ISSN: 2444-250X | ISSN-e: 2444-2887

El impacto de las tecnologías de la información y la comunicación en la educación. La importancia de la formación, la información y la sensibilización

María José Garrido Antón

Doctora en Psicología por la Universidad Autónoma de Madrid/ Capitán de la Guardia Civil (España)
mjganton@yahoo.es | https://orcid.org/0000-0002-1290-7959

Ángel García-Collantes

Doctor en Derecho/Licenciado en Criminología y Psicología por la Universidad Camilo José Cela (Madrid, España)
007agc@gmail.com | https://orcid.org/0000-0001-9517-3884

Extracto

Profesorado y progenitores deben promover el uso responsable de las nuevas tecnologías al objeto de proteger la seguridad y ciberseguridad de los menores. Al igual que en otras disciplinas y campos, la importancia de la formación, la información y la sensibilización (FIS) se convierte en algo fundamental para evitar comportamientos delictivos o preocupantes. Los profesores (hombres y mujeres) deben estar suficientemente informados y sensibilizados para poder detectar comportamientos relacionados con la violencia cometida a través de las tecnologías de la información y la comunicación (TIC). El *cyberstalking*, el *sexting*, el *cyberbullying* o la *sextortion* son, lamentablemente, comportamientos que se dan con frecuencia, pero con cuyas conductas el profesorado no está familiarizado, por lo que suponen un factor de riesgo a la hora de detectar situaciones de violencia entre niños, niñas y adolescentes y alertar sobre ellas. El propósito principal de este trabajo es elaborar material detallado sobre la descripción de estos comportamientos, además de informar sobre qué hacer y qué no si se observan señales de alarma y/o situaciones de riesgo que vulneren los derechos de los menores.

Palabras clave: nuevas tecnologías; *cyberbullying*; *grooming*; *sextortion*; jóvenes.

Fecha de entrada: 04-05-2021 / Fecha de aceptación: 10-09-2021

Cómo citar: Garrido Antón, M.ª J. y García-Collantes, Á. (2022). El impacto de las tecnologías de la información y la comunicación en la educación. La importancia de la formación, la información y la sensibilización. *Tecnología, Ciencia y Educación*, *21*, 155-182. https://doi.org/10.51302/tce.2022.660

The impact of information and communication technologies on education. The importance of training, information and awareness

María José Garrido Antón

Ángel García-Collantes

Abstract

Teachers and parents must promote the responsible use of new technologies to protect the safety and cybersecurity of minors. As in other disciplines and fields, the importance of training, information, and awareness (TIA) becomes essential to avoid criminal or worrying behavior. Teachers (men and women) must be sufficiently informed and sensitized to be able to detect behaviors related to violence committed through information and communication technologies (ICT). Cyberstalking, sexting, cyberbullying or sextortion are, unfortunately, behaviors that frequently occur, and teachers are not always familiar with, so it become a risk factor when they detect violence situations between children, girls and adolescents. The main purpose of this paper is to describe this criminal and worrying behaviors and to establish what to do in case of alarm signals and/or risk situations.

Keywords: new technologies; cyberbullying; grooming; sextortion; youth.

Citation: Garrido Antón, M.ª J. and García-Collantes, Á. (2022). The impact of information and communication technologies on education. The importance of training, information and awareness. *Tecnología, Ciencia y Educación*, *21*, 155-182. https://doi.org/10.51302/tce.2022.660

Sumario

1. Introducción

Hoy en día, los procesos de comunicación han experimentado una evolución muy significativa, tanto que se puede hablar de una auténtica revolución digital gracias a las TIC. La percepción del espacio y del tiempo se ha modificado. La transmisión de la información se puede llevar a cabo en formato 24/7, es decir, a cualquier hora del día durante los 365 días del año y desde cualquier parte del mundo. En este escenario de procesos de comunicación transversal constante y continua surgen nuevas herramientas de interacción digital, como son las redes sociales (Facebook, Twitter, YouTube, Instagram, Telegram o TikTok), que adquieren el principal protagonismo social en el siglo XXI, permitiendo que las personas estén conectadas de manera permanente, creando nuevos espacios y, consecuentemente, nuevos hábitos sociales.

Hoy en día, los procesos de comunicación han experimentado una evolución muy significativa, tanto que se puede hablar de una auténtica revolución digital gracias a las TIC. La percepción del espacio y del tiempo se ha modificado

Para situar este fenómeno desde un punto de vista cuantitativo, se puede afirmar que, a nivel global, el uso de las TIC asciende aproximadamente a 4.538 millones de personas conectadas a internet, según el informe realizado por Hootsuite & We Are Social[1] en enero de 2020. Además, se puede añadir que alrededor del 42 % de la población mundial utiliza las redes sociales para comunicarse e interactuar (Kemp, 2018). Más recientemente, IAB Spain (2021) afirmó que todo el mundo está en internet y que un 87 % de los internautas (más de 25.000.000 de españoles de entre 16 y 65 años) usan a menudo las redes sociales.

Las ventajas que ofrecen las nuevas tecnologías son infinitas e innegables, pero no se puede obviar que allí donde existe el ser humano también aparece el riesgo de que se produzcan comportamientos delictivos (en algunas ocasiones) y preocupantes (en otras muchas ocasiones) relacionados con el uso patológico de internet. Por ejemplo, Pérez y Cifuentes (2008) destacaron la existencia de algunas salas de conversación cibernéticas sobre el suicidio, provocando los «ciberpactos suicidas». Los trastornos de alimentación también se proyectan en la red con gran despliegue de páginas web, blogs, foros y testimonios personales, donde se hace apología del estilo de vida de las personas que padecen estas enfermedades (Bermejo *et al.*, 2011). El racismo también se ha promocionado

Las ventajas que ofrecen las nuevas tecnologías son infinitas e innegables

[1] https://wearesocial.com/es/blog/2021/01/digital-report-2021-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/

por internet. Existen también comunidades que promueven la autolesión (*self-harm*), otras que incitan al odio (*hate-speech*), aquellas que promueven hábitos de vida no saludable o las que realizan apología de la pedofilia o de la violencia de género.

Se puede afirmar que un número considerable de personas, especialmente menores, ha desarrollado una verdadera adicción a internet, creándose nuevos tecnoconceptos, como el *vamping* (uso de dispositivos durante la noche), la «nomofobia» (miedo irracional a estar sin el teléfono móvil), el *gambling* (participar en juegos de azar a través de la red), el *infosurfing* (navegar de forma continuada y prolongada sin un objetivo claro) o el *hikikomori* (casos extremos de aislamiento, como no salir de la habitación refugiándose en el mundo virtual absolutamente), que forman parte de las llamadas «tecnoadicciones». Se podría resumir diciendo que un uso normal de un dispositivo electrónico no tiene consecuencias psicológicas negativas siempre que no afecte al completo desarrollo de otras actividades y facetas de la vida con amigos, familia, cultura y deporte. Se puede hablar de «abuso» cuando el uso es excesivo de manera puntual durante el inicio y, pasada la novedad, se sigue haciendo uso de manera normal. Finalmente, la «dependencia» hace alusión a la necesidad de estar conectado todos los días a internet y solo el pensamiento de no estarlo produce sintomatología ansiosa o irritabilidad.

