FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

LOS DESAFÍOS DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE LOS MENORES EN SU ENTORNO FAMILIAR

TRABAJO FIN DE GRADO DE TRABAJO SOCIAL

Autora: María Costa Rodríguez
5º Doble Grado en Criminología y Trabajo Social

Director: D. Alberto Serrano Molina

Madrid
Abril 2024

A mi madre, por brindarme siempre su ayuda
y por no perder nunca paciencia.

RESUMEN

El presente trabajo trata de abordar desde una revisión bibliográfica de la normativa aplicable de los menores de edad en el entorno digital y de algunos riesgos que estos enfrentan en internet, como el grooming online, el sexting, el *ciberbullying*, las compras sin permiso paterno y el contenido inadecuado en redes sociales. Nos centraremos en cómo abordar estos dentro de su entorno familiar. Además, se intenta encontrar cabida al trabajo social dentro de este ámbito.

Palabras clave: *ciberseguridad, menores, riesgos en internet, trabajo social, grooming, sexting, ciberbullying.*

ABSTRACT

This work attempts to address, from a bibliographic review, the regulations applicable to minors in the digital environment and some risks that they face on the Internet, such as online grooming, sexting, cyberbullying, purchases without parental permission and inappropriate content on social networks. We will focus on how to address these within your home environment. In addition, an attempt is made to find a place for social work within this area.

Key words: *cybersecurity, minors, risks on the internet, social work, grooming, sexting, cyberbullying.*

ÍNDICE

LISTA DE ABREVIATURAS

CE: Constitución Española.

CC: Código Civil.

TIC: Tecnologías de la Información y las Comunicaciones.

CTIM: ciencia, tecnología, ingeniería y matemáticas.

IA: Inteligencia Artificial.

UNESCO: Organizaciones de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

MAETD: Ministerio de Asuntos Económicos y Transformación Digital de España.

CP: Código Penal.

RAE: Real Academia Española.

INCIBE: Instituto de Cierseguridad Español.

TS: Tribunal Supremo

I. INTRODUCCIÓN

En la era digital, el acceso a Internet y las tecnologías de la información se ha vuelto una parte imprescindicle de la vida cotidina, especialmete para los menores, quienes crecen inmersos en un entorno digital desde su nacimiento. La omnipresencia de las plataformas en línea y de los dispositivos que permiten conectase a estas ofrece a los jóvenes oportunidades educativas, sociales y recreativas. Sin embargo, esta misma conectividad también conlleva una serie de desafios y riesgos, especialmente en lo que respecta a su protección.

Los menores son vulnerables a una amplia gama de amenazas en línea, por lo que los padres se ven obligados a enfrentarse diariamente a desafíos relacionados con la ciberseguridad en el entorno familiar. ¿Cómo proteger adecuadamente a los menores? ¿De qué modo equilibrar la autonomía y el acceso a la tecnología con la necesidad de supervisar y proteger a sus hijos de los peligros en línea? Estas son las preguntas a las que deben dar respuesta continuamente.

A tal fin y como vamos a poder mostrar en este trabajo, existen políticas y normas jurídicas destinadas a abordar estos problemas. Todas ellas deben ser lo suficientemente flexibles y con capacidad de adaptación para mantenerse al día con los rápidos avances tecnológicos y los nuevos desafíos emergentes.

1. Objetivos e Hipótesis

En el presente estudio se plantea como objetivo general explorar desafíos de la ciberseguridad en la protección de los menores en su entorno familiar.

Los objetivos específicos son los siguientes:

- Examinar las políticas y regulaciones existentes relacionadas con la protección de los menores en línea y en las redes sociales.
- Analizar los principales riesgos y amenazas que enfrentan los menores en el ámbito digital.

Las hipótesis que se proponen son las siguientes:

- H_1: Cuánto más expuestos estén los menores al uso de redes sociales es más probable que tengan experiencias negativas en línea.

- H_2: Cuantas más políticas y regulaciones haya más efectiva será la protección de los menores en línea.

2. Metodología

La metodología seleccionada para realizar la presente investigación ha sido la revisión bibliográfica, esta se llevará a cabo mediante un enfoque sistemático que abarcará diversas fuentes de información, incluyendo bases de datos académicas, revistas científicas, libros especializados y documentos gubernamentales relacionados con la ciberseguridad y la protección de los menores en línea.

Se han establecido criterios de inclusión y exclusión para la selección de los estudios y documentos relevantes, priorizando aquellos que aborden directamente los desafíos de la ciberseguridad en el entorno familiar. Para su localización he utilizado términos clave relacionados con políticas y regulaciones, riesgos cibernéticos, y uso del internet por los menores.

II. LAS PERSONAS MENORES DE EDAD Y LA SOCIEDAD DIGITAL

De acuerdo con nuestra Constitución (art. 12 CE) y con el Código civil español (art. 240 CC), una persona alcanza la mayoría de edad a los dieciocho años. Por ende, las personas que tienen la condición de menores de edad son aquellas que no han alcanzado dicha edad.

Entre los principales retos a los que se enfrenta la sociedad actual son los peligros que para las niñas, los niños y los adolescentes representa su acceso a la información que existe en internet. Nacionas Unidas ha afirmado a este respecto que “sin duda la juventud es la mayor impulsora de la conectividad a nivel mundial. Un 79 % de los jóvenes de entre 15 y 24 años tenían conexión a internet en 2023, en comparación con el 65% del resto de la población mundial.

Los niños también pasan más tiempo en línea que nunca. De hecho, están llegando a edades cada vez más tempranas. En todo el mundo, un niño se conecta a internet por primera vez cada medio segundo. Todo ello ha creado oportunidades sin precedentes para

que niños y jóvenes se comuniquen, aprendan, socialicen y jueguen, exponiéndolos a nuevas ideas y fuentes de información más diversas. Pero a la vez que el entorno digital ofrece oportunidades, también conlleva serios riesgos…" (Naciones Unidas, 2024).

Por este motivo es importante que definamos qué es la ciberseguridad. Esta engloba la práctica de proteger sistemas informáticos, redes, programas y datos contra amenazas, ataques y accesos no autorizados. Implica la implementación de medidas y tecnologías diseñadas para preservar la integridad, confidencialidad y disponibilidad de la información digital, con el objetivo de prevenir daños a los sistemas y garantizar el correcto funcionamiento de las operaciones en el entorno cibernético (Giant, 2016).

Asímismo, esta disciplina también abarca el uso seguro y responsable de los productos de la tecnología de la información y la comunicación (TIC), como Internet, dispositivos móviles, herramientas de comunicación y dispositivos tecnológicos diseñados para almacenar, compartir o recibir información, como teléfonos móviles y ordenadores, entre otros (Giant, 2016).

La revolución tecnológica del siglo XXI ha conllevado que los infantes hayan experimentado una transformación profunda en su forma de vivir, aprender y relacionarse, impulsada por la rápida difusión de la tecnología digital. Esta generación se ha desarrollado en un entorno donde los dispositivos electrónicos, como ordenadores, teléfonos, videojuegos y la televisión, son omnipresentes desde una temprana edad. En contraste con las generaciones anteriores, cuyo acceso a la tecnología era limitado o inexistente en su juventud, los jóvenes y menores de edad actuales han adoptado naturalmente estas herramientas como parte integral de sus vidas (Prensky, 2001).

Esta inmersión tecnológica se refleja en las actividades diarias que realizan, puesto que dedican una cantidad significativa de tiempo a actividades digitales como conversar por mensajería instantánea, el consumo de contenido en línea y el uso de redes sociales. Es común que los menores pasen más tiempo interactuando con pantallas que leyendo libros o realizando actividades tradicionales.

Además, la forma en que estos niños procesan la información es notablemente diferente a la de sus predecesores. Han desarrollado habilidades para buscar, filtrar y

analizar datos en línea de manera rápida y eficiente, gracias a su exposición continua a una gran cantidad de información digital. Esta habilidad para navegar por los datos en línea ha llevado a una mayor fluidez en el manejo de la tecnología, superando a menudo a la de sus progenitores y profesores (Prensky, 2001).

La tecnología se ha convertido en una parte imprescindible en la vida de los menores, moldeando no solo su forma de aprender, sino también su manera de comunicarse, socializar y entender el mundo que los rodea. Esta brecha digital entre los niños y sus padres plantea desafíos significativos en el ámbito educativo, que requieren una adaptación continua de los métodos de eduación y un mayor énfasis en la integración de la tecnología en el hogar para satisfacer las necesidades de esta nueva generación de jóvenes digitales (Prensky, 2001).

