo et al. otros, 2010), lo que claramente denota una transgresión de barreras físicas que antes brindaban seguridad a las víctimas del ciberacoso.

Alba, A. (2020), en cuanto a las características del ciberacoso manifiesta que "La forma de contacto entre víctimas y agresores en el caso del ciberacoso introduce factores de riesgo específicos, como el anonimato del agresor, la gran difusión social de la situación, las dificultades prácticas para detener la agresión y, por extensión, terminar con el sufrimiento de la víctima".

Resulta evidente la facilidad de la práctica del ciberacoso, pues, las TIC permiten al agresor ejecutar sus intenciones de manera anónima, es decir, la comisión del acto sin la menor posibilidad de una evidente responsabilidad social o penal (según corresponda), por las consecuencias de sus actos. La difusión masiva, sin contar las secuelas producidas a la víctima, es, al parecer, la peor de las consecuencias del ciberacoso, pues dificulta la detención de la transferencia de la información de la que se trate y, por tanto, el agravio es, por mucho, más considerable.

Romero, A. (2017), quien es citado por Torres y otros, en su artículo Características del ciberacoso y psicopatología de las víctimas, hace énfasis en las características del ciberacoso y las describe como "el componente tecnológico, la naturaleza hostil del acto, la intención de

causar sufrimiento, considerado por la mayoría de los conocedores e investigadores como crucial para la definición y la repetitividad"

Por otro lado, la definición convencional de *bullying* incluye tres características: intencionalidad, desequilibrio de poder entre agresor y víctima y la repetición de la conducta en el tiempo. (Cerezo y Rubio, 2017)

Por tanto, se podrá entonces identificar el ciberacoso cuando exista una evidente manifestación intencional de causar daño, infringiéndolo mediante cualquiera de las modalidades mencionadas anteriormente, de manera repetitiva y mediante el uso de dispositivos tecnológicos. Es importante destacar también la magnitud de los efectos provocados por este ciberacoso y la cantidad de sujetos receptores de esta información, pues se debe considerar que, tradicionalmente el acoso no comportaba necesariamente la socialización de estos actos, pues los mismos podían ser ejercidos sin la posibilidad de ser presenciados por más personas que los sujetos participes del mismo (acosador/es y víctima/s); sin embargo, la difusión de esta información en ciertos casos tiene numerosos destinatarios y esto comporta intencionalmente también, la humillación social de la víctima, modalidad que actualmente, podría ser mucho más nociva de la violencia física.

5.4. Prácticas del ciberacoso identificadas

En la era digital, el avance tecnológico ha traído consigo una serie de beneficios, pero también desafíos significativos para la sociedad. Uno de estos desafíos es el ciberacoso, una preocupación creciente que afecta a personas de todas las edades y en diferentes contextos. El ciberacoso se manifiesta en diversas prácticas, desde el acoso en línea hasta el *grooming*, el *sexting* y el *cyberbullying*.

Así, podemos identificar algunas prácticas de ciberacoso, por ejemplo:

a. **Acoso en Línea:** El acoso en línea es una práctica común en la que los acosadores utilizan plataformas digitales, como redes sociales, correos electrónicos o mensajes instantáneos, para hostigar, amenazar o difamar a sus víctimas. Esto puede incluir insultos, difamación, suplantación de identidad y publicación de contenido ofensivo (Aníbal Sierra & Espinosa Cabrera, 2021). Los acosadores en línea a menudo se aprovechan del anonimato que ofrecen estas plataformas, lo que les permite actuar con impunidad y minimizar las consecuencias directas de sus acciones. El impacto del acoso en línea en las víctimas puede ser profundo y duradero, afectando su salud mental, autoestima y bienestar general. Las víctimas pueden experimentar ansiedad, depresión, estrés postraumático e incluso pensamientos suicidas. Esta, no solo afecta a individuos, sino que también puede tener repercusiones significativas en comunidades enteras y en el tejido social. Las campañas de acoso coordinadas pueden dirigirse contra grupos específicos, exacerbando divisiones y tensiones sociales. Es por ello que en muchas legislaciones se está comenzando a implementar normativa más estricta para combatir el acoso en línea y proteger a las víctimas. Además, las plataformas digitales, por su parte, han empezado a tomar medidas más rigurosas para combatir el acoso en línea mediante la implementación de algoritmos de detección, políticas de uso más estrictas y herramientas que permiten a los usuarios reportar comportamientos inapropiados. Sin embargo, estas medidas

aún son insuficientes en muchos casos, y es necesario que se continúe trabajando en la mejora de la seguridad y el bienestar en línea. La educación y la concienciación también juegan un papel crucial, ya que empoderar a los usuarios con conocimientos sobre cómo protegerse y responder al acoso en línea puede ser una herramienta poderosa para mitigar sus efectos.