Se puede afirmar que un número considerable de personas, especialmente menores, ha desarrollado una verdadera adicción a internet, creándose nuevos tecnoconceptos que forman parte de las llamadas «tecnoadicciones». [...] La «dependencia» hace alusión a la necesidad de estar conectado todos los días a internet y solo el pensamiento de no estarlo produce sintomatología ansiosa o irritabilidad

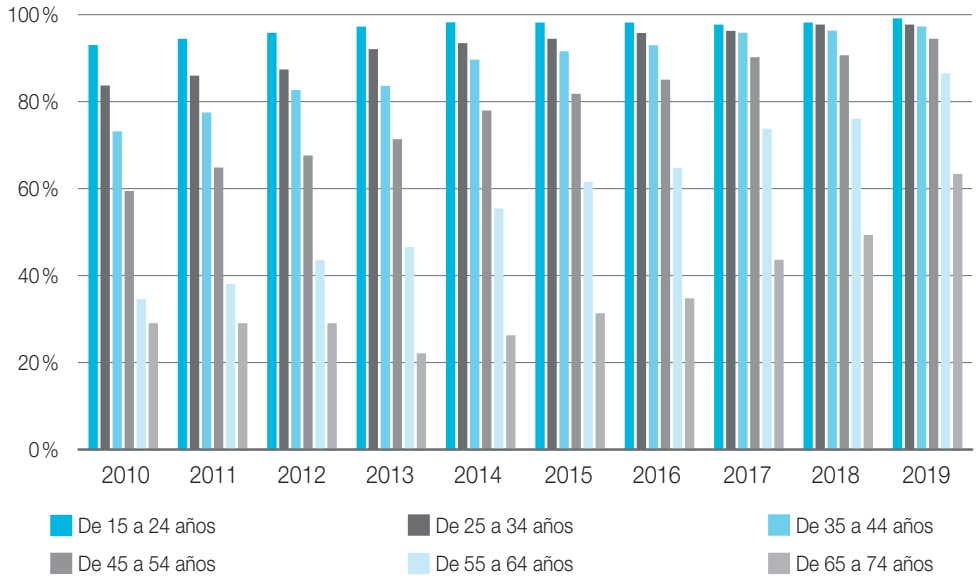
Las TIC, como se ha dicho, han provocado cambios profundos en las relaciones, así como en la forma de comunicarnos. En 2015, un 98 % de los adolescentes españoles entre 10 y 14 años ya contaban con un teléfono móvil, incluso de última generación con conexión a internet (Ditendria, 2016). Y el 27 % de estos jóvenes manifestaron no apagar nunca el teléfono. El 66,80 % de la muestra manifestó haber participado en redes sociales en los tres últimos meses, principalmente en Facebook, Twitter y otras redes como Instagram. Otra de las actividades frecuentes es la creación de perfiles de usuarios y envío de mensajes. Destaca que el grupo más participativo es aquel correspondiente a los estudiantes, con el 90,70 % (Ditendria, 2016). Así, el uso de las TIC entre los jóvenes muestra cómo el acceso a páginas web frecuentemente y de manera inapropiada puede crear en los usuarios la ciberadicción (Nocentini *et al.*, 2015).

En los últimos años, y como consecuencia de este uso y abuso de internet, el aumento progresivo de la ciberadicción se ha experimentado de forma exponencial. Por ello, y atendiendo a los estudios de ciberseguridad de España, se desprenden los siguientes datos relevantes. Los jóvenes, con un 98,50 %, son los que hacen un mayor uso de internet, especialmente en edades comprendidas entre los 16 y los 24 años. Los menores

de edad entre los 10 y los 15 años manifestaron haber tenido acceso a internet en un 92,50 %. Por otro lado, las personas con una franja de edad comprendida entre los 65 y los 74 años representan un 49,10 %.

Como se puede ver a continuación, la figura 1 representa el uso de internet por franjas de edad durante el periodo 2010-2019. Al analizar la misma, se observa que el uso de internet ha ido ascendiendo a lo largo de los años en todas las franjas de edad, destacando el incremento de estas tecnologías en personas de edad avanzada, entre los 65 y los 74 años (crece algo más de un 40 % durante el periodo analizado) (Cereceda *et al.*, 2018).

Figura 1. **Uso de internet por franjas de edad durante el periodo 2010-2019**



Fuente: Ministerio del Interior (2021).

En este escenario virtual es preciso familiarizarse con conceptos como la «identidad digital», es decir, todo aquello que se publica y queda registrado, creando de manera directa e indirecta un perfil que nos define ante el resto de ciberusuarios. Esto viene a ser como la huella digital. Uno de los peligros de compartir material en la red es que, una vez subidos los contenidos, estos no desaparecen nunca al 100 %, incluso denunciando o poniendo de manifiesto la prohibición de su publicación. En el momento en que se pulsa la tecla «Enter», los contenidos pasan del patrimonio individual de cada usuario al de la comunidad internauta.

Como se puede observar, internet es una excelente plataforma para mejorar e innovar, pero esta serie de ventajas se pueden convertir en traumáticas consecuencias cuando se utilizan con la finalidad de zaherir a otros.

2. Redes sociales

Las redes sociales han venido para quedarse. Especialmente, son utilizadas por la población adolescente, pero no menos despreciable es la frecuencia de uso por personas de todas las edades. Se podría decir que hay diversidad de uso de redes en función de la edad cronológica y de las preferencias. Streeter y Gillespie (1992) ya las definían como cualquier conjunto limitado de entidades sociales conectadas. Por otro lado, Wasserman y Faust (1999) definen una «red social» como un conjunto finito de actores y la relación o relaciones que los vinculan. Castañeda *et al.* (2011) las definen como «aquellas herramientas telemáticas de comunicación que tienen como base la web, se organizan alrededor de perfiles personales o profesionales de los usuarios y tienen como objetivo conectar secuencialmente a los propietarios de dichos perfiles a través de categorías, grupos, etiquetados, personales, etc., ligados a su propia persona y perfil profesional» (Casteñeda y Gutiérrez, 2010, citado por Castañeda *et al.*, 2011, p. 6).

Las redes sociales son espacios de relación, lugares de encuentro colectivo que ofrecen nuevas formas de comunicación, de socialización y hasta de relaciones afectuosas. Este tipo de formas de comunicarse permite la conexión de personas en espacio y tiempo. Su crecimiento es exponencial, siendo millones los usuarios que hacen uso de estas herramientas en todo el mundo con diferentes intereses, bien como medio de comunicación, bien como entretenimiento y/o acceso a información especializada (Calderón-Cañola, 2010).