Debido a este auge de la tecnología Marc Prensky (2001) creó el concepto “nativos digitales”, con el ánimo de denorminar a aquellas personas que se han criado en el entorno digital desde su nacimiento

Así es, las redes sociales están en todas partes y se han convertido en una parte esencial de la vida diaria para millones de personas en todo el mundo. Estas plataformas digitales son fáciles y gratuitas, lo que las hace accesibles para una amplia diversidad de personas. Cuando se suscriben a una red social, los usuarios pueden crear perfiles personalizados que compartir con otros y explorar perfiles de individuos con las que deseen conectarse.

En estos perfiles los usuarios tienen la opción de agregar diferentes tipos de información personal, que van desde datos básicos como el nombre y la ubicación hasta detalles más específicos como antecedentes educativos, laborales, intereses, pasatiempos y preferencias. Asimismo, las fotografías suelen formar parte integral de estos perfiles, lo cual les permite mostrar su vida y personalidad de manera visual.

La capacidad de agregar "amigos" o "seguidores" es una de las características distintivas de las redes sociales, lo que permite a los usuarios conectarse con otras personas y compartir contenido. Esta conexión puede ser bien de doble dirección, lo que implica que ambos usuarios pueden ver y compartir información entre sí, o bien de de

una sola, donde uno de los usuarios sigue al otro pero no necesariamente recibe reciprocidad en la relación.

Esta nueva modalidad de relaciones interpersonales ha heche que en los últimos años, las redes sociales hayan experimentado un desarrollo vertiginoso en popularidad. A nadie le resultan desconocidas plataformas como Facebook, X (o más conocido como Twitter), Instagram o LinkedIn. Cada una de ellas ofrece un conjunto exclusivo de características y funciones que atraen a distintos tipos de usuarios.

Como anunciábamos al principio de nuestra exposición, la utilización de las redes sociales aunque tienen beneficios obvios, también conlleva riesgos y desafíos. Por ejemplo, los jóvenes tienden a acumular un gran número de "amigos" en sus redes sociales, lo que puede resultar una exposición excesiva de información personal a extraños o conocidos superficiales. La falta de comprensión sobre la configuración adecuada de privacidad también puede llevar a perfiles públicos que exponen información sensible (como su ubicación) al alcance de cualquier persona en la red, lo cual podría comprometer la seguridad y privacidad del usuario (Giant, 2016).

Otra de las manifestaciones del avance continuo de la tecnología es la mensajería instantánea. Se trata de una herramienta digital que permite la comunicación instantánea entre usuarios a través de computadoras o teléfonos móviles con acceso a Internet. Los usuarios se registran mediante su correo electrónico o número de teléfono y agregan contactos utilizando las direcciones de correo electrónico o números de teléfonos de otras personas. Si los contactos están registrados en el mismo servicio de mensajería, los usuarios pueden comunicarse en tiempo real enviando mensajes de texto, por llamadas o através de videollamadas (Giant, 2016).

Sin duda, esta herramienta digital cuenta con aspectos positivos como facilitar el contacto instantáneo y gratuito con personas en cualquier parte del mundo. A la reducción de costes de las llamadas telefónicas internacionales, debemos añadir como ventajas la posibilidad de mantener múltiples conversaciones privadas simultáneas, con la capacidad de compartir fácilmente fotografías, videos y documentos.

Sin embargo, también debemos ser conscientes acerca del riesgo de agregar a demasiadas personas como contactos, lo que puede conducir a conversaciones no deseadas o incluso acosadoras. Al igual que en las redes sociales, la mensajería puede ser utilizada con fines ilícitos.

En ocasiones, incluso, la interpretación precisa de las intenciones y emociones detrás de los mensajes puede verse dificultada por la ausencia de señales no verbales, como expresiones faciales y lenguaje corporal.

En otro orden de cosas, los niños pueden experimentar consecuencias físicas y emocionales debido al uso excesivo de Internet. Se ha comprobado en diversas investigaciones que el uso prolongado de dispositivos electrónicos puede causar problemas físicos como la obesidad y los dolores musculares, así como afectar la salud mental con problemas como la ansiedad y la depresión. Dado que los niños utilizan cada vez más dispositivos electrónicos desde una edad temprana, estas preocupaciones son, a mi juicio, especialmente relevantes. Dentro de este contexto, el uso constante del Internet y de las redes sociales ha acarreado una serie de patologías nuevas. Entre estas se encuentra el cibermareo (fatiga visual y nauseas tras el uso prolongado de tecnologías), el síndorme de la llamada imaginaria (alucinación de que el teléfono suena o vibra), la nomofobia (miedo irracional a no tener el teléfono móvil o a no poderse conectar a internet), el FOMO (ansiedad social caracterizada por querer mantenerse activo en redes sociales) y la cibercondría (trastorno obsesivo compulsivo por diagnosticarse de enfermedades a través de Internet) (López-Iglesias et al, 2023).

Para abordar eficazmente todo estos desafíos consideramos que, en primer lugar, es necesario conocer las normas jurídicas que protegen a los menores ante este entorno digital y, en segundo lugar, comprender por qué los niños y jóvenes utilizan inapropiadamente los dispositivos informáticos y cuáles son sus implicaciones. Estos van a ser los próximos objetivos de mi investigación.

III. LOS DERECHOS DE LAS PERSONAS MENORES DE EDAD. NORMATIVA APLICABLE

1. Consideraciones Generales

Los derechos de las personas menores de edad constituyen un aspecto fundamental en el marco legal de cualquier sociedad. Los mismos están diseñados para proteger su bienestar, su desarrollo e integridad, reconociéndolos como individuos con necesidades, intereses y capacidades propias.

La normativa aplicable varía según el país, pero suele estar fundamentada en instrumentos internacionales como la Convención sobre los Derechos del Niño de las Naciones Unidas. Esta convención establece un conjunto de derechos fundamentales que deben ser respetados y protegidos en todas las circunstancias, incluyendo el derecho a la vida, la salud, la educación, la protección contra la violencia, la explotación y el abuso, entre otros.

Como vamos a poder comprobar, además de los instrumentos internacionales, los países, como el nuestro, cuentan con leyes y políticas específicas que garantizan y promueven los derechos de los menores y establecen medidas de protección especial en el ámbito de las redes sociales.

Es importante destacar que los derechos de las personas menores de edad deben ser abordados de manera integral y considerando su interés superior en todas las decisiones y acciones que les afecten. Esto implica no solo garantizar su protección legal y física, sino también promover su participación activa en los asuntos que les conciernen y asegurar que sus opiniones sean tenidas en cuenta de manera significativa.

A mi juicio, los derechos de las personas menores de edad son un pilar fundamental en la construcción de sociedades justas y equitativas, y su protección y promoción deben ser una prioridad en la legislación y las políticas públicas de cualquier país.

2. La regulación fuera de la Unión Europea

2.1. Comité de los Derechos del Niño: Observación General núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital

El Comité de los Derechos del Niño ofrece una explicación detallada sobre cómo los Estados partes deben abordar diversos aspectos para garantizar el cumplimiento efectivo de los derechos de los menores en el entorno digital y orienta sobre medidas legislativas, normativas y de otra índole dirigidas a tal objetivo y que han de estar presididas por una serie de principios generales, tales como la no discriminación; el interés sueperior del menor; el derecho a la vida, a la supervivencia y al desarrollo y el respeto de las opiniones de los niños (Naciones Unidas, 2021).

Los Estados deben reconocer y respetar el desarrollo progresivo de las capacidades del niño, especialmente en el entorno digital, donde su participación es más independiente. Al diseñar medidas de protección y acceso al entorno digital resulta crucial considerar las diferencias de edad y etapa de desarrollo en la que se encuentran los menores, teniendo siempre en cuenta los derechos y libertades de éstos en dicho entorno. Además, se debe encontrar un equilibrio entre la evolución de los niños y su nivel de autonomía, y la importancia de garantizar entornos seguros que apoyen el ejercicio de sus derechos. Los proveedores de servicios digitales deben adaptarse a esta evolución para ofrecer servicios que se ajusten a las capacidades en desarrollo de los niños (Naciones Unidas, 2021).

Los Estados también tienen la responsabilidad de apoyar a padres y cuidadores en la crianza de los niños, promoviendo su conciencia sobre la importancia de respetar su autonomía y privacidad lo que incluye proporcionarles recursos y conocimientos digitales (Naciones Unidas, 2021).

2.2. Organizaciones de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO): Directrices para la gobernanza de las Plataformas

La UNESCO ha establecido recientemente unas directrices, con el objetivo de establecer un marco para salvaguardar el derecho a la libertad de expresión en la gobernanza de las plataformas digitales, asegurando al mismo tiempo el acceso a la información y el respeto a los derechos humanos (UNESCO, 2023)

Estas Directrices se basan en la normativa internacional de derechos humanos, promoviendo la diversidad cultural y de contenidos. Sirven como un recurso para varias partes interesadas, incluyendo responsables de políticas públicas, organismos reguladores, plataformas digitales, sociedad civil y medios de comunicación. Se espera que contribuyan a la construcción de una gobernanza digital centrada en el ser humano (UNESCO, 2023).