b. ***Cyberbullying:*** El *cyberbullying* es una forma específica de acoso en línea que se enfoca en intimidar a menudo a niños y adolescentes. Los acosadores utilizan la web y las redes sociales para hostigar a sus víctimas a través de mensajes crueles, exclusión social, la divulgación de secretos y la difusión de rumores (Aníbal Sierra & Espinosa Cabrera, 2021). Esta práctica puede manifestarse de diversas maneras, incluyendo el envío de amenazas directas, la creación de perfiles falsos para suplantar la identidad de la víctima, y la publicación de fotos o videos comprometedores sin consentimiento. Este abuso se ve agravado debido a la naturaleza omnipresente y rápida de las tecnologías digitales, lo que amplifica el impacto de esta problemática, ya que los contenidos pueden ser compartidos instantáneamente con una audiencia amplia, dificultando el control y la eliminación del material ofensivo. El *cyberbullying* puede tener consecuencias devastadoras para las víctimas, pues a menudo, los niños y adolescentes que sufren este tipo de acoso experimentan una disminución significativa en su autoestima y pueden desarrollar problemas de salud mental como ansiedad, depresión y estrés postraumático. Además, esta práctica presenta desafíos únicos para padres,

educadores y autoridades. A diferencia del acoso tradicional, que puede ser observado y abordado en entornos físicos, el *cyberbullying* ocurre en el espacio digital, donde la supervisión es más complicada y las pruebas del acoso pueden ser efímeras. Es por ello que es necesario fomentar una cultura de respeto y empatía tanto en línea como fuera de línea, enseñar a los jóvenes sobre el uso responsable de la tecnología y proporcionarles herramientas para manejar conflictos digitales de manera constructiva. Las plataformas digitales también tienen la responsabilidad de implementar y hacer cumplir políticas que protejan a los usuarios de acoso y abuso. Además, la colaboración entre padres, educadores, legisladores y empresas tecnológicas es esencial para desarrollar estrategias integrales que aborden el problema de manera eficaz y sostenible.

c. ***Grooming:*** El *grooming* se refiere a la manipulación en línea de niños y adolescentes por parte de adultos con intenciones dañinas. Los agresores buscan ganarse la confianza de sus víctimas con el objetivo de explotarlas sexualmente o involucrarlas en actividades, por lo menos, inapropiadas (Calvete, y otros, 2021). Este proceso de manipulación puede ser largo y sofisticado, involucrando una serie de tácticas destinadas a desensibilizar y aislar a la víctima. Los *groomers* a menudo comienzan estableciendo una relación de amistad y empatía, mostrando un interés genuino en la vida y los problemas de la víctima para crear una conexión emocional fuerte. A medida que la relación progresa, el agresor puede comenzar a introducir conversaciones de naturaleza sexual, compartiendo contenido explícito y solicitando

imágenes o videos íntimos de la víctima. En muchos casos, los *groomers* utilizan técnicas de coerción y chantaje, amenazando con divulgar las imágenes o información privada si la víctima no cumple con sus demandas. Este tipo de explotación puede tener consecuencias devastadoras para la salud mental y emocional de los jóvenes, pues las víctimas pueden experimentar sentimientos de culpa y vergüenza, lo que dificulta que busquen ayuda o revelen lo que les está sucediendo. Además, esta práctica puede llevar a encuentros físicos peligrosos. Algunos agresores buscan trasladar la relación en línea a un encuentro cara a cara, aumentando significativamente el riesgo de abuso sexual y otros tipos de explotación. Además, el *grooming* puede ser un precursor de otros delitos graves, como la trata de personas y la pornografía infantil. La detección y prevención de esta práctica presenta varios desafíos. Los agresores suelen utilizar perfiles falsos y enmascarar su identidad, lo que dificulta la identificación y el rastreo. Además, los niños y adolescentes pueden no ser conscientes de los riesgos y peligros asociados con las interacciones en línea, lo que los hace más vulnerables a las tácticas de manipulación. Por lo tanto, es fundamental que los padres, educadores y cuidadores estén informados sobre los signos de advertencia del *grooming* y mantengan una comunicación abierta y honesta con los jóvenes sobre su actividad en línea. Las plataformas digitales y las autoridades también juegan un papel crucial en la lucha contra esta amenaza. Las empresas tecnológicas deben implementar y reforzar medidas de seguridad, como algoritmos de detección de comportamiento sospechoso y herramientas de denuncia

accesibles para los usuarios. Asimismo, las fuerzas del orden deben recibir capacitación adecuada para investigar y perseguir casos de *grooming*, y los sistemas legales deben actualizarse para reflejar la naturaleza evolutiva de estos crímenes en el entorno digital.