Según un informe realizado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), la definición de «red social» más compartida por los autores es la siguiente:

> Un sitio en la red cuya finalidad es permitir a los usuarios relacionarse, comunicarse, compartir contenido y crear comunidades, o como una herramienta de democratización de la información que transforma a las personas en receptores y en productores de contenidos (Urueña, 2011, p. 12).

Como establecen Méndez-Lois *et al.* (2015) es evidente que las redes sociales se han instaurado en la sociedad y, especialmente, en la adolescencia. Tal es así que el ciberprotocolo de detección e intervención en la atención a las víctimas de ciberdelincuencia de género (Instituto Andaluz de la Mujer, 2018) llega a establecer diferencias entre los/las nativos/as e inmigrantes digitales. Con el término «nativo/a digital», hacen referencia a todas las personas nacidas en países con capacidad tecnológica en la década de los años ochenta y posteriores, cuando la tecnología digital ya se encontraba bastante desarrollada y al alcance de

buena parte de la sociedad. Por otro lado, los «inmigrantes digitales» son todas las personas que han nacido entre 1940 y 1980, ya que, aunque no han accedido a las TIC de manera natural, se han incorporado a ese mundo, bien como espectadores y receptores de las consecuencias del fenómeno, bien como parte activa, tanto en el ámbito privado como en el laboral y social (*ibidem*).

Actualmente existen múltiples redes sociales. Se pueden clasificar en función de los intereses que persiguen (sociales o profesionales), de la población para la que están diseñadas, así como por temas, por actividades o por contenidos. Otras clasificaciones las dividen entre horizontales –dirigidas a un público genérico con el fin de crear una red de personas con contenido diverso (Facebook, Hi5, MySpace, etc.)– y verticales –se especializan en los intereses de los usuarios con finalidades concretas–. En el cuadro 1 se ofrece una clasificación de las redes sociales más populares en España divididas por categorías temáticas.

Cuadro 1. **Algunos tipos de redes sociales**

Tipo de red social	Descripción	Ejemplos
Intereses varios	Comunicación.	Facebook, Myspace y WhatsApp.
	Identidad cultural.	Spaniards.
	Hobbies.	BlooSee.
	Sociabilidad.	SocialVibe.
	Ocio.	Travel Buddy.
	Perfil lingüístico.	Busuu y Duolingo.
Actividad	*Microbloggins.*	Twitter.
	Juegos y ocio.	World of Warcraft.
	Geolocalización.	Google Maps.
	Deportes.	Strava.
Contenido compartido	Música y vídeos.	Spotify, SoundCloud y YouTube.
Profesionales	Laboral.	LinkedIn, Monster y Plaxo.

Fuente: García-Collantes y Garrido (2021).

Analizando las características de los usuarios en el *Estudio anual de redes sociales 2020* (IAB Spain, 2020), el 87 % de las personas con una franja de edad comprendida entre los 16 a 65 años hace uso de redes sociales (en torno a los 25.000.000 solo en España). De todas las redes sociales, WhatsApp es la más usada. En función del género es preciso mencionar que el 49 % de los usuarios son hombres, frente al 51 % de mujeres. Se usan alrededor de 3,7 redes sociales por usuario, siendo la aplicación WhatsApp, como se ha comentado anteriormente, la más utilizada (88 %), seguida de Facebook (87 %), YouTube (68 %), Instagram (49 %) y Twitter (50 %).

En relación con el tiempo de conexión, la investigación referenciada dio los datos que se pueden ver en el cuadro 2. Si nos centramos en las actividades realizadas en las redes sociales, los porcentajes de uso más frecuentes se pueden observar en el cuadro 3.

Cuadro 2. **Tiempo de conexión en redes sociales**

Redes sociales	Tiempo de conexión por persona y día (promedio)
WhatsApp	1h y 47 min
YouTube	1h y 34 min
Twitch	1h y 30 min
Todas	**55 min**

Fuente: elaboración propia a partir de IAB (2020).

Cuadro 3. **Actividades en redes sociales**

Actividades	Porcentajes de uso
Chatear y mensajear	65 %
Vídeos y música	57 %
Observar a otros usuarios	45 %
Todas	**55 %**

Fuente: elaboración propia a partir de IAB (2020).

El informe también concluye que el teléfono portátil es el primer dispositivo de acceso (95 %) y le sigue el ordenador (92 %) y después las tabletas (54 %).

A modo de conclusión, es preciso puntualizar que las redes sociales son solo una pequeña parte de las TIC. A veces se utilizan ambos conceptos indistintamente, como si fueran lo mismo, pero es preciso indicar algunas diferencias entre ellos. Las TIC, generalmente, se desarrollan de manera independiente a las redes sociales y no necesitan usar internet, a diferencia de estas, que sí necesitan internet para establecer la comunicación. Las redes sociales funcionan a través de las nuevas tecnologías y algunas de las conductas delictivas objeto de este artículo se dan en las redes sociales a través de los nuevos medios, aunque, en muchas ocasiones, el contacto traspasa el universo *online* para entrar en el mundo real de la víctima, y viceversa.

3. Propiedades del ciberespacio

Las tecnoadicciones son comportamientos que solo se pueden llevar a cabo usando un ordenador, las redes informáticas u otra forma de tecnología internauta. Esta cualidad ofrece una mayor sensación de anonimato y superioridad, además de impunidad, seguridad y tranquilidad, en los casos del ciberacoso o del *cyberbullying*, por ejemplo, pues complica la identificación del origen de dichos hechos en un gran número de ocasiones (Guadaño, 2016). A continuación, exponemos algunas de las características que pueden darse en el mundo *online*:

- **Anonimato (el agresor puede mantenerse como alguien desconocido para la víctima).** Constituye un factor de riesgo que potencia el hecho de poder delinquir en la red. La dificultad de perseguir el grado de participación de determinadas acciones perpetradas en el ciberespacio puede contribuir a que se perciba una cierta sensación de impunidad sobre el autor. Además, la ausencia de la identificación del autor puede ser percibida como deserción de reglas o responsabilidad. El anonimato reduce la inhibición. Como ya decía LeBon (1895) en su obra *La psicología de las masas*, el individuo se siente protegido en las multitudes bajo una capa de anonimato que le hace percibir sus propios actos carentes de responsabilidad. Comportamientos como el *cyberstalking* se basan mayoritariamente en el anonimato (Roberts, 2008).
- **Pensamiento en masa (el grupo arrastra a las masas).** Esta característica se encuentra muy relacionada con el anonimato. Se trata del posicionamiento hacia algo o alguien solo por no salirse del grupo de referencia *online*. Además, la variedad y disponibilidad de la mayoría de las tecnologías lo hacen realmente accesible tanto para los agresores como para las decenas de potenciales personas a las que les podría llegar una imagen abusiva, un texto o un vídeo. El impacto emocional en la víctima escala por estos extremos.
- **Gratuidad e inmediatez (aquí y ahora).** La facilidad de acceso y que, en la mayoría de las ocasiones, sea suficiente con un dispositivo que tenga conexión a internet, se convierte en un factor de riesgo, puesto que provoca que cualquier usuario pueda hacer un uso inadecuado. Además, las acciones abusivas a través de las nuevas tecnologías requieren menos tiempo y esfuerzo. Este tipo de

comportamientos fomenta la cultura de «lo quiero ahora y ya». Internet refuerza las desideratas, proporcionando información, datos y acceso con un solo clic y, la mayoría de las veces, de forma gratuita.