Además, están diseñadas para contribuir a los procesos en curso en las Naciones Unidas, como la implementación de propuestas en "Nuestra Agenda Común", la preparación de la Cumbre para el Futuro en septiembre de 2024 y la revisión de la Cumbre Mundial sobre la Sociedad de la Información, entre otros (UNESCO, 2023).

3. La regulación en la Unión Europea

3.1. Comisión Europea Comunicación al parlamento europeo, al consejo, al comité económico y social europeo y al comité de regiones: Una década digital para os niños y jóvenes: la nueva estrategia europea pata una internet mejor para los niños (BIK+). Día 11 de año 2022.

En los últimos años, la Unión Europea ha prestado una especial atención a la protección de los derechos de los niños en el mundo digital a través de la aprobación leyes e impulso de políticas que deberán ser adaptadas y actualizadas a medida que aparezcan nuevas amenazas o o evolucionen los avances y las tecnologías. Por ejemplo, la IA impacta y seguirá teniendo un gran efecto en los niños y sus derechos, como por ejemplo en la educación, el entretenimiento y la atención médica (Comisión Europea, 2022).

La Comisión Europea (2022) ha establecido una serie de acciones clave para promover un entorno en línea más seguro y accesible para los niños. Esto incluye la adopción de una estrategia actualizada para una "Internet mejor para los niños", así como la facilitación de un proceso liderado por los propios niños para desarrollar principios que la industria tecnológica deberá promover y respetar. Además, se está promoviendo el desarrollo y la utilización de las TIC accesibles para niños con discapacidad, a través del reconocimiento de voz y el subtitulado opcional, no solo en plataformas digitales, sino también en conferencias y actos oficiales de la Comisión Europea. Otras medidas incluyen garantizar la plena implementación del Acta Europea de Accesibilidad e

intensificar la lucha contra el abuso sexual infantil mediante la propuesta de legislación que obligue a los proveedores de servicios en línea a detectar y comunicar material relacionado con este tipo de abuso.

Asimismo, la Comisión Europea (2022) ha solicitado a los Estados miembros que adopten medidas concretas para garantizar la igualdad de acceso a las herramientas digitales y la conexión a internet de alta velocidad para todos los niños. Se enfatiza en el apoyo al desarrollo de competencias digitales básicas a través de un marco establecido para los ciudadanos y en la promoción de la alfabetización mediática en el ámbito educativo, permitiendo que los niños puedan evaluar críticamente el contenido en línea y detectar la desinformación. Dentro de este contexto, se promueve el respaldo a iniciativas como los centros para una internet más segura y líneas de asistencia a la infancia, facilitando vías de comunicación en línea seguras y efectivas. Además, se busca fomentar la participación equitativa de niños y niñas en áreas de estudio CTIM, eliminando estereotipos de género para garantizar la igualdad de oportunidades en el mercado laboral digital.

Finalmente, la Comisión Europea (2022) insta a las empresas de tecnologías de la información y la comunicación (TIC) a adoptar acciones concretas para proteger los derechos de los niños en el entorno digital. Se les solicita que integren los derechos de los niños, como la privacidad, la protección de datos personales y el acceso a contenido adecuado para su edad y para niños con discapacidad, en sus productos y servicios digitales desde el diseño y por defecto. Además, se les exhorta a proporcionar herramientas a los niños y a los padres para controlar su tiempo y comportamiento en línea, protegiéndolos de los efectos nocivos del uso excesivo y la adicción a productos digitales. Por último, se les insta a fortalecer, de una parte, las medidas para reaccionar ante contenidos nocivos y comunicaciones comerciales inadecuadas, mediante canales de notificación y bloqueo fáciles de usar, así como herramientas eficaces de verificación de la edad. Y, de otra, a continuar con los esfuerzos dirigidos a detectar, denunciar y eliminar contenidos ilícitos en línea (por ejemplo, el el abuso sexual de menores), de sus plataformas y servicios.

3.2. Parlamento y Consejo europeos: Reglamento de Servicios Digitales (UE) 2022/2065. Día 19 de octubre de 2022

La protección de los menores en plataformas en línea es un objetivo político fundamental de la Unión Europea. Se establece que una plataforma en línea se considera accesible para los menores cuando sus condiciones generales les permiten activamente utilizar el servicio. Esta accesibilidad puede manifestarse de diversas maneras, como cuando el servicio está específicamente diseñado para ser utilizado por menores, cuando es utilizado mayoritariamente por menores o cuando el proveedor tiene conocimiento de que algunos de los usuarios son menores, lo cual puede deducirse a través del procesamiento de datos personales que revelan la edad (Reglamento de Servicios Digitales 2022/2065).

Los proveedores de estas plataformas en línea tienen la responsabilidad de tomar medidas adecuadas y proporcionadas para proteger a este grupo vulnerable. Entre ellas, por ejemplo, destacamos el diseño de interfaces en línea con altos estándares de privacidad, seguridad y protección de menores por defecto. Asimismo, pueden adoptar normas específicas orientadas a la protección de los menores o participar en códigos de conducta diseñados con ese propósito ((Reglamento de Servicios Digitales 2022/2065).

Es esencial que los proveedores consideren las mejores prácticas y las orientaciones disponibles en este ámbito. Una fuente de orientación importante es la Comunicación de la Comisión titulada "Una década digital para los niños y los jóvenes: la nueva estrategia europea para una internet mejor para los niños (BIK+)", que proporciona directrices valiosas para garantizar un entorno en línea seguro y apropiado para los menores (Reglamento de Servicios Digitales 2022/2065).

Además, se establece una prohibición para los proveedores de plataformas en línea de presentar anuncios basados en la elaboración de perfiles utilizando datos personales del usuario cuando tengan conocimiento razonable de que el usuario es un menor. Esta prohibición se ajusta al Reglamento (UE) 2016/679, específicamente al principio de minimización de datos, el cual establece que los proveedores no deben recopilar, obtener o procesar más datos personales de los necesarios para determinar si el usuario es menor de edad. Esta obligación no debe incentivar a los proveedores a solicitar la edad del usuario antes de utilizar el servicio, y se aplica sin perjuicio del Derecho de la

Unión en materia de protección de datos personales (Reglamento de Servicios Digitales 2022/2065).

4. La Regulación en España

4.1. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Dentro de esta ley hay dos preceptos que recogen cómo se debe abordar la protección de datos personales cuando se trata de un menor. Por un lado, el artículo 7 prevé disposiciones específicas para el tratamiento de datos personales de menores de edad. En primer lugar, se estipula que el consentimiento para dicho tratamiento solo puede fundamentarse en el consentimiento del propio menor si este tiene catorce años o más. Sin embargo, se establecen excepciones a esta regla general, en los casos en que la ley requiera la intervención de los titulares de la patria potestad o tutela para autorizar ciertos actos jurídicos que impliquen el tratamiento de datos (Ley Orgánica 3/2018).

Por otro lado, se ordena que si el tratamiento de los datos de menores de catorce años se basa en su consentimiento, este solo será lícito si también se obtiene el consentimiento del titular de la patria potestad o tutela. Esta medida busca garantizar que los datos de los menores sean tratados de manera responsable y respetuosa, asegurando que los padres o tutores estén involucrados en decisiones que afecten a la privacidad y protección de sus hijos o tutelados (Ley Orgánica 3/2018).

Y, por otro lado, el artículo 84 de la Ley Orgánica aborda la protección de los menores en el contexto de Internet. A este respeto, se establece la responsabilidad de los padres, tutores u otros representantes legales para garantizar que los menores hagan un uso equilibrado y responsable de los dispositivos digitales y los servicios en línea. Esto se hace con el objetivo de asegurar su adecuado desarrollo y preservar su dignidad y derechos fundamentales, especialmente en lo que respecta a la difusión de información personal o imágenes en redes sociales y servicios en línea, donde se prevé la intervención del Ministerio Fiscal para garantizar la protección de los derechos de los menores (Ley Orgánica 3/2018).

4.2. Proposición de Ley Orgánica de refuerzo de las medidas para restringir el acceso de los menores de dieciséis años a la pornografía

El aumento del consumo de pornografía entre menores de edad y sus consecuencias sociales, especialmente el incremento de las agresiones sexuales entre menores, ha generado la necesidad de reforzar legislativamente las medidas destinadas a limitar el denominado "uso problemático de la pornografía". Este tema ha sido objeto de discusión en varias comparecencias de expertos para la renovación del Pacto de Estado contra la Violencia de Género, resaltando el riesgo que implica no abordar la situación de manera urgente (Proposición Ley Orgánica 122/000326).