d. ***Sexting***: El *sexting* implica el envío de contenido sexualmente explícito a través de dispositivos electrónicos. Aunque algunas personas lo hacen consensuadamente, puede convertirse en una forma de ciberacoso cuando las imágenes o mensajes son compartidos sin el consentimiento de la persona implicada (Quesada, Fernández-González, & Calvete, 2018). Este tipo de comportamiento no consensuado puede tener graves consecuencias emocionales, sociales y legales para las víctimas, quienes pueden enfrentar humillación, vergüenza, y estrés psicológico intenso. La difusión no autorizada de contenido íntimo, conocida como "pornografía de venganza," es una forma particularmente dañina de ciberacoso que puede arruinar reputaciones y causar un daño irreparable a la vida personal y profesional de la víctima. El impacto negativo del *sexting* no consensuado se ve exacerbado por la naturaleza viral de internet y las redes sociales, donde las imágenes y videos pueden ser compartidos rápida y ampliamente, quedando fuera del control de la persona afectada. Este tipo de exposición puede llevar a la víctima a experimentar aislamiento social, depresión y ansiedad. En algunos casos extremos, las víctimas pueden tener pensamientos suicidas o incluso intentar suicidarse debido a la desesperación y el sentimiento de pérdida de control sobre su propia imagen y privacidad.

Además de las consecuencias emocionales y psicológicas, el *sexting* no consensuado puede tener implicaciones legales significativas, pues en nuestro país, así como en otras jurisdicciones, se tienen leyes que penalizan la distribución no autorizada de material sexualmente explícito y, los responsables, pueden enfrentar una responsabilidad penal. Además, las víctimas también pueden tener la opción de buscar reparaciones civiles por los daños sufridos, aunque este proceso puede ser largo y emocionalmente agotador. Dentro de esta problemática, es importante que las personas, especialmente los jóvenes, comprendan las posibles repercusiones de compartir contenido íntimo y sean conscientes de los peligros de confiar en otros con dicho material. Para ello es necesario que se eduque respecto a una mayor comprensión y conciencia sobre el consentimiento y el respeto por la privacidad de los demás. Además, las plataformas digitales también tienen un papel crucial en la mitigación de los riesgos del *sexting*. Deben implementar políticas y herramientas eficaces para detectar y eliminar contenido no consensuado, así como proporcionar recursos y apoyo a las víctimas de ciberacoso.

El ciberacoso es una amenaza persistente en el mundo digital actual, y sus diversas formas impactan negativamente a individuos de todas las edades, como se habla en el presente manual.

5.5. Formas de prevención del ciberacoso

En la era digital, donde la tecnología se ha vuelto parte fundamental de nuestras vidas, el ciberacoso se ha convertido en un problema cada vez más común y perjudicial. Para abordar este desafío, es esencial implementar estrategias efectivas de prevención. Así, a continuación, se detalla formas de prevenir el ciberacoso, destacando la importancia de la educación, la promoción de la empatía y el fomento de un entorno en línea seguro.

5.5.1. Educación sobre el Ciberacoso

Una de las estrategias fundamentales para prevenir el ciberacoso es la educación. Tanto en las escuelas como en los hogares, es esencial crear conciencia sobre los riesgos asociados con el uso de la tecnología y cómo prevenir el ciberacoso (Rojas-Díaz & Yepes-Londoño, 2022). Esto implica:

- **Educación temprana:** Iniciar la educación sobre el ciberacoso desde una edad temprana, enseñando a los niños sobre la importancia del respeto en línea y cómo reconocer comportamientos de ciberacoso. Esta educación debe comenzar en los primeros años de la escolarización, integrando conceptos básicos de respeto y empatía digital en el currículo de los niños pequeños. Utilizar recursos interactivos y adaptados a la edad, como cuentos, juegos y actividades lúdicas, puede hacer que los niños comprendan mejor la importancia de tratar a los demás con amabilidad en el entorno digital. Además, es crucial enseñarles a identificar señales de ciberacoso y qué pasos deben seguir si son testigos o víctimas de estas conductas.

- **Concientización en las escuelas:** Las instituciones educativas deben incluir programas de prevención del ciberacoso en su currículo, informando a los estudiantes sobre los riesgos y las consecuencias de estas acciones. Estos programas deben ser integrales y abarcar desde la educación primaria hasta la secundaria. Es importante que las escuelas desarrollen talleres y sesiones interactivas que aborden temas como la seguridad en línea, la privacidad digital, y las estrategias para manejar conflictos y resistir la presión de grupo. Invitar a expertos en ciberseguridad y psicólogos puede proporcionar a los estudiantes una perspectiva profesional y práctica sobre cómo enfrentar y prevenir el ciberacoso. También es fundamental que las escuelas implementen políticas claras y consistentes sobre el manejo del ciberacoso, asegurando que los estudiantes comprendan las consecuencias de participar en este tipo de comportamiento.