- **Trasnacionalidad (falta de fronteras).** El ciberespacio no está localizado en un lugar concreto, sino que se encuentra en todos los sitios a la vez. Es algo deslocalizado, donde prima la inexistencia de fronteras. Por eso es importante, a nivel de la Unión Europea, compartir definiciones, normativa y algún modo de «comunitarizar» los delitos para estudiarlos y perseguirlos bajo el mismo paraguas europeo. Se trata de conglomerados de redes interconectadas que permiten a los seres humanos establecer lazos desde cualquier parte del mundo con cualquier persona en cualquier momento.
- **Pérdida de intimidad (la era de la intimidad ha terminado).** En el momento que una persona deposita material en internet, existe automáticamente un desnudo público de las propiedades de ese sujeto. El *big data* funciona segundo a segundo perfilando y prediciendo nuestro comportamiento. Hay que tener en cuenta que, cuando se sube algo a internet, se pierde la autoridad y no se sabe para qué y con qué objetivos puede ser utilizado ese material. Como dijo el fundador de Facebook, Mark Zuckerberg, en 2010[2], la era de la intimidad ha terminado. Con un simple clic se puede producir un «desnudo» público de la vida privada de cualquiera, especialmente teniendo en cuenta que en las redes sociales es posible declarar la situación sentimental de cada individuo, sus emociones, sus estados, sus opiniones, incluso colgar imágenes y vídeos de uno mismo y de otras personas, etc. (Mejías y Rodríguez, 2014). Es importante destacar que por parte de determinados ámbitos se está intentando construir algún tipo de sistema que permita la identificación de los usuarios en la red. Parece que esta realidad es complicada, máxime teniendo en cuenta que las redes wifi libres permiten acceder desde sitios abiertos o que existen proveedores de servicios gratuitos que no exigen la identificación de los usuarios, sin olvidarnos de los múltiples sistemas que permiten enviar correos electrónicos de forma anónima y, desde un punto de vista más criminal, la posibilidad de infectar un determinado sistema informático para convertirlo en robot o zombi y utilizarlo para la actividad criminal (Miró, 2012). En los medios digitales, una gran cantidad de datos personales son recogidos sin nuestro consentimiento y usados diariamente para perfilarnos y producir predicciones de nuestro comportamiento futuro. Cuando subimos algún dato a internet, se desconoce quién, cómo y para qué objetivo puede ser utilizado. Es preciso recordar que la privacidad es un derecho fundamental del ser humano, esencial para vivir en dignidad y seguridad.

[2] https://www.abc.es/tecnologia/redes/abci-mark-zuckerberg-privacidad-acabado-201001110300-1132992452646_noticia.html

- **Vulneración de nuestra privacidad e intimidad.** La amenaza real o percibida de vulneración de nuestra privacidad e intimidad, así como de nuestras comunicaciones o imágenes más personales puede provocar pensamientos obsesivos en la víctima y una sensación de control sobre ella (Iglesias, 2018).
- **Permanencia de datos y revictimización.** El contenido subido al ciberespacio dura y perdura en el tiempo pese a los esfuerzos por intentar su desaparición. Internet y las redes sociales mantienen las imágenes y los contenidos subidos durante largos periodos de tiempo o, si no se toman medidas legales, indefinidamente, lo que para la víctima puede ser muy destructivo psicológicamente.

4. Delitos ciberdependientes

Constituyen comportamientos que solo se pueden cometer usando un ordenador, las redes informáticas o las TIC. Los entornos virtuales también permiten la conexión desde diferentes países, siendo posible enviar datos por medio de una selección variada de servidores. Ello va a ofrecer una mayor sensación de anonimato y superioridad, además de impunidad, seguridad y tranquilidad. En los casos de ciberacoso o *cyberbullying*, por ejemplo, complica la identificación del origen de dichos hechos en un gran número de ocasiones (Guadaño, 2016).

Todas estas características favorecen la aparición de la violencia *online*. Aunque podamos pensar que este tipo de violencia se da más en adolescentes, sucede en todas las edades (Martínez, 2017). El cibercrimen es un fenómeno global que afecta a todos los Estados y no tiene fronteras. La superficie de ataque continúa creciendo a medida que la sociedad se digitaliza cada vez más, con mayor número de ciudadanos, empresas, servicios públicos y dispositivos que se conectan a internet.

Asimismo, y relacionado indudablemente con los peligros de internet, han de destacarse los riesgos a los que tanto adolescentes como adultos se exponen al utilizar las redes sociales sin la conciencia y la responsabilidad que ello debería suponer.

Según Alonso (2017), los riesgos del uso de las redes sociales, en general, podrían resumirse en cinco:

- Riesgos derivados de la comunicación entre iguales, como el *cyberbullying*.
- Riesgos derivados de la difusión de contenidos inapropiados o ilegales.
- Riesgos asociados con el abuso de la privacidad.
- Riesgos debidos al uso excesivo, como adicción o depresión.
- Riesgos como el fraude *online* o la exposición de virus informáticos.

5. Comportamientos delictivos/preocupantes en el ciberespacio

En el cuadro 4 podemos observar un listado lo más realista y novedoso posible sobre los comportamientos que se están dando en internet en la actualidad. Siguiendo los objetivos de este artículo, sería preciso que profesores y educadores conociesen y estuviesen sensibilizados con todos estos comportamientos para poder detectarlos y educar, así, a los estudiantes.