Una investigación destacada en este contexto es el "Estudio Sobre Pornografía en las Baleares, acceso e impacto sobre la adolescencia", publicado en diciembre de 2022 y liderado por expertos como el Doctor Lluís Ballester y Sandra Sedaño de la Universitat de les Illes Balears. Este estudio examina el acceso a la pornografía de menores desde los ocho hasta los dieciocho años, tanto cualitativa como cuantitativamente, así como el marco legal nacional, europeo e internacional relacionado. También investiga las tecnologías utilizadas por los menores para acceder a contenido sexualmente explícito y propone medidas para bloquear dicho acceso (Proposición Ley Orgánica 122/000326).

Los datos recopilados son preocupantes: un porcentaje significativo de adolescentes tiene su primer contacto con la pornografía a una edad temprana, y la mayoría ha consumido pornografía para los 14 años. Además, una minoría se autoexcluye del consumo a los 16 años. Este consumo problemático de pornografía tiene implicaciones graves, ya que puede influir en la formación de relaciones sexuales y afectivas basadas en la falta de respeto, el desequilibrio de poder y la violencia (Proposición Ley Orgánica 122/000326).

La preocupación aumenta ante la pornografía que retrata violaciones individuales o grupales, que pueden servir como modelos a seguir y se consideran un factor en el aumento de las agresiones sexuales entre adolescentes. Los datos oficiales muestran un aumento significativo en los delitos sexuales cometidos por menores en los últimos años, lo que subraya la necesidad de abordar este problema de manera integral (Proposición Ley Orgánica 122/000326).

En respuesta a esta problemática, se ha propuesto una Ley para reforzar las medidas destinadas a limitar el acceso de los menores de 16 años a la pornografía. Esta ley incluye disposiciones para castigar a los responsables de plataformas que incumplan las obligaciones de control de acceso a contenido para adultos, así como para penalizar el uso de tecnologías como "*deepfake*" para dañar la intimidad de las personas. También propone modificaciones en la Ley de la Comunicación Audiovisual y en la Ley de Protección Integral a la Infancia y la Adolescencia para fortalecer la supervisión y control de contenidos y promover el uso responsable de la tecnología desde edades tempranas (Proposición Ley Orgánica 122/000326).

4.3. Carta de derechos digitales

La carta de derechos digitales también incluye la protección de las personas menores de edad en el entorno digital. En este sentido, se establecen diversas disposiciones para garantizar su seguridad, desarrollo personal y **la** preservación de sus derechos fundamentales (Ministerio de Asuntos Económicos y Transformación Digital de España, 2021).

En primer lugar, se establece que las personas progenitoras, tutoras, curadoras, representantes legales o personas que presten apoyo para el ejercicio de la capacidad jurídica, tienen la responsabilidad de asegurar que los menores hagan un uso equilibrado y responsable de los entornos digitales. Esto se realiza con el fin de garantizar su adecuado desarrollo personal y preservar su dignidad y derechos fundamentales, como la intimidad, el honor, la propia imagen, el secreto de las comunicaciones y el derecho a la protección de datos personales (MAETD, 2021).

Asimismo, se establece que los centros educativos, las Administraciones y cualquier persona física o jurídica involucrada en actividades en entornos digitales que incluyan la participación de menores, están obligados a proteger el interés superior de estos y sus derechos fundamentales. Esto incluye el consentimiento necesario para la publicación o difusión de sus datos personales o imagen a través de servicios de redes sociales, así como el establecimiento de procedimientos para verificar la edad, ofrecer formación e información adecuada sobre los entornos digitales y facilitar el acceso a medios para proteger sus derechos ante acciones lesivas o ilícitas (MAETD, 2021).

Por otra parte, se prohíbe el tratamiento de la información de menores con el fin de establecer perfiles de personalidad en entornos digitales, y se establece su derecho a recibir información suficiente y necesaria sobre el uso responsable de las tecnologías. Además, se reconoce su libertad para expresar opiniones e ideas a través de medios tecnológicos y participar en asuntos públicos que les afecten, potenciando el uso de la tecnología para el pleno desarrollo de estos derechos (MAETD, 2021).

Se impulsa el estudio del impacto en el desarrollo de la personalidad de los menores derivado del acceso a entornos digitales, así como de contenidos nocivos o peligrosos, prestando atención especial a aspectos como la educación afectivo-sexual, las conductas dependientes, la igualdad, la orientación sexual e identidad de género, y los comportamientos antidemocráticos o discriminatorios (MAETD, 2021).

IV. EL USO POR LAS PERSONAS MENORES DE EDAD DE INTERNET Y REDES SOCIALES

1. Consideraciones Generales

El uso de Internet y redes sociales por parte de personas menores de edad es algo que vemos todos los días, y aunque ofrece muchas oportunidades positivas, también presenta una serie de riesgos y desafíos. Uno de los problemas más graves asociados con el mal uso de Internet y redes sociales por parte de los jóvenes es el impacto en su salud mental.

En casos extremos, el mal uso de Internet y redes sociales puede incluso estar relacionado con el suicidio entre los jóvenes. Los estudios han demostrado que el acoso en línea y la exposición a contenido perjudicial pueden aumentar el riesgo de pensamientos suicidas y comportamientos autodestructivos entre los adolescentes.

Es importante reconocer que el uso de Internet y redes sociales no es intrínsecamente negativo, pero es fundamental que los jóvenes sean educados sobre cómo utilizar estas plataformas de manera segura y responsable.

2. Los principales riesgos en internet para las niñas, los niños y los adolescentes

A continuación, voy a proceder al análisis de algunos de los riesgos en internet para los menores de edad, ya que resulta inabordable exponer todos los existentes en un Trabajo Fin de Grado. Los escogidos a tratar han sido el *ciberbullying*, *sexting*, *grooming online*, contenido inadecuado en redes y las compras *online* sin permiso paterno.

El criterio de selección que he seguido ha sido la gravedad y la relevancia que han tomado actualmente en nuestra sociedad.

2.1. Ciberbullying

El término "ciberacoso" fue acuñado por primera vez en 1999. A pesar de no haber un consenso general sobre su definición, todas las diferentes versiones suelen incluir el uso de tecnología digital con el fin de infligir daño repetidamente o acosar (Englader et al., 2017).

Patchin y Hinduja (2006) entendieron como ciberacoso "el daño intencional y repetido infligido a través del uso de computadoras, teléfonos celulares u otros dispositivos electrónicos" y Kowalski et al (2014) lo definieron como "el uso de tecnologías de comunicación electrónica para acosar a otros".

La mayoría de las definiciones de ciberacoso han sido influenciadas por la definición de acoso escolar tradicional, y parece que hay cierta superposición entre el acoso escolar y el ciberacoso (Englader et al., 2017). En el caso de los niños que sufren acoso escolar, el ciberacoso se ha convertido en una extensión de este, ya que ya no se limita únicamente al horario escolar como solía ocurrir antes, sino que se mantiene durante todo el día a través de las redes sociales.

Debido a la relevancia que ha tomado el acoso escolar en la sociedad y a la problemática de que este se haya expandido a través de las redes sociales la Fiscalía General del Estado ha redactado una doctrina sobre el tratamiento del acoso escolar desde el sistema de justicia juvenil.

En esta enfatiza la necesidad de un abordaje integral para este fenómeno y que no se limite a medidas penales o represivas, sino que se incluya acciones preventivas y

rectivas desde la jurisdicción de menores. Se establece que todos los casos deben trartarse con seriedad aunque parezcan casos leves de acoso ya que, si son sostenidos en el tiempo se agravan. Además, se proponen acciones a tomar en el proceso judical, como la de realizar una investigación exhaustiva en la que se incluya el testimonio de la víctima y se contacte con los centros educativos y padres; así como, el evitar estigmatizar al *buller* o *ciberbuller* menor y que las medidas cautelares que se tomen contra de este sean proporcionales a la gravedad de sus actos. También se surgire implementar soluciones extrajudiciales en casos no graves de acoso y reconocer el derecho de la víctima a ser informada y participar en el proceso. Por último, se señala la posibilidad de demandar civilmente a los centros educativos por los daños causados por delitos cometidos por menores bajo su supervisión (Instrucción 10/2005).