- **Participación de los padres:** Los padres deben estar involucrados en la educación de sus hijos sobre el ciberacoso y establecer pautas para un uso seguro de la tecnología. Es esencial que los padres mantengan una comunicación abierta y constante con sus hijos sobre sus actividades en línea y les enseñen a utilizar internet de manera responsable. Organizar sesiones informativas y talleres para padres en colaboración con las escuelas puede ayudarles a entender mejor los riesgos del ciberacoso y cómo pueden apoyar a sus hijos en la prevención de estos comportamientos. Los padres deben ser modelos a seguir en el uso ético y seguro de la tecnología, y establecer reglas claras sobre el tiempo de pantalla y el tipo de contenido que sus hijos pueden acceder. También

es importante que los padres conozcan las herramientas de control parental y las utilicen para supervisar la actividad en línea de sus hijos, sin invadir su privacidad, para asegurarse de que están protegidos contra posibles amenazas.

5.5.2. Promoción de la Empatía y la Resolución de Conflictos

Otro enfoque importante en la prevención del ciberacoso es fomentar la empatía y la resolución de conflictos (Estévez, Flores, Estévez, & Huéscar, 2019). Esto implica:

- **Enseñar empatía:** En la educación, enfatizar la importancia de ponerse en el lugar de los demás y comprender cómo las acciones en línea pueden afectar emocionalmente a las personas. Los programas educativos pueden incluir actividades y ejercicios que ayuden a los estudiantes a desarrollar habilidades de empatía, como el *role-playing*, donde los alumnos toman el papel de las víctimas para experimentar sus sentimientos y reacciones. También es útil incorporar historias y casos reales de ciberacoso en el currículo para ilustrar el impacto real de estas acciones en la vida de las personas.
- **Fomentar la comunicación:** Enseñar habilidades de comunicación efectiva para resolver conflictos de manera pacífica y constructiva, tanto en línea como fuera de línea. Esto puede incluir técnicas de mediación y negociación, así como la enseñanza de la escucha activa y la expresión asertiva de los sentimientos y necesidades. Los talleres y las actividades grupales pueden proporcionar a los estudiantes un espacio seguro para practicar estas habilidades y recibir

retroalimentación constructiva. Además, las escuelas pueden establecer programas de mentoría donde los estudiantes mayores guíen a los más jóvenes en la gestión de conflictos y la comunicación efectiva.

- **Promover la intervención:** Incentivar a los testigos del ciberacoso a intervenir, denunciando la conducta y apoyando a las víctimas. Es crucial educar a los estudiantes sobre la importancia de no ser espectadores pasivos ante el ciberacoso. Las campañas de concienciación pueden resaltar el papel vital que los testigos pueden desempeñar en la detención del acoso y el apoyo a las víctimas. Proveer guías y recursos sobre cómo intervenir de manera segura y efectiva puede empoderar a los estudiantes para tomar medidas cuando presencian ciberacoso. Además, reconocer y premiar a aquellos que actúan en defensa de sus compañeros puede fomentar una cultura de intervención positiva.

5.5.3. Creación de un Entorno en Línea Seguro.

Para prevenir el ciberacoso, es esencial crear un entorno en línea seguro. Esto incluye (Álvarez del Cuvillo, 2021):

- **Plataformas seguras:** Las empresas tecnológicas deben implementar medidas de seguridad, como la moderación de contenido y la detección de comportamientos dañinos. Utilizar algoritmos avanzados y equipos de moderación humana para identificar y eliminar rápidamente contenido inapropiado. Además, proporcionar herramientas para que los usuarios puedan bloquear y reportar cuentas abusivas de manera sencilla y efectiva.

- **Privacidad y seguridad:** Enseñar a los usuarios cómo proteger su información personal y configurar adecuadamente las opciones de privacidad en línea. Esto incluye la educación sobre contraseñas seguras, la importancia de no compartir información sensible públicamente y el uso de autenticación de dos factores. También es crucial informar a los usuarios sobre los riesgos asociados con la publicación de datos personales y cómo pueden ser explotados por los acosadores.

- **Denuncias y consecuencias:** Establecer procedimientos claros para denunciar el ciberacoso y garantizar que haya consecuencias para los acosadores. Crear sistemas accesibles y eficaces para que las víctimas puedan reportar incidentes de acoso, y asegurarse de que estas denuncias sean tratadas con seriedad y rapidez. Las plataformas deben cooperar con las autoridades legales cuando sea necesario y tomar medidas disciplinarias firmes contra los acosadores, incluyendo la suspensión o eliminación de cuentas.