Cuadro 4. **Comportamientos *online***

Hacking (piratería)	Uso de la tecnología para tener acceso ilegal o no autorizado a determinados sistemas o páginas con el propósito de obtener información personal, alterar o modificar información, calumniar o denigrar. Por ejemplo, acceder a información personal, como listas de contacto, mensajes o correos electrónicos, etc.
Suplantación de identidad	Uso de la tecnología para asumir la identidad de la víctima con el propósito de acceder a información privada, avergonzar o culpar a la víctima, o crear falsos documentos de identidad. Por ejemplo, crear un perfil falso de identidad en redes sociales. Cuando alguien se hace pasar por otra persona y tiene intención no solo de este hecho, sino también de perjudicarle, se considera delito.
Surveillance/tracking (vigilancia/rastreo)	Uso de la tecnología para acosar y monitorizar a la víctima y sus actividades. Saber su comportamiento tanto *online* como *offline*. Por ejemplo, utilizar programas espía o utilizar el GPS del móvil de la víctima para saber dónde se encuentra.
Harassment/spamming (acoso *spam/cyberstalking*)	El uso de la tecnología para contactar continuamente con la víctima, molestarla, amenazarla o asustarla. Se trataría de un patrón de comportamiento vivo y no solo de un incidente aislado. Algunos ejemplos pueden incluir reiteradas llamadas y mensajes tanto de texto como de voz.
Recruitment (reclutamiento)	El uso de la tecnología para reclutar víctimas potenciales como se hace con el tráfico de seres humanos; por ejemplo, usando *chat rooms* y determinadas páginas web.
Malicious distribution, doxing and revenge pornography	Manipular y distribuir información difamatoria relacionada con la víctima, sin su consentimiento, que puede incluir contenidos con connotación erótica o sexual. Por ejemplo, chantajes en los que se amenaza a la víctima con distribuir por la red fotos y vídeos suyos si esta no envía más material fotográfico o audiovisual.

Phising	Se trata del envío de mensajes simulando su procedencia de fuentes fidedignas. El delincuente reproduce en formato y forma páginas de empresas. Al usuario se le suelen solicitar datos e información personal.
Pharming	Consiste en manipular direcciones electrónicas para engañar al usuario y cometer fraude.
Cyberbullying o *cybermobbing*	Agresión psicológica sostenida y repetida en el tiempo que trata de acosar y perseguir por medio de cualquier plataforma o escenario virtual a las víctimas.
Stalking	Íntimamente relacionada con la conducta anterior. Se trata de una forma de acoso a través de las TIC que consiste en la persecución interrumpida e intrusiva de modo compulsivo a una persona con la que se quiere contactar constantemente a través de varias páginas y de redes sociales. Este comportamiento se da sin el consentimiento de la víctima y en contra de su voluntad.
Cyberbaiting	Los alumnos confeccionan material sobre los profesores (imágenes, fotografías, montajes, etc.) y lo difunden a través de las redes sociales, insultándolos y desprestigiándolos.
Delito de *sexting*	Envío y recepción de material (imágenes y vídeos mayormente) con contenido sexual a través de dispositivos tecnológicos sin consentimiento de la persona.
Sextortion	Extorsión a una persona haciendo público material comprometido sobre ella sin su consentimiento.
Grooming	Engatusamiento *online* por parte de adultos con el objetivo de ganarse la confianza de un menor fingiendo empatía, celos o cariño. La finalidad es la satisfacción sexual obteniendo imágenes de menores con contenido sexual.

Fuente: elaboración propia a partir de García-Collantes y Garrido (2021).

Conviene indicar que cuando estos comportamientos se dan en el marco de una relación de pareja (Ley orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género) se convierten en ciberviolencia de género y se aplica el agravante de género. Quedarían, de esta manera, incardinados en los siguientes tipos penales, como se puede ver en el cuadro 5.

Cuadro 5. **Comportamientos *online* en el marco de la ciberviolencia de género**

Definición	Tipo	Código Penal	Medio
Delitos de amenazas y coacciones.	Amenazas. Coacciones.	Artículos 169 a 172.	Internet/telefonía, intranet, correos electrónicos, redes sociales, blogs y mensajes electrónicos.
Delitos contra el honor.	Calumnias. Injurias.	Artículos 205 a 210 y 620.2.	Internet/telefonía, intranet, correos electrónicos, redes sociales, blogs y mensajes electrónicos.
Delitos de acceso de interceptación ilícita.	Revelación de secretos. Intimidad.	Artículos 197 a 201.	Internet/telefonía, intranet, correos electrónicos, redes sociales, blogs y mensajes electrónicos.
Usurpación de identidad.	Suplantación de identidad.	Títulos X a XII.	Internet/telefonía, intranet, correos electrónicos, redes sociales, blogs y mensajes electrónicos.
Delitos de acceso de interceptación ilícita.	*Cyberstalking*	Artículo 172 ter 1.2.ª (en vigor desde el 1 de julio de 2015)*	Internet/telefonía, intranet, correos electrónicos, redes sociales, blogs y mensajes electrónicos.

* Artículo 172 ter 1.2.ª del Código Penal: «Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas».

Fuente: García-Collantes y Garrido (2021).

Como se ha podido observar a lo largo de este apartado, en España, al igual que sucede en el resto del mundo, han ido apareciendo nuevos comportamientos delictivos cometidos a través de las nuevas tecnologías. Algunos de ellos no son delictivos como tal, pero sí suponen un factor de riesgo para que se comentan otros; por ejemplo, el *sexting* es la antesala del delito de *sexting.*

A pesar de la importancia de estas conductas, puesto que, en muchos casos, se vulneran derechos fundamentales, sin olvidarnos de las devastadoras consecuencias psicológicas que tienen para la víctima, son escasos los estudios sistemáticos que existen sobre el tema de la ciberviolencia de género en particular. Todos los comportamientos que se han ido viendo consisten en dañar a la víctima por medio de la vigilancia y de persecuciones *online*, enviando mensajes de manera reiterada, escribiendo despectivamente en las redes sociales sobre ella, interceptando su identidad o haciéndose pasar por ella robando sus contraseñas y accediendo a sus cuentas personales. La mayoría de las conductas pueden solaparse unas con otras de manera sencilla y es difícil considerarlas como comportamientos aislados o estancos.

6. Aportaciones de las nuevas tecnologías a la educación

Con el avance de las tecnologías se puede constatar que, últimamente, destaca el gran desarrollo en materias TIC. Incluso se puede llegar a decir que han cambiado los hábitos de muchas de las tareas que tradicionalmente se hacían de manera mecánica (a mano). El sector educativo no puede ser diferente y también se ha hecho eco de estos cambios, adaptándose a los nuevos entornos. Estas modificaciones han acarreado a su vez cambios muy profundos en las formas de relacionarse dentro y fuera de las aulas (Rodríguez-Álvarez *et al.*, 2018).

Los últimos tiempos, después de todo lo vivido como consecuencia de la COVID-19 y de los reiterados confinamientos, han marcado un antes y un después, pues los centros educativos se han visto obligados a adaptarse a las nuevas tecnologías, al tener que realizar tareas y trasladar las aulas físicas al entorno virtual, ratificando, con ello, la utilidad de las nuevas tecnologías. Con estos cambios, se ha comprobado que los estudiantes pueden seguir formándose en cualquier entorno o lugar con solo conectarse a un terminal dotado de acceso a internet.

Por ello, es evidente que todos estos avances han modificado muchos hábitos, metodologías, formas de enseñar y de aprender, y, lo que está claro, es que han venido para quedarse. Consecuentemente, ha cambiado la forma de enseñar y el modo de interacción entre los profesores y los alumnos en las aulas del entorno virtual, así como entre los propios alumnos.