No obstante, el fenómeno del *ciberbullying* también requiere un análisis independiente, dado que este también puede darse auqnue no se de *bullying* en el colegio. Cuando el acoso se lleva a cabo exclusivamente a través de *Internet*, los supuestos acosadores no siempre encajan en el estereotipo clásico de abusador de la escuela, sino que pueden ser cualquier persona, de cualquier edad y de cualquier parte del mundo. Además, *internet* permite al ciberacosador ser anónimo, lo que provoca en este una clara distancia emocional con su víctima provocando que aumente la crueldad y gravedad de los ataques (Giant, 2016)

Al igual que no existe consenso en su definición, tampoco lo hay en lo relativo a las clases de ciberacoso. En este trabajo y siguiendo a Willard (2007) voy a exponer siete tipos de ciberacoso. Son los siguientes:

1. Mensajes insultantes (*flaming*): mensajes con rabia, groseros, vulgares, dirigidos a una persona o personas, de forma privada o a un grupo en línea.
2. Hostigamiento (*harassment*): enviar a una persona mensajes ofensivos con intención de intimirarla o molestarla.
3. Denigración: enviar o divulgar en linea rumores o información perjudicial y no verificada sobre una persona, con el propósito de dañar su reputación.
4. Ciberamenazas: mensajes ofensivos que incluyen amenazas de daños físico o emocional, o que sean muy intimidantes.

5. Suplantación de identidad: la acción de hacerse pasar por otra persona y publicar o enviar materiales en línea que puedan dañar la reputación de la persona suplantada.
6. Engaño: el acto de persuadir a una persona para que divulgue información confidencial, como secretos o datos embarazosos, que pueda utilizarse para reenviar a otros en línea.
7. Exclusión: excluir a alguien adrede de un grupo en lína.

El estudio realizado por Del Río et al (2010), en el que se encuestó a 13.000 menores de entre 6 y 18 años concluye que en España el ciberacoso a través de *internet* es un fenómeno de baja incidencia. Apenas un poco más del 10% de los menores son víctimas o perpetradores.

Mientras que, según una encuesta realizada por *Save the Children* en 2019 a 400 jóvenes en toda España, más del 75% de los encuestados informaron haber experimentado violencia en línea durante su infancia, con el 47% experimentando más de un tipo de violencia. El *ciberbulllying* fue el tipo más común, afectando al 40% de los jóvenes encuestados, y generalmente comenzó entre los 8 y los 9 años (Save the Children, 2019).

Tras las encuestas expuestas, se puede apreciar que el ciberacoso ha ganado importancia en la sociedad. Comparando estudios realizados con un intervalo de nueve años acerca del ciberacoso se observa que más menores manifiestan ser víctimas. Este aumento puede atribuirse tanto a un incremento real en el número de víctimas como a una mayor conciencia sobre qué constituye el ciberacoso, o incluso a ambos factores.

2.2. Sexting

El término "*sexting*" es un neologismo de la combinción se la palabra *sex* (sexo) y *texting* (enviar mensajes por dispositivos electrónicos) que ha sido ampliamente aceptado en la literatura de habla hispana, ya que se encuentra añadido en la RAE, y se refiere al acto de enviar, recibir o reenviar mensajes de texto, imágenes o vídeos con contenido sexual explícito, utilizando Internet o teléfonos celulares (Mercado et al, 2016).

Sin embargo no existe a la fecha un consenso sobre las características que debe cubrir un mensaje para considerarse *sexting*. Muchas de estas imágenes se comparten de manera instantánea, sin control a través de las redes sociales, por lo que el uso indebido puede tener consecuencias impredecibles y en la mayoría de los casos, catastróficas (Mercado et al, 2016).

El acto de *sexting* no constituye un delito *per se*, siempre y cuando se trate de una conversación entre adultos que consienten y que luego no difunden ese contenido sin el consentimiento de ambas partes. Sin embargo, la situación es diferente cuando involucra a menores, ya que aunque sean ellos mismos quienes compartan una imagen o video con contenido sexual explícito, lo que están distribuyendo es considerado pornografía infantil. Esto agrava la pena, si el menor involucrado tiene menos de 16 años (art. 189.2ª CP).

El problema es que el envío de imágenes sugerentes sexualmente, ya sea de desnudos o semidesnudos, o de vídeos explícitos se ha vuelto una práctica considerada común entre los adolescentes, quienes la perciben como parte normal de su desarrollo y llevar a cabo esta práctica puede aumentar su popularidad, debido a que en las nuevas generaciones la sensualidad es muy importante en esa etapa de sus vidas, creyendo que esta actividad no les generará ningun tipo de problemas (Mercado et al, 2016).

A pesar de que los adolescentes ahora mismo están más concienciados y cuentan con más información que nunca acerca de los diversos riesgos y peligros asociados a compartir imágenes de sí mismos en redes sociales donde la privacidad no está garantizada, muchos de ellos consideran que están inmunes a las posibles consecuencias negativas (Mercado et al, 2016).

Para comprender este fenómeno se ha de hacer una revisión de los antecedentes, a la omnipresencia de la sexualidad y las imágenes sexualizadas en la sociedad occidental. Esta saturación de mensajes y representaciones sexuales se ha vuelto tan común que muchos de nosotros ni siquiera nos damos cuenta de las tácticas provocativas, reveladoras o degradantes que se utilizan para retratar a hombres y mujeres en la publicidad, la televisión, el cine, los vídeos musicales y los medios impresos y en línea (Giant, 2016).

Los jóvenes, en particular, están aún más acostumbrados a estas imágenes que los rodean a diario. Han crecido en un mundo saturado de sexualidad, donde la sociedad a menudo parece exigir que parezcan maduros y sexualmente dispuestos desde una edad cada vez más temprana (Giant, 2016).

Esta sexualización también se encuentra en la comercialización de servicios y productos para adultos dirigidos a niños, como tiendas que venden ropa interior *sexy* a menores de 12 años, muñecas para niñas con maquillaje y aspecto sexualizado, y el aumento de fiestas de cumpleaños temáticas de cóctel, paseos en limusina y cambios de imagen para niñas de hasta cinco años. Este incremento del marketing dirigido a niños pequeños y su creciente consumismo, especialmente en productos propios de adultos, ha sido denominado por algunos como "pedofilia empresarial", dado el impacto negativo percibido de estas prácticas de venta (Giant, 2016).

Esta exposición tempana y constante de los menores al contenido sexual se manifiesta en el *sexting*. Este puede tener un impacto negativo en la salud mental y bienestar emocional de los jóvenes, puesto que si se comparten sin su consentimiento sus imágenes íntimas y/o vídeos pueden experimentar vergüenza, culpa, ansiedad, depresión e incluso llevarles al suicidio (Giant, 2016).

Por último, el *sexting* plantea diferentes interrogantes dentro de nuestro Ordenamiento Jurídico. En primer lugar, al ubircarse junto al *grooming* se puede creer, erróneamente, que hay una relación entre ambos, lo cierto es que el Tribual Supremo ha considerado el *grooming* como un acto de tipo autónomo, mientras que el *sexting* como un acto preparatorio de pornografía infantil. A su vez, el hecho de que el TS lo nombrase un acto preparatorio también genera discrepancias, ya que las penas se igualan o incluso, pueden superar a las impuestas por un delito de captación de pornografía infantil, siendo incongrunete que se pene con mayor condena un acto preparatorio que un delito consumado. Por lo expuesto, se puede pensar que el sexting, o protege bienes jurídicos que el TS no ha considerado, o bien el legislador ha establecido un rango de penas excesivo para este delito (Gutiérrez, 2020).

2.3. Groomig online

El grooming según el INCIBE (s.f.), se define como "práctica en la que un adulto se hace pasar por un menor en Internet o intenta establecer un contacto con niños y adolescentes que dé pie a una relación de confianza, pasando después al control emocional y, finalmente al chantaje con fines sexuales.".

Los objetivos específicos incluyen tener acceso al niño a través de *internet*, obtener la conformidad del niño y mantener en secreto el abuso del niño para evitar su divulgación. Este proceso sirve para fortalecer el patrón abusivo del delincuente, ya que puede usarse como medio para justificar o negar sus acciones (Whittle, 2013).

Este tipo de comportamientos se encuentra regulado en el artículo 183 de nuestro Código Penal. Se trata de una conducta punible siempre y cuando el menor no haya alcanzado la edad de dieciséis años. Para poder ser constitutivo de un delito contra la libertad sexual, el adulto ha debido utilizar medios tecnológicos para concertar una cita con él (González, 2023).

El *grooming* es un proceso multifacético y complejo, ya que puede resultar difícil establecer dónde comienza y dónde termina. Además, se le añade la imposibilidad de la detección de los *groomers* debido a la heterogeneidad del perfil de estos. Este proceso puede tomar diferentes períodos de tiempo y depende de la personalidad del delincuente y las circunstancias individuales de la víctima (Whittle, 2023).

Según un estudio realizado por Save the Children (2023) sobre 61 niños de entre 6 y 17 años víctimas de *grooming* (reconocidas judicialmente), el 57,4% son de las víctimas resultan ser chicas y el 42,6% chicos, lo que no supone una diferencia significativa, y la edad media se sitúa en 13 años en ambos sexos, hay que tener en cuenta que siempre existe una cifra negra, de la que no conocemos magnitud. Mientras que el perfil del *groomer* resulta ser en un 47,5% desconocidos de la víctima, distribuyéndose el resto enrtre conocidos, profesores, entrenadores y familiares; resulta sorprendete que el 95,1% de estos agresores no cuenta con antecedentes.