Prevenir el ciberacoso es un esfuerzo conjunto que involucra a la educación, la empatía y la promoción de un entorno en línea seguro. La educación temprana, la concientización en las escuelas y la participación de los padres son esenciales para crear una base sólida de prevención. Fomentar la empatía y la resolución de conflictos ayuda a crear relaciones saludables en línea, y la creación de un entorno seguro en línea es responsabilidad de todos los usuarios y las empresas tecnológicas. La prevención del ciberacoso es un objetivo alcanzable si, en la sociedad, trabajamos juntos para crear una cultura en línea de respeto y empatía.

Referencias

Abarca, F. (2016). La metodología participativa para la intervención social: Reflexiones desde la práctica. *Revista Ensayos Pedagógicos* V, 9(1), 87-109. Recuperado de https://dialnet.unirioja.es/descarga/articulo/5585469.pdf

Alba, A. (2020) Acoso escolar, ciberacoso y las nuevas tecnologías de la información y comunicación. Revista cubana de medicina general integral (36)3, 1120. URL. https://www.medigraphic.com/pdfs/revcubmedgenint/cmi-2020/cmi203l.pdf

Álvarez del Cuvillo, A. (2021). El Ciberacoso en el trabajo como categoría jurídica. *Revista andaluza de trabajo y bienestar social*(157), 167-192. Obtenido de https://dialnet.unirioja.es/descarga/articulo/7968641.pdf

Aníbal Sierra, J., & Espinosa Cabrera, C. (2021). Prácticas de ciberacoso predominantes en estudiantes de 10° y 11° de una institución educativa privada. *Busqueda, 8*(2). doi:https://doi.org/10.21892/01239813.559

Asamblea Constituyente del Ecuador. (2008, 20 de octubre). Constitución de la República del Ecuador. Registro Oficial 449. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Calvete, E., Cortazar, N., Fernández-González, L., Echezarraga, A., Beranuy, M., León, A., . . . Orue, I. (2021). Los efectos de una intervención preventiva breve en ciberacoso y *grooming* en adolescentes. *Psychosocial Intervention, 30*(2), 75-84. doi:https://dx.doi.org/10.5093/pi2020a22

Cerezo, F. y Rubio, F. (2017) Medidas relativas al acoso escolar y ciberacoso en la normativa autonómica española. Un estudio comparativo. *Revista Electrónica Interuniversitaria de Formación del Profesorado* (20)1, 113126.

Estévez, E., Flores, E., Estévez, J. F., & Huéscar, E. (2019). Programas de intervención en acoso escolar y ciberacoso en educación secundaria con eficacia evaluada: una revisión sistemática. *Revista Latinoamericana de Psicología, 51*(3). doi:http://dx.doi.org/10.14349/rlp.2019.v51.n3.8

Felix, V., Soriano, M., Godoy, C., Sancho, S., (2010). *El ciberacoso en la enseñanza obligatoria*. URL. http://hdl.handle.net/11162/5058

Linne, J, (2014), Dos generaciones de nativos digitales, *Intercom – RBCC, 37* 2, pp.203 -221.

Quesada, S., Férnandez-González, L., & Calvete, E. (2018). El sexteo (*sexting*) en la adolescencia: Frecuencia y la asociación con la victimización de ciberacoso y violencia en el noviazgo. *Behavioral Psychology, 26*(2), 225-242.

Rojas-Díaz, J. S., & Yepes-Londoño, J. J. (2022). Panorama de riesgos por el uso de la tecnología en América Latina. Trilogía Ciencia Tecnología Sociedad, 14(26). Obtenido de https://doi.org/10.22430/21457778.2020

Slonje, R. Smith, P. y Frisen, A. (2012) *La naturaleza del cyberbullying y estratégias para su prevención*. https://www.sciencedirect.com/science/article/pii/S0747563212002154

Torres, Y., Mejía, J., Reryna, E., (2018). *Características del ciberacoso y psicopatología de las víctimas.* URL. https://revistas.fucsalud.edu.co/index.php/repertorio/article/view/213

6. Conclusiones Generales

- En la Sentencia 456-20-JP /21 de la Corte Constitucional de Ecuador, se analiza de manera integral la justicia restaurativa y el derecho al debido proceso como garantías del interés superior del niño en los procesos sancionatorios aplicados en un colegio de Quito. Este caso marca un hito en el análisis y juzgamiento del sexting, dado que la Corte Constitucional del Ecuador, antes de tomar su decisión, llevó a cabo un análisis jurídico profundo sobre las comunidades de aprendizaje y los códigos de convivencia como garantías del derecho al debido proceso en el ámbito educativo, además de la reparación integral. Cabe destacar que esta sentencia tiene jurisprudencia vinculante.