En relación con la figura del profesor/docente, Cerezo y Rubio (2017) afirman que la mayor parte de este colectivo dedicado a la educación de los menores manifiesta una falta de formación sobre la materia para poder intervenir e, incluso, para detectar comportamientos como el ciberacoso en sus propias aulas (Montoro y Ballesteros, 2016).

Así, estudios en los que han participado algunos docentes destacan que las estrategias más comunes a las que recurre este colectivo son apoyarse en otros compañeros, ofrecer apoyo a las víctimas, implicar a los progenitores o hablar con los alumnos (DeSmet *et al.*, 2015).

De la literatura analizada se deduce que el profesorado necesita una formación especializada para poder intervenir en aquellos casos en los que los jóvenes son objeto de ciberacoso, *cyberbullying* o comportamientos similares (Bevilacqua *et al.*, 2017).

También, es importante resaltar el esfuerzo que se hace por parte de los docentes para prevenir e intervenir en entornos escolares donde se producen comportamientos como el *ciberacoso*, el *cyberbullying* y otros similares, incluso fuera de los entornos virtuales (Nocentini *et al.*, 2015).

La formación, información y sensibilización es muy importante. Estudios recientes ponen de manifiesto el descenso en la incidencia del *cyberbullying* tras implementar programas de sensibilización. Con estos programas se consigue una mejora en la forma que tienen los

adolescentes de relacionarse en el ciberespacio al haber sido incluidos como temas de trabajo cuestiones referentes a la ciudadanía digital (Pozas *et al.*, 2018). Así, iniciativas recientes más específicas, que atienden a la problemática del *cyberbullying*, del *sexting* y del uso abusivo de las TIC, están teniendo resultados positivos entre los participantes (Del Rey y Ojeda, 2018).

En los últimos años se han publicado manuales y guías con recomendaciones y consejos para educadores y familias. Este material hace hincapié en el uso seguro de los teléfonos móviles y de los videojuegos y, por supuesto, de internet (Labrador *et al.*, 2015).

En esta línea, encontramos material esencial sobre estos temas en la *Guía para el buen uso de las nuevas tecnologías para familias y profesionales en el ámbito de la infancia*[3] o en la *Guía de seguridad en redes sociales para familias*[4]. Más específica es la *Guía de uso seguro y responsable de internet para profesionales de servicios de protección a la infancia*[5]. Dichas guías han sido editadas por el Centro de Seguridad en Internet para menores en España que presta servicios al Instituto Nacional de Ciberseguridad (INCIBE).

En definitiva, y por lo que se está viviendo actualmente, se vislumbra un cambio en la forma de enseñar, que se adapta (y se debe adaptar) al entorno tecnológico, lo que ha supuesto (y lo seguirá haciendo) un cambio importante para los estudiantes y profesores, ya que el peligro subyace en cada clic. Por ello, la formación del profesorado y de los entornos familiares en las conocidas (y cada vez más frecuentes) «escuelas de padres» es imprescindible con el objeto de evitar un mal uso de las nuevas tecnologías y conseguir proteger a los jóvenes.

7. La importancia de la detección por parte del sector educativo

Cuando ocurren hechos delictivos relacionados con las nuevas tecnologías a las que se encuentran expuestas los jóvenes, los peligros que encierran detrás suelen pasar desapercibidos para todo su entorno (padres, otros adultos y, por supuesto, profesores). La gran mayoría de las víctimas de delitos como el ciberacoso no se lo cuentan a ningún adulto ni solicitan ayuda de terceros para superarlo, y, lo que es más preocupante, en algunas personas con baja resiliencia, puede convertirse en un factor de riesgo del gesto autolítico.

Está demostrado que la detección de las conductas de intimidación o ciberacoso en los primeros estadios permite minimizar el daño, así como las consecuencias negativas que sufren las víctimas. Por ello, padres, profesores y otros adultos que están en contacto con

[3] https://www.octsi.es/images/documentos/2019/guia_buen_uso_tecnologias.pdf

[4] https://www.is4k.es/sites/default/files/contenidos/materiales/Campanas/is4k-guia-rrss.pdf

[5] https://www.is4k.es/sites/default/files/contenidos/guia_para_profesionales_de_servicios_de_proteccion_a_la_infancia.pdf

los menores deben estar, muy atentos a conductas y síntomas que puedan indicar la existencia de este tipo de victimización (Sánchez *et al.*, 2016).

Algunos de los indicadores que se encuentran en la base para que un menor llegue a ser víctima de este tipo de comportamientos delictivos pueden estar relacionados con el estado emocional, las costumbres, los hábitos, el rendimiento académico, las relaciones sociales o la alimentación. Es decir, según Sánchez *et al.* (2016), se pueden producir:

- **Cambios físicos o problemas psicosomáticos.** Sienten nauseas, dolor de cabeza, problemas intestinales o dolor de estómago; sufren insomnio, pesadillas, etc.
- **Cambios emocionales.** Tienen miedo a estar solos, a salir sin compañía a la calle; sufren estados depresivos, tristeza, apatía, etc.
- **Cambios en las relaciones sociales.** Los menores pasan el mayor tiempo del día solos, no quieren saber nada de los amigos, se produce un cambio repentino en su grupo de iguales, etc.
- **Cambios en el rendimiento académico.** No quieren ir al colegio, no se concentran en las actividades, se vuelven agresivos en clase, etc.
- **Cambios en el uso de las TIC.** Se dan de baja de las redes sociales, cambian la frecuencia de uso de los soportes electrónicos, bien por exceso o por defecto, sufren cambios de humor tras acceder a internet o a las redes sociales, evitan conectarse a internet en presencia de terceras personas, no quieren compartir con sus padres la identidad de las personas con las que interactúan en el ciberespacio, no desean recibir llamadas cuyo origen sea oculto, etc.

Para detectar la cibervictimización se utiliza el cuestionario CBV-44, que recoge las distintas formas de ciberacoso que puede sufrir la víctima. Consta de 26 preguntas perfectamente seleccionadas (Sánchez *et al.*, 2016).

Al analizar los factores que influyen en una prevención adecuada por parte del sector educativo no hay que olvidar las innumerables bondades de las TIC. Un uso inadecuado de las mismas acarrea riesgos a los que son más vulnerables los menores. Este tipo de herramientas ha propiciado una nueva forma de violencia entre iguales. El acoso (amenazas, insultos, etc.) que antes se suscribía al espacio escolar, ahora se hace de forma virtual (Sánchez *et al.*, 2016). Entre ellos podemos destacar el ciberacoso o el *cyberbullying* entre iguales para causar daño de forma deliberada. El *sexting,* el *grooming* o incluso la suplantación de la personalidad de otra persona. Pero el que más preocupa a padres y a educadores es el ciberacoso, debido a su rápida expansión y por las consecuencias que provoca en las víctimas. En palabras de Solberg y Olweus (2003), la definición de *bullying* incluye tres características: intencionalidad, desequilibrio de poder entre víctimas y agresores, así como la repetición de la conducta en el tiempo.