A continuación, siguiendo a Whittle, voy a exponer cinco características del *grooming* (Whittle, 2013):

La manipulación es un aspecto principal utilizado por delincuentes sexuales para preparar a menores para el abuso, implica manipulación psicológica, donde el delincuente usa diversos métodos como soborno, adulación, intimidación y regalos para ganar acceso y control sobre la víctima, el tipo de manipulación que use dependerá de las características de la víctima (Whittle, 2013).

La accesibilidad de las víctimas a través de internet ha ampliado el alcance del *grooming*, permitiendo que los delincuentes se conecten con niños sin dejar sus hogares y manteniendo el anonimato (Whittle, 2013).

La construcción de una relación de confianza con la víctima, a menudo a través de la creación de un ambiente íntimo y exclusivo, es crucial en el proceso de *grooming*. Esto se logra mediante la sincronización del comportamiento del delincuente con el del joven y el establecimiento de una conexión basada en intereses comunes (Whittle, 2013).

La introducción gradual de contenido sexual en las conversaciones es una parte central del proceso de *grooming*, normalizando tal comportamiento y aumentando el control del delincuente sobre la víctima. Además, los delincuentes evalúan continuamente el riesgo asociado con el *grooming* de un niño particular, adaptando sus estrategias para evitar la detección y maximizar la explotación (Whittle, 2013).

La decepción también desempeña un papel importante, ya que los delincuentes pueden hacerse pasar por jóvenes en línea para reducir las sospechas de la víctima. Aunque los jóvenes a menudo son conscientes de que están comunicándose con adultos, continúan participando en el riesgo, lo que demuestra la intensidad del proceso de *grooming* y la vulnerabilidad de las víctimas (Whittle, 2013).

A pesar de haber identificado los elementos clave del grooming en línea, aún no se comprende completamente cómo interactúan estos elementos con el comportamiento en línea de los jóvenes. Especialmente, se necesita una mayor exploración de las implicaciones de la accesibilidad y el comportamiento de riesgo de los jóvenes (Whittle, 2013).

El 54,1% de las veces que se ha puesto en conocimiento de las autoridades el *grooming online* ha sido por la madtre de la víctima. Tras haberse denunciado o querellado este delito, el proceso judicial tirene una duración en el 45,9% de 3 años, y en el menor de los casos es de 1 año o, en el peor de los casos, puede alargase incluso a 7 años (Save the Children, 2023).

El proceso judicial puede ser largo y arduo para los menores, por lo que desde Save the Children (2023) propone una intervención desde el ámbito judical para garantizar un tratamiento eficar y atento. La propuesta es la siguiente: creación de juzgados especializados y una fiscalía específica que aborden estos casos junto con la garantía de asistencia letrada conforme a la legislación pertinente. La presencia de equipos técnicos especializados y oficinas de asistencia a las víctimas del delito, al igual que la formación continua de operadores jurídicos. En esta debe ser imprescindible la realización de exploraciones y pruebas preconstituidas, así como la implementación del modelo Barnahus para una atención integral. La coordinación y delimitación de competencias entre los distintos órganos judiciales son también fundamentales para asegurar una respuesta eficaz ante la violencia infantil.

2.4. Contenido inadecuado en redes sociales

Cabe afirmar que existen dos categorías de contenido que se consideran inapropiados. Por un lado, el contenido ilícito, que es el que está relacionado con actividades ilegales (por ejemplo, la pornografía infantil, los contenidos de pedofilia, el racismo o la xenofobia, la apología del terrorismo, la fabricación de bombas, drogas, armas, y actividades asociadas a la ilegalidad: Acabacus Cooperativa, 2019). Y, por otro, lado el contenido nocivo, peligroso o poco saludable que resulta perjudicial para el desarrollo intelectual y emocional de los menores, llegando incluso, en ocasiones, a ser también ilegales. Dentro de esta última categoría cabe incluir la pornografía, los juegos en línea, las apuestas y juegos de azar en *internet*, las comunidades que promueven trastornos alimenticios o el suicidio, entre otros (Acabacus Cooperativa, 2019).

Este tipo de contenido tiene el potencial de causar daño psicológico y emocional a los jóvenes. Esta susceptibilidad se debe a su falta de madurez y autoestima, lo que los hace propensos a ser influenciados fácilmente por estas circunstancias. De hecho, los jóvenes pueden internalizar ciertos contenidos como verdaderos o positivos, adoptando

actitudes perjudiciales como el sexismo, machismo, homofobia, racismo, así como la promoción de trastornos alimenticios, autolesiones, consumo de drogas y participación en retos peligrosos. El acceso a este tipo de contenido inapropiado contribuye a la exacerbación de estos trastornos, ya que los jóvenes carecen de la capacidad crítica necesaria para gestionar los riesgos asociados con estas actividades (Acabacus Cooperativa, 2019).

2.5. Las compras *online* sin permiso

Las compras *online* sin permiso, son aquellas que realizan los menores a escondidas de sus padres, usualmente utilizan el número de tarjeta o cuenta bancaria que tienen los padres registrado y guardado en su dispositivo, o cogen la tarjeta física e introducen manualmente el número (Valero, 2020).

Este comportamiento puede tener diversas implicaciones y riesgos para los menores y sus familias. En primer lugar, puede llevar a problemas económicos, ya que los menores pueden gastar dinero sin tener pleno conocimiento de las consecuencias financieras de sus acciones. Además, estas compras no autorizadas pueden generar conflictos familiares y tensiones entre padres e hijos, especialmente si se descubren después de que se han realizado.

También plantean preocupaciones sobre la seguridad en línea y la privacidad de los datos personales, ya que los jóvenes pueden verse expuestos a estafas en línea o a compartir información sensible durante el proceso de compra.

V. LAS MEDIDAS DE PROTECCIÓN EN EL ÁMBITO FAMILIAR

1. Consideraciones Generales

Con el ánimo de abordar de manera integral los riesgos anteriormente expuestos se proponen unas medidas de protección dentro del entorno familiar, en las que no solo sean los progenitores los que tomen acción, sino que los menores también tengan su propio rol.

Se plantea esta polaridad en la intervención porque al involucrar a los menores de manera activa en la implementación de medidas de protección en el entorno familiar se promueve un sentido de responsabilidad compartida, empoderando, así, a los hijos para que sean agentes activos de su propia responsabilidad en línea.

2. El rol de los progenitores

La familia representa la principal fuente de confianza y autoestima para los niños. En este entorno se practican y modelan las conductas y actitudes que luego se aplican en otros ámbitos. Los padres, deben transmitir valores esenciales, tanto personales, como sociales, ya que estos suponen una gran factor de protección ante los dieversos riesgos que hay en internet. (Labrador et al, 2018).

La relación entre padres e hijos es el factor más importante y protector frente a diversos problemas, incluida la adicción a las redes. La familia desempeña un papel crucial como agente preventivo en el ámbito de las nuevas tecnologías. Aunque su función debe complementarse con la de los centros educativos y otras instituciones, es fundamntal que los padres informan a los niños sobre los riesgos de *internet* y su uso adecuado y responsable. (Labrador et al, 2018).

Para que evitar riesgos en internet se han de realizar una prevención desde el hogar, por lo que Labrador et al (2018) plantea dos formas de implementar medidas de protección, por un lado mediante el fomento de las habilidades sociales del menor, y por otro incorporando en la vida familiar habilidades de comunicación, normas y límites, y, último, pero no menos importante, dar ejemplo a los hijos.

Las habilidades personales que los padres debe potenciar en los hijos son la autoestima, la asertividad, las habilidades sociales y la adecuada resolución de problemas, puesto según afirma Labrador et al (2018) un menor que cuente con todas estas habilidades tendrá menos posibilidades de ser víctima ciberbullying o groomig.

A continuación se expondrán tres habilidades familiares que actuarán como factores de protección según Labrador et al. (2018):

Primero, las habilidades de comunicación familiar. Estas son fundamentales para que los niños se sientan cómodos compartiendo sus experiencias en línea, incluyendo cualquier situación de riesgo que puedan enfrentar. La comunicación y escucha activa implican escuchar activamente sus preocupaciones y brindar apoyo emocional cuando sea necesario sin que se creen discusiones o se impongan castigos, fortaleciendo así el vínculo familiar y la comunicación abierta (Labrador et al., 2018).