- Para prevenir el ciberacoso, es importante tomar medidas que incluyan educar sobre el uso seguro de la tecnología, mejorar la comunicación y crear entornos digitales seguros. Es clave enseñar a estudiantes, padres y maestros sobre los peligros del ciberacoso y cómo usar internet con responsabilidad, fomentando el respeto y la empatía. Para ello se requiere plantear reglas claras para reportar y manejar casos de ciberacoso. Acciones como monitorear las actividades en línea, trabajar juntos con las escuelas y las plataformas tecnológicas, y promover habilidades emocionales ayudan a crear un ambiente escolar digital libre de acoso. Además, estas estrategias deben estar respaldadas por leyes y políticas que protejan los derechos de los estudiantes en internet.

- El ciberacoso es un problema que sigue creciendo y afecta a personas de todas las edades, debido al aumento del uso de internet y las redes sociales. Para reducir sus riesgos, es clave promover buenas prácticas tanto a nivel personal como institucional. Es fundamental fomentar una cultura digital basada en el respeto y la empatía, donde las plataformas en línea impulsen interacciones positivas y eviten el uso de lenguaje ofensivo. Las personas deben ser conscientes de que sus palabras en internet tienen impacto, y que el anonimato no es excusa para el maltrato. También es importante enseñar a identificar situaciones de ciberacoso y saber cómo actuar. Además, cuidar la privacidad en las redes sociales, ajustando configuraciones adecuadamente, ayuda a protegerse de personas con malas intenciones. Padres, educadores y organizaciones deben participar activamente en la prevención, creando un ambiente de confianza donde las víctimas puedan hablar. Programas de concientización y políticas claras en escuelas y trabajos son esenciales para abordar el problema

7. Biografía de autores

PhD. Luis Oswaldo Ordoñez Pineda

DIRECTOR DEL GRUPO DE INVESTIGACIÓN DERECHOS DIGITALES Y PROTECCIÓN DE DATOS PERSONALES.

Doctor (PhD) en Ciencias Sociales y Jurídicas por la Universidad de Cádiz - España. Maestro en Derecho por la Universidad Nacional Autónoma de México. Abogado y Especialista en Derecho Procesal Penal por la Universidad Técnica Particular de Loja. Docente - Investigador de la Universidad Técnica Particular de Loja en la cátedra de Derecho Informático y Protección de Datos Personales. Coordinador del Grupo de Investigación: "Derechos Digitales y Protección de Datos Personales" en la Universidad Técnica Particular de Loja.

Orcid: https://orcid.org/0000-0002-0262-2212
Email: loordonez@utpl.edu.ec
https://investigacion.utpl.edu.ec/loordonez

Mgtr. Andrea Catalina Aguirre Bermeo

Docente Universitario Titular del Departamento de Ciencias Jurídicas de la Modalidad Presencial y a Distancia de la Universidad Técnica Particular de Loja. Abogado de los Juzgados y Tribunales de la República, Especialista Superior en Tributación, Magíster en Derecho con mención Derecho Tributario. Funcionaria Judicial de la Sala de lo Contencioso Tributario de la Corte Nacional de Justicia, Procuradora de la Dirección Zonal 7 del Servicio de Rentas Internas, Grupo de Investigación Derechos Digitales y Protección de Datos Personales.

Orcid: https://orcid.org/0000-0003-3993-1999
email: acaguirre28@utpl.edu.ec
https://investigacion.utpl.edu.ec/acaguirre28

Mgtr. Sara Auxiliadora Cabrera Jiménez

Máster Universitario en Propiedad Intelectual y Derecho de las Nuevas Tecnologías por la Universidad Internacional de La Rioja, Abogada de la Universidad Técnica Particular de Loja, docente autora y tutora de algunos componentes educativos como: Práctica Procesal Laboral I, Derecho Civil I, Personas y Familia, Filosofía del Derecho, Derecho Laboral, Nuevas Tecnologías Aplicadas al Derecho, Introducción al Derecho, Metodología de Estudio, Investigación, Manejo de TIC aplicadas a la Educación, Técnicas y Metodología de estudio para docentes. Experiencia de 19 años de servicio en la Universidad Técnica Particular de Loja.

Orcid: https://orcid.org/0009-0004-4956-1471
email: scabrera@utpl.edu.ec

Mgtr. Denisse Elizabeth Condolo Pardo

Docente investigadora del Departamento de Ciencias Jurídicas de la Modalidad Presencial y a Distancia de la Universidad Técnica Particular de Loja. Abogada de los Juzgados y Tribunales de la República del Ecuador por la Universidad Técnica Particular de Loja. Magíster en Propiedad Intelectual y Derecho de las Nuevas Tecnologías por la Universidad Internacional de la Rioja – España.