Así, varios informes del Defensor del Pueblo (2000 y 2007) alertaron de la necesidad de adoptar medidas para controlar el acoso entre escolares y mejorar la convivencia en las aulas. Sus recomendaciones fueron recogidas por las comunidades autónomas y plasmadas en normativas propias (Giménez-Gualdo *et al.*, 2021).

En esa línea, el informe de Save the Children (Sastre, 2016) recoge que los niños tienen el derecho de ser protegidos de todas las formas de violencia y de que se les facilite el desarrollo de todo su potencial de aprendizaje en un ambiente seguro; también inciden sobre estos temas la Convención de Naciones Unidas sobre los Derechos del Niño (1989) –que desarrolla el Comité de Derechos del Niño (ACNUDH [Alto Comisionado de las Naciones Unidas para los Derechos Humanos], 2011b) y el Comité de los Derechos Económicos, Sociales y Culturales (ACNUDH, 2011a)–, haciendo mención explícita al *cyberbullying* (Cerezo y Rubio, 2017).

En función de todo esto, la preventiva y corrección han de ser los objetivos principales de los centros escolares, dado que estas instituciones tienen un papel fundamental en la protección de la infancia contra cualquier tipo de violencia (Ortega y Núñez, 2012). Pero, en muchas ocasiones las aulas se convierten en escenarios de exclusión social y maltrato por parte de los niños. Es necesario contar con unos protocolos adecuados con la intención de intervenir de forma ordenada para erradicar cualquier tipo de violencia. Según Cerezo y Rubio (2017), antes de proceder a cualquier intervención, es preciso llevar a cabo una evaluación que permita implantar las medidas sancionadoras y educativas adecuadas, siempre respetando los derechos que reconoce la Convención de Naciones Unidas sobre los derechos del Niño, que defiende la sustitución de la represión y el castigo por medidas de índole rehabilitadora y restitutiva.

En ocasiones, al tratarse de hechos grupales, se deben tomar medidas hacia el grupo de iguales (Ortega, 2008). Así, la propia Constitución española de 1978, el preámbulo de la Ley orgánica 1/1990, de 3 de octubre, de ordenación general del sistema educativo y el Real Decreto 732/1995, de 5 de mayo, establecen los derechos y deberes de los alumnos, las normas de convivencia en los centros educativos y el carácter educativo y recuperador de las sanciones.

Es importante mencionar en este contexto la Ley orgánica 2/2006, de 3 de mayo, de educación (LOE). Esta reconoce en su articulado la importancia que tiene la institución escolar en la prevención y en la lucha contra determinadas conductas que se producen en dichos entornos, así como la educación basada en la no violencia. Como quedó patente anteriormente por las recomendaciones de los informes del Defensor del Pueblo, el llamamiento para una absoluta implicación de todos los sectores sociales, al objeto de prevenir e intervenir en todos estos casos tan pronto como existan indicios de cualquier comportamiento de los que se recogen en dichos textos, es imprescindible.

Por ello, se creó el Observatorio de la Violencia Escolar, a nivel nacional y en las distintas comunidades autónomas, desde donde se insta a todos los centros escolares a elaborar un plan de convivencia para ir en comunión con la LOE.

En nuestro ordenamiento no existe ninguna disposición que haga alusión a los fenómenos aludidos (acoso, ciberacoso*, bullying*, *cyberbullying*, etc.). La Ley orgánica 10/1995, de 23 de noviembre, del Código Penal sí señala implícitamente que quien inflija un trato degradante que menoscabe gravemente la integridad moral será castigado con la pena de prisión de seis meses a dos años. Pero en la mayoría de los casos el sujeto activo de este tipo de agresiones es un menor de edad (14 años) y, por consiguiente, inimputable, por lo que no se le puede aplicar esta norma penal (Fanjul, 2012). En el caso de ser mayor de 14 años y menor de 18 se le podría aplicar una responsabilidad penal especial y no ordinaria, como es la Ley orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal del menor.

En la misma línea, la Instrucción 1/2005 de la Fiscalía General del Estado alerta de conductas como el acoso, de la que reconoce su probabilidad de incidencia y para lo que propone abierta y públicamente la necesidad de sancionar siempre este tipo de comportamientos, haciendo partícipes a los agentes de socialización, primarios y secundarios.

Por todo lo expuesto, sería necesario contar con un marco normativo actualizado que aborde todos los comportamientos aquí señalados, es decir, además de los cometidos en el medio *offline*, también los perpetrados a través de las TIC en escenarios *online.*

Así, varias comunidades autónomas han creado sus propias normativas, que recogen una intervención específica. Al tener cedidas las competencias de educación, estas son diferentes en cada comunidad. Alguna de ellas ha creado órganos de control y ha establecido instrumentos normativos, recogidos en leyes, decretos, órdenes y/o resoluciones, para hacer frente al acoso escolar (Cerezo, 2015).

También se han elaborado los planes de convivencia. Estos planes no dejan de ser el marco de certificación para el control, la gestión y la monitorización del *bullying* y del *cyberbullying*, pues su misión es analizar estos fenómenos. En función de esto, se elaboran protocolos que regulan la forma de estudiar y regular los procesos (Viana-Orta, 2013).

8. Consejos de ciberseguridad

Con la finalidad de contribuir a la ciberseguridad, en este artículo se proponen una serie de medidas fundamentales para psicoeducar a los profesionales de la educación que en su quehacer diario trabajan con niños y adolescentes a través de las aulas virtuales y *offline*:

- No existe una edad cronológica idónea para administrar un dispositivo electrónico a un niño. Está más relacionado con el grado de madurez del menor y con el control parental que los padres siempre deben vigilar.
- Nunca se deben proporcionar datos e información personal.

- Hacer uso de la configuración «privado». Cuando se publican contenidos en la esfera pública, automáticamente se está permitiendo que todas las personas, incluidas aquellas que no tienen cuenta en una red social, accedan y puedan «usar» la información facilitada.
- Custodiar la información que se tenga en dispositivos de almacenamiento externos mediante cifrado o contraseña y no facilitar estas contraseñas a nadie.
- Realizar copias de seguridad diariamente o con relativa frecuencia.
- Analizar, mediante un antivirus, los archivos adjuntos de los correos electrónicos.
- Actualizar periódicamente el *software* del sistema operativo de los dispositivos para reducir su vulnerabilidad.
- Utilizar contraseñas seguras y cambiarlas una vez cada tres meses.
- Instalar antivirus y aplicaciones *antimalware.*
- Cerrar siempre las sesiones al abandonar las redes sociales.
- Activar el Firewall del sistema para bloquear accesos no autorizados.
- Desconectarse de internet cuando no se utilice para evitar que intrusos se conecten a la red y a los equipos.
- Proteger la red wifi con contraseñas robustas.
- No compartir la cuenta de usuario con nadie. En el móvil se puede instalar App Lock para crear contraseñas en las aplicaciones.
- Consultar con expertos en seguridad informática por si el dispositivo personal presenta geolocalizadores, aplicaciones espía o similares.
- Siempre que se reciba un *e-mail* o una *pop-up* (ventana emergente) con un mensaje en el cual se solicite información personal financiera o de cualquier otra índole, es importante que jamás se responda, pero, además, tampoco habrá que hacer clic en los enlaces que puedan aparecer en el mensaje.