Segundo, las normas y los límites. Es fundamental establecer reglas de comportamiento claras y límites definidos, en estas normas se deben crear horarios específicos para el uso de los dispositivos electrónicos, con el fin de establecer un equilibrio saludable entre el tiempo en línea y otras actividades; así como establecer áreas donde se permita su uso (ej. Usar el ordenador en el salón) para que se de una vigilancia natural. Es importante crear un equilibrio en los limites, ya que tanto el exceso como la falta de ellos pueden ser perjudiciales y afectar negativamente el desarrollo de los niños (Labrador et al., 2018).

Y, tercero y último, el ejemplo dado a los niños. En la dinámica familiar, se produce de manera natural uno de los procesos de aprendizaje más significativos: el aprendizaje vicario o por modelado. Los hijos observan el comportamiento de sus padres y aprenden nuevas formas de actuar al observar lo que hacen. Por lo tanto, los padres deben ofrecer un modelo de conducta y actitud coherente en cuanto al uso de las redes sociales y de los dispositivos móviles (Labrador et al., 2018).

Además, desde este trabajo proponemos dos medidas más a implementar en el ámbito familiar. Una es educar a los hijos sobre los riesgos de la actividad en línea, en la que los padres tienes que proporcionarles pautas claras sobre cómo proteger su privacidad y seguridad en internet, así como enseñarles sobre el respeto hacia los demás en línea y la importancia de tratar a los demás con empatía. Y la otra, es que los padres deben mantenerse informados sobre las últimas tendencias y riesgos en línea también es fundamental para así puedan abordar estos desafíos de manera efectiva con sus hijos.

Al tomar estas medidas de protección en el ámbito familiar, los padres no solo están protegiendo la seguridad en línea de sus hijos, sino que también están fortaleciendo

los lazos familiares y promoviendo un uso saludable y responsable de la tecnología en el hogar.

3. El Rol de los Menores

Dado el alto nivel de conocimiento de los jóvenes en el uso de dispositivos digitales, tienen un papel crucial en la creación y difusión de mensajes sobre ciberseguridad. La brecha entre los padres y los hijos en el uso de sistemas informáticos puede resultar en que los más pequeños estén más informados sobre ciertos aspectos, como el uso seguro de redes sociales (Giant, 2016).

Por esto, la educación entre pares puede ser muy efectiva, los jóvenes pueden educar a sus hermanos menores, o en caso de ser hijos únicos pueden educarse entre otros familiares o amigos. Estos pueden compartir su conocimiento sobre la privacidad en línea, la importancia de contraseñas seguras y cómo identificar y evitar posibles peligros en internet. La eduación entre pares suele relutar exitosa, ya que los jóvenes suelen escuchar más a sus hermanos mayores, primos o amigos (Giant, 2016).

VI. LA INTERVENCIÓN DESDE EL TRABAJADO SOCIAL

El Consejo General del Trabajo Social define el trabajo social como “una profesión basada en la práctica y una disciplina académica que promueve el cambio y el desarrollo social, la cohesión social y el fortalecimiento y la liberación de las personas cuyos principios de la justicia social, los derechos humanos, la responsabilidad colectiva y el respeto a la diversidad son fundamentales para el trabajo social”.

Esta definición evidencia que los desafíos de la ciberseguridad atañen directamente a la responsabilidad colectiva y, por ende al Trabajo Social Comunitario con el fin de abordar el reto no solo desde la intervención, sino de la prevención.

El Trabajo Social Comunitario ayuda a la comunidad en la toma de conciencia sobre sus necesidades, su situación y sus posibilidades de cambio. Friedlander en 1978 identifica los siguientes objetivos del Trabajo Social Comunitario (Raya, s.f.):

- Ayudar a los ciudadanos a encontrar los medios necesarios para su bienestar en su entorno social.
- Alentar los esfuerzos cooperadores para perseguir objetivos comunes.
- Construir para los individuos y grupos canales de mutuo entendimiento en la acción común.

Los profesores de la UNED, López y Fernández (2008), ponen de manifiesto la colectividad del ser humano y la necesidad de resolver algunos retos de forma comunitaria y no individual. La necesidad de agruparse para entre todos poder cambiar un entorno estructural. En unas sociedades cada vez más individualistas se hace necesario capacitar a los individuos para trabajar juntos ya que cuánto más individualista sea más vulnerables se vuelven sus individuos.

Un ejemplo de alentar para perseguir objetivos comunes y que nos atañe en este trabajo es la iniciativa surgida en Poblenou que ha generado el movimiento Adolescencia Libre de Móviles. Esta cuenta con la participación de familias y profesionales del ámbito de la educación, la salud y la tecnología cuyo objetivo principal es propiciar un cambio de paradigma para que no se perciba como normal y socialmente instalado proporcionar un *smartphone* a los menores en el paso de primaria a secundaria.

Este grupo se ha movilizado para dar a conocer el impacto del abuso de internet, sus riesgos y sus consecuencias e intentan realizar una difusión lo más amplia posible para poder presionar y lograr una regulación e incluso prohibición para aquellos menores de 16 años en el acceso a dispositivos sin supervisión.

Siguiendo con el foco en la prevención de los riesgos no deseados y posibles desarrollos de conductas adictivas existen programas de ocio alternativo saludable para jóvenes que intenta recuperar el sentido de exploración real, quedar cara a cara con las amistades, salidas a la naturaleza, practicando deportes o compartiendo ocio con sus familias. Disfrutar del tiempo libre de forma saludable es fuente preventiva frente a cualquier adicción.

En la Comunidad de Madrid se coordina desde el Servicio PAD recursos, entidades y asociaciones que se dedican a estas alternativas saludables que contribuyen a:

- Empoderar a jóvenes y su vinculación al ocio saludable.
- Fomentar la participación en los distritos y su implicación en el diseño de la oferta de ocio alternativo.
- Descubrir y despertar talentos con actividades que les apasione.
- Motivarles para que lideren la elección en acciones de ocio.
- Implicarse dentro de las entidades y asociaciones.

El ocio es un contexto de socialización fundamental, espacio privilegiado para potenciar determinados factores de protección. Se debe potenciar desde las propias familias porque como ya referimos, los menores y adolescentes actúan por modelaje. Estas prácticas y vivencias positivas contribuyen al bienestar y desarrollo integral de los estos.

VII. CONCLUSIONES

Tras haber realizado la pertinente investigación acerca de los desafíos de la ciberseguridad en el entorno familiar de los menores y haber cumplido los objetivos planteados, vamos a proceder a validar o refutar las hipótesis anteriormente propuestas.

Primera hipótesis: cuánto más expuestos estén los menores al uso de redes sociales es más probable que tengan experiencias negativas en línea.

La primera hipótesis se da por válida. La realidad es que sí existe una correlación entre el uso de las redes y la posibilidad de tener experiencias negativas en estas. Se puede apreciar como en el estudio realizado por Del Río et al. en 2010 la incidencia del ciberbullying era mucho más baja que en el estudio realizado por Save the Children en 2019, esto puede ser debido a que en 2010 no usábamos tanto el *internet*, las redes sociales o los dispositivos móviles como ahora.

Las redes sociales están creadas para fomentar la conexión y comunicación entre los usuarios, careciendo de controles de edad restrictivos, ya que al crearte una cuenta prácticamente ninguna red social te pide alguna certificación de tu edad. Por tanto, cuanto más tiempo se pasa conectado en internet, más se amplifica la interacción en línea, dando lugar a que aumente el riesgo de ser una potencial víctima. Pero, ¿cómo se justifica tal afirmación?

Esta pregunta se puede responder con la teoría de las actividades cotidianas de Felson y Clarke (1998), la cual pretende explicar que para que se cometa un delito tienen que existir tres elementos que concurran en espacio y tiempo: un delincuente motivado, una víctima u objeto plausible y que no se de control social. Esta relaciona el factor de la oportunidad con la opción de delinquir.

Bien, propongamos que el medio que carece de control social es *internet* (siendo más nulo que nunca este control gracias al anonimato), y en este concurren un usuario motivado para cometer un delito y un usuario con posibilidades de ser víctima, en ese preciso instante se da el delito, lo que provoca otra víctima de ciberacoso o grooming, entre otros.

Es la misma naturaleza de las redes sociales, donde los usuarios pueden interactuar de manera anónima y sin restricciones geográficas, la que aumenta la exposición de los menores a una amplia cantidad de personas y experiencias en línea, y por tanto, aumenta las probabilidades de a ser victimizados

Además, la propia inocencia e inexperiencia de los niños actúa como un factor de riesgo a la hora de navegar por internet, ya que al no saber evaluar la veracidad de la información en línea o reconocer situaciones potencialmente peligrosas pueden ser víctimas fáciles de manipulación por parte de otros usuarios malintencionados o de depredadores en línea.

Por ello, y como se ha repetido numerosas veces en este trabajo, es crucial el papel de los padres a la hora de educar a los menores en los riesgos del mundo digital y que tomen medidas, como las anteriormente expuestas, con el fin de mitigarlos.