Orcid: https://orcid.org/0009-0005-1500-2900
email: decondolo@utpl.edu.ec
https://investigacion.utpl.edu.ec/decondolo

Mgtr. Jorge Luis Cueva Flores

Magíster en Derecho Civil y Procesal Civil por la UTPL, Abogado de la República del Ecuador por la UTPL, Abogado de la Procuraduría Universitaria UTPL. Docente Universitario del Departamento de Ciencias Jurídicas de la Modalidad Presencial y a Distancia de la Universidad Técnica Particular de Loja, Miembro del Grupo de Investigación Derechos digitales y protección de datos personales. Subdirector de la Carrera de Derecho modalidad en línea UTPL.

Orcid: https://orcid.org/0000-0002-0365-0450.
email: jlcuevaxxx@utpl.edu.ec

Mgtr. María Augusta Herrera Vásquez

Título de Abogada - Universidad Técnica Particular de Loja Egresada de la Maestría en Derecho Laboral y Seguridad Social - Universidad Católica de Cuenca Docente de la Universidad Técnica Particular de Loja - Pregrado Modalidad Presencial y Modalidad Abierta y a Distancia Mediadora del Centro de Análisis y Resolución de Conflictos de la Universidad Técnica Particular de Loja Abogada de la Compañía Constructora Técnica General de Construcciones S.A. en el área Laboral y en Proyecto de Indemnizaciones Procuradora Judicial de la Compañía Constructora del Pacífico S.A. Procuradora Judicial del Consorcio CONSERBEG S.A. y Luis Rodríguez Asociados

Orcid: https://orcid.org/0000-0002-7563-2518
email: maherrera@utpl.edu.ec
https://investigacion.utpl.edu.ec/maherrera

Mgtr. Juan Andrés Jaramillo Valdivieso

Abogado graduado en el 2010. Magíster en Derecho Civil y Procesal Civil en el 2015. En la actualidad realiza estudios de Doctorado en Derecho en la Universidad de La Coruña de España. Trabajó en diversos estudios jurídicos tanto de Quito (Fernández & Calderón, Charpentier & Jaramillo), fue abogado de Standard Consultoría, y ejerció distintos cargos en el Consejo de la Judicatura. Desde el 2016 es profesor en la Universidad Técnica Particular de Loja de diversos componentes relativos al Derecho Privado. Ha sido profesor de posgrado en la Uniandes y en la UTPL. Tiene numerosas publicaciones en temas de Derecho Privado. Miembro del Grupo de Investigación Derechos Digitales y Protección de Datos Personales. Desde septiembre del 2017 maneja un blog de Derecho Civil:

https://derechocivilecuadorblog.wordpress.com/.
Orcid: https://orcid.org/0000-0003-0940-2287
email: jajaramillo@utpl.edu.ec.

Mgtr. Carlos Rubén Mogrovejo Riofrío

Investigador Predoctoral (Doctorado en Derecho y Ciencia Política) por la Universidad de Barcelona. Abogado por la Universidad San Francisco de Quito. Magíster en Protección de Datos Personales por la Universidad Internacional de la Rioja. Magíster en Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información por la Universidad Carlos III de Madrid. Docente invitado y miembro del Grupo de Investigación: "Derechos Digitales y Protección de Datos Personales" en la Universidad Técnica Particular de Loja. Coordinador del Máster en Contratación Pública Avanzada por la Universidad de Barcelona.

Orcid: 0009-0008-4113-6031
https://es.linkedin.com/in/carlos-mogrovejo-riofrio

Mgtr. Paul Javier Moreno Quizhpe

Abogado de los juzgados y tribunales de la República por la Universidad Internacional del Ecuador Sede Loja, Magíster en Derecho Civil y Procesal, por la Universidad Técnica Particular de Loja, Docente de las asignaturas de pregrado modalidad a distancia: Derecho Societario, Legislación Mercantil y Societaria, Introducción al Derecho, Derecho Civil I Personas y Familia, Derecho Procesal Civil I e Investigación Jurídica, docente de pregrado modalidad presencial. Director de la Maestría en Derecho mención Derecho Procesal.

Orcid: 0009-0008-4782-6543
Email: pjmoreno2@utpl.edu.ec
https://investigacion.utpl.edu.ec/pjmoreno2

Mtra. Maritza Elizabeth Ochoa Ochoa

Maestra en Derecho con Mención Honorífica, por la Universidad Nacional Autónoma de México, Magíster en Desarrollo Comunitario por la Universidad Nacional de Loja, Abogada de la Republica del Ecuador por la Universidad Técnica Particular de Loja, Ingeniera Comercial por la Universidad Nacional de Loja, Mediadora Familiar en Procesos Sistémicos por la Pontificia Universidad Católica del Ecuador, Docente de grado y posgrado de la Universidad Técnica Particular de Loja, miembro del grupo de investigación Derechos digitales y protección de datos personales, autora de libros y artículos científicos, experiencia de 15 años en desarrollo de proyectos de investigación, vinculación e intervención social