La Agencia Española de Protección de Datos (AEPD)[6] desarrolló recursos de gran relevancia en materia de ciberseguridad para las víctimas, como un *Catálogo de medidas*

[6] En el ejercicio de las competencias que le atribuye el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, tiene como misión velar por el cumplimento de la legislación sobre protección de datos. Entre las acciones con esta finalidad se encuentran las de promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de los mismos, promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben y facilitar información a cualquier interesado en relación con el ejercicio de sus derechos (www.aepd.es).

preventivas y herramientas para proteger la privacidad en la red[7] con enlaces a la web de la Oficina de Seguridad del Internauta del INCIBE. También destaca *Privacidad y seguridad en internet*, una guía dirigida a las cibervíctimas, donde se pueden encontrar un montón de fichas realizadas en colaboración con el INCIBE[8]. Por último, es interesante conocer que en la web de la AEPD[9] existe información sobre seguridad tecnológica para poder navegar en modo incógnito sin dejar rastro en el historial de navegación.

Por todo lo anteriormente expuesto, y siguiendo con uno de los objetivos principales de este trabajo (diseñar información divulgativa, informativa, práctica y real sobre los riesgos del ciberespacio), hemos diseñado unas fichas informativas (véanse anexos 1 y 2) con el objetivo de informar sobre los comportamientos delictivos *online* que pueden tener lugar entre los estudiantes, si bien es preciso puntualizar que estos pueden darse a cualquier edad. La ficha del anexo 1 está enfocada a describir los diferentes tipos de violencia. La ficha del anexo 2 ha sido diseñada para informar a las víctimas sobre medidas y recursos de ciberseguridad.

Del mismo modo que iniciativas como la *Guía para uso seguro y responsable de internet por los menores: itinerario de mediación parental*[10] se convirtió en una magnífica herramienta de ayuda para padres, se pretende, con esta iniciativa, desarrollar material divulgativo con información relevante, útil y práctica tanto para los profesionales como para las víctimas.

Es indudable que profesores y educadores forman parte del colectivo de profesionales que, de manera directa e indirecta, trabajan tanto en la prevención como en la respuesta a la víctima una vez que el delito se ha efectuado. Por este motivo es imprescindible que los docentes estén sensibilizados y concienciados y que comprendan de manera exhaustiva todas las formas de ciberviolencia, así como los medios cibernéticos por los que pueden cometerse estos delitos. Es imprescindible que se encuentren en disposición de detectar dicha violencia, así como de prevenir la victimización.

9. Conclusiones

El cibercrimen es un fenómeno global que afecta a todos los Estados y no tiene fronteras. La superficie de ataque continúa creciendo cada vez más a medida que la sociedad se digitaliza, afectando a más ciudadanos, empresas, servicios públicos y dispositivos que se conectan a internet.

7 https://www.aepd.es/es/áreas-de-actuación/recomendaciones/medidas

8 https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-y-seguridad-en-internet.pdf

9 https://www.aepd.es/es/areas-de-actuacion/recomendaciones/informacion

10 https://www.observatoriodelainfancia.es/ficherosoia/documentos/4979_d_osi_menores_guia_mediacion_parental_internet.pdf

Los dispositivos electrónicos facilitan nuestras vidas la mayor parte de las veces, pero, también, se usan para agredir, humillar o extorsionar a otras personas.

Publicar imágenes, compartir a través de la red fotografías no consentidas o la humillación pública *online* son prácticas que han ido aumentando en los últimos años y que pueden provocar devastadoras consecuencias psicológicas en las personas y, especialmente, en los más jóvenes. Además, la amenaza real o percibida que puede sentir una víctima de que alguien está vulnerando su privacidad e intimidad, sus comunicaciones o sus imágenes más personales puede provocar pensamientos obsesivos de control, lo que, a su vez, podría desembocar en que esta persona se dé de baja en redes sociales o limite el acceso de sus conexiones cibernéticas, a riesgo de perder desde relaciones sanas de amistad hasta ofertas laborales de las que solo tiene acceso a través de la web.

Las diferentes redes sociales existentes comparten una serie de elementos comunes. Dichos elementos son el perfil; las herramientas de búsqueda, que permiten añadir al listado nuevos amigos o seguidores; las herramientas de comunicación, que incluso permiten enviar mensajes privados; la posibilidad de expresar el estado de ánimo con pocas palabras y de subir fotos y vídeos, etiquetando a personas, y que además pueden ser comentadas por otros usuario; por último, la posibilidad de crear grupos de interés, lo que permite a los usuarios compartir material que a veces puede ser peligroso o convertirse en un factor de riesgo para que se den determinadas conductas de tinte delictivo, en algunas ocasiones, y preocupantes, en otras muchas.

La sensibilización y la concienciación de la sociedad son fundamentales para prevenir la ciberdelincuencia, por ello, se deben adoptar las medidas de seguridad oportunas cuando se utilicen los sistemas de información, debiendo realizar un uso responsable para minimizar los riesgos en los entornos escolares.

Es imprescindible que por parte de los centros educativos se confeccionen guías y el resto de material FIS (protocolos, procedimientos, talleres, etc.) tanto para padres como para docentes. El objetivo final es enseñarles a detectar, prevenir y proteger a los menores frente a cualquier incidente que pueda ser indicador de alguno de los comportamientos que se han ido exponiendo en este artículo.

Como conclusión general se puede determinar que las TIC, incluyendo dentro de estas las redes sociales, ofrecen al ciberusuario un escenario adimensional donde poder operar en contra de sus cibervíctimas sin tener que interactuar con ellas de manera física, lo que no quiere decir que las consecuencias psicológicas negativas sean inferiores. Este universo virtual ofrece nuevos riesgos para las víctimas por lo que la educación y la inversión de recursos en ciberseguridad debe ser una obligación tanto a nivel personal como a nivel institucional.

Referencias bibliográficas

ACNUDH. (2011a). *Comité de los Derechos Económicos, Sociales y Culturales*. https://www.ohchr.org/SP/hrbodies/cescr/pages/cescrindex.aspx

ACNUDH. (2011b). *Comité de Derechos del Niño*. https:// www.ohchr.org/sp/HRBodies/CRC/Pages/CRCIndex.aspx

Alonso Ruido, P. (2017). *Evaluación del fenómeno del sexting y de los riesgos emergentes