Por último, la segunda hipótesis, cuantas más políticas y regulaciones haya más efectiva será la protección de los menores en línea.

Se rechaza la segunda hipótesis, aunque las políticas y regulaciones desempeñen un papel importante al establecer directrices y requisitios legales para las plataformas en línea, los servidores *online* y aplicaciones en las que los menores interactúan y establezacan regulaciones específicas, como las mencionadas anteriormente, la protección de los menores en línea depende de multitud de factores, no únicamente de las regulaciones y políticas.

La efectividad de estas políticas y regulaciones depende en gran medida de varios factores. En primer lugar, de la implementación y el cumplimiento adecuado de las estas, lo que resulta un desafío, debido a la globalidad de *Internet* y las diferencias en las leyes y culturas en otros países. Además, algunas regulaciones podrían tener efectos no deseados que coarten libertades fundaentales, como la censura excesiva o la limitación de la libertad de expresión, por lo que es necesario encontrar un equilibrio entre la protección de los menores y la preservación de los derechos en línea.

Además, es crucial adoptar un enfoque integral que incluya otros aspectos importantes. La educación digital es imprescindicle para capacitar a los menores con habilidades y conocimientos para navegar de manera segura por Internet. La participación de los padres también es importante, ya que, como ya se ha expuesto estos desempeñan un papel clave en la supervisión y orientación de los menores en su uso de la tecnología.

En conclusión, a pesar de que las políticas y regulaciones pueden ser parte de que haya más protección de los menores en lína, es importante adoptar un enfoque integral que combine políticas sólidas e internaciones con educación en ciberseguridad tanto en el colegio como en el entorno familiar.

BIBLIOGRAFÍA

1. LEGISLACIÓN

Carta de Derechos Digitales, 14 de julio de 2021. Ministerio de Asuntos Económicos y Transformación Digital de España. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (Fecha de última consulta 3 de marzo de 2024).

Comisión Europea Comunicación al parlamento europeo, al consejo, al comité económico y social europeo y al comité de regiones: Una década digital para os niños y jóvenes: la nueva estrategia europea pata una internet mejor para los niños (BIK+).https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=COM:2022:212:FIN (Fecha de última consulta 15 de febrero de 2024).

Convención de las Naciones Unidas sobre los Derechos del Niño, 2 de marzo de 2021. https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFO6kx0VqQk6dNAzTPSRNx0myCaUSrDC%2F0d3UDPTV4y05%2B9GME0qMZvh9UPKTXcO12 (Fecha de última consulta 27 de enero de 2024).

Instrucción 10/2005, de 6 de octubre, sobre el tratamiento del acoso escolar desde el sistema de justicia juvenil. Doctrina de la Fiscalía General del Estado. Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=FIS-I-2005-00010 (Fecha de última consulta 7 de marazo de 2024).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y parantía de los derechos digitales. Boletín Oficial del Estado, *núm. 294*, 6 de diciembre de 2018. https://www.boe.es/eli/es/lo/2018/12/05/3/con (Fecha de última consulta 6 de marzo de 2024).

Proposición de Ley Orgánica 122/000326, 19 de mayo de 2023, de refuerzo de las medidas para restringir el acceso de los menores de dieciséis años a la pornografía. Boletín Oficial de las Cortes Generales, *núm 353-1*.

https://www.congreso.es/public_oficiales/L14/CONG/BOCG/B/BOCG-14-B-353-1.PDF (Fecha de última consulta 2 de abril de 2024).

Reglamento (UE) 2022/2065 del Parlamento europeo y del Consejo relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). Boletín Oficial del Estado, *núm 277*, 27 de octubre de 2022. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81573 (Fecha de última consulta 4 de marzo de 2024).

2. OBRAS DOCTRINALES

Ciberacoso o ciberbullying. (s. f.). Save The Children. https://www.savethechildren.es/donde/espana/violencia-contra-la-infancia/ciberacoso-ciberbullying (Fecha de última consulta 16 de abril de 2024).

Del Río, J. et al (2010). Menores y redes ¿sociales?: de la amistad al cyberbullying. Universidad de Navarra. https://dadun.unav.edu/bitstream/10171/20588/1/articulo.pdf (Fecha de última consulta 17 de abril de 2024).

Giant, N. (2016). Ciberseguridad para la i-generación. Usos y riesgos de las redes sociales. (1ªed.). Narcea. ISBN: 9788427721432

Gutiérrez, D. A. (2020). Delito de «sexting», configuración jurisprudencial. *Diario de Ley,* 9760. https://diariolaley.laleynext.es/Content/DocumentoRelacionado.as (Fecha de última consulta 15 de abril de 2024).

Kowalski, R. et al (2014). Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth. Psychological bulletin, 140(4), 1073-1137. DOI: http://dx.doi.org/10.1037/a0035618 (Fecha de última consulta 12 de enero de 2024).

López-Iglesias, M. et al (2023). Patologías y dependencias que provocan las Redes Sociales en los jóvenes nativos digitales. Revista de Comunicación y Salud, 13,

pp.1-21. http://doi.org/10.35669/rcys.2023.13.e301 (Fecha de última consulta 16 de febrero de 2024).

López, A. y Fernández, T. (2008). Trabajo Social Comunitario: afrontando juntos los desafíos del siglo XXI. Alianza (1ªed.). ISBN: 978-84-206-4860-6

Mercado, C.T., et al (2016) Sexting: su definición, factores de riesgo y consecuencias. Revista Sobre la infancia y la adolescencia, 1, 1-18. DOI: http://dx.doi.org/10.4995/reinad.2016.3934 (Fecha de última consulta 20 de enero de 2024).

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2023). *Directrices para la gobernanza de las plataformas digitales*. UNESCO. ISBN: 978-92-3-300215-9

Patchin, J. W., et Hinduja, S. (2006). Bullies Move beyond the Schoolyard: A Preliminary Look at Cyberbullying. Youth Violence and Juvenile Justice, 4, 148-169. https://doi.org/10.1177/1541204006286288 (Fecha de última consulta 19 de enero de 2024).

Prensky, M. (2001). Digital natives, digital inmigrants. On the Horizon, 9(5). https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf (Fecha de última consulta 27 de enero de 2024).

Whittle, H. et al (2013) A review of online grooming: Characteristics and concerns. Aggression and violent Behavior, 1(18), 62-70. DOI: https://doi.org/10.1016/j.avb.2012.09.003 (Fecha de última consulta 16 de abril de 2024).

Willard, N. E. (2007). Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Research Press. https://psycnet.apa.org/record/2007-02981-000 (Fecha de última consilta 13 de abril de 2024)

3. RECURSOS DE INTERNET

Abacus Cooperativa (2019). Què són els continguts inadequeats a internet i com affecten els menors?. Abacus (Fecha de última consulta 16 de abril de 2024)

Englander, E. et al (2017) Defining Cyberbillying. Pediatrics, 140(2), 148-151. DOI: 10.1542/peds.2016-1758U (Fecha de última consulta 17 de abril de 2024).

González, A. et al (2023). El delito de "grooming" o ciberacoso sexual a menores. Dexia Abogados. https://www.dexiaabogados.com/blog/delito-ciberacoso-sexual-menores/#:~:text=Se%20conoce%20por%20grooming%20el,menores%20en%20el%20artículo%20183. (Fecha de última consulta 16 de abril de 2024).

INCIBE (s.f.) Grooming, "Amistades muy peligrosas". https://www.incibe.es/aprendeciberseguridad/grooming#:~:text=El%20grooming%20es%20una%20práctica,al%20chantaje%20con%20fines%20sexuales. (Fecha de última consulta 17 de abril de 2024)

La profesión - El trabajo social - Portal del Colegio Profesional de Trabajo Social de Córdoba. (s. f.). Consejo General del Trabajo Social. https://www.cgtrabajosocial.es/cordoba/El_trabajo_social (Fecha de última consulta 18 de abril de 2024).

Labrador, E. et al (2018). Guía para padres y educadores sobre el uso seguro de Internet, móviles y videojuegos. Fundación Gaudium. https://www.observatoriodelainfancia.es/oia/esp/documentos_ficha.aspx?id=5686 (Fecha de última consulta 17 de abril de 2024)

Raya, E. (s. f.). Fundamentos y objeto del Trabajo Social Comunitario [Archivo PDF]. https://www.unirioja.es/dptos/dchs/archivos/TEMA4FUNDAMENTOS.pdf (Fecha de última consulta 18 de abril de 2024).

Save the Children (2023). Informe: por una justicia a la altura de la infancia. Save the Children. https://www.savethechildren.es/sites/default/files/2023-11/Por_una_justicia_a_la_altura_de_la_infancia_STC_2023.pdf (Fecha de última consulta 18 de abril de 2024).