Orcid: https://orcid.org/0000-0002-7196-9914
Email: meochoa@utpl.edu.ec
https://investigacion.utpl.edu.ec/meochoa

Mtra. Emma Patricia Pacheco Montoya

Maestra en Derecho por la Universidad Nacional Autónoma de México (Mención honorífica); Especialista y Magister en Derecho Empresarial de la Universidad Técnica Particular de Loja; Diploma Superior Las Nuevas Tecnologías de Información y Comunicación y su aplicación en la Práctica Docente Ecuatoriana de la Universidad Nacional de Loja; Doctora en Jurisprudencia, Abogada y Licenciada en Ciencias Sociales Políticas y Económicas de la Universidad Nacional de Loja; Docente de Pregrado y Post Grado de la Universidad Técnica Particular de Loja en la Modalidad Presencial y Abierta y a Distancia.

Orcid: https://orcid.org/0000-0002-6606-8855
Email: eppacheco@utpl.edu.ec
https://investigacion.utpl.edu.ec/eppacheco

PhD. Lucía Puertas Bravo

Ecuatoriana, es Licenciada en Ciencias Sociales Políticas y Económicas, Abogada y Doctora en Derecho, por la Universidad Nacional de Loja, Ecuador. Doctora en derecho (PhD) por la Universidad Nacional de Educación a Distancia, UNED, España, obteniendo la calificación de sobresaliente cum laude además de premio extraordinario de doctorado en el año 2013. Ex becaria de Fundación Carolina, estancia postdoctoral en el Departamento de Educación Comparada e Historia de la Educación de la Universidad de Valencia, España en el año 2018.

Desde agosto de 2003 docente del Departamento de Ciencias Jurídicas de la UTPL institución en la que ha desempeñado varios cargos como Directora del Centro de Investigación, Transferencia de Tecnologías, extensión y servicio, "Gestión Legal", desde el año 2009 hasta octubre de 2012 y como Directora de Investigación y Postgrado desde noviembre de 2012 hasta el 31 de agosto de 2023.

Orcid: https://orcid.org/0000-0002-2173-8966
Email: lpuertas@utpl.edu.ec
https://investigacion.utpl.edu.ec/lpuertas

Mgtr. Santiago Israel Puertas Monteros

Abogado de los Tribunales y Juzgados de la República del Ecuador, Magíster en Derecho Civil y Procesal Civil, Secretario Auxiliar de la Notaría Quinta Cantonal de Loja, Secretario Auxiliar de la Notaría Séptima Cantonal de Loja, Secretario Auxiliar de la Notaría Octava Cantonal de Loja, Secretario Auxiliar de la Notaría Sexta Cantonal de Loja, Docente de la Universidad Internacional del Ecuador – Sede Loja, Secretario Abogado de la Facultad de la Salud Humana de la Universidad Nacional de Loja y Docente de la Universidad Técnica Particular de Loja.

Orcid: https://orcid.org/0009-0006-8029-875X
Email: sipuertas@utpl.edu.ec
https://investigacion.utpl.edu.ec/sipuertas

Mgtr. María Carolina Sacoto Romo

Doctoranda en Derecho en la Universidad de Buenos Aires. Máster en Propiedad Intelectual y Derecho de las Nuevas Tecnologías por la Universidad Internacional de la Rioja. Abogada por la Universidad Técnica Particular de Loja e Ingeniera Comercial por la Universidad del Azuay. Docente de grado y de posgrado en la maestría de Derecho Constitucional de la Universidad Técnica Particular de Loja. Miembro del grupo de investigación en Derechos Digitales y Protección de Datos Personales. Autora y Coautora de varios artículos académicos y capítulos de libros con publicaciones nacionales e internacionales.

Orcid: https://orcid.org/0000-0002-8799-8947
Email: mcsacoto1@utpl.edu.ec
www.linkedin.com/in/carolina-sacoto

Agradecimiento

Expresamos nuestro reconocimiento a la Universidad Técnica Particular de Loja, en especial al Vicerrectorado de Investigación, a la Facultad de Ciencias Jurídicas y Políticas; y, al Departamento de Ciencias Jurídicas, por su invaluable apoyo en la ejecución del proyecto integrador "Ciberacoso en las comunidades de aprendizaje".

La intervención de las instancias antes señaladas ha sido fundamental para impulsar la investigación como un pilar en la generación y transferencia del conocimiento. Asimismo, su compromiso con la vinculación con la sociedad ha permitido abordar una problemática actual con impacto directo en nuestras comunidades educativas. Este proyecto refleja también el esfuerzo constante por fortalecer el desarrollo académico y contribuir al bienestar social desde una perspectiva ética y profesional.

ISBN-13: 978-9942-26-364-3

9 789942 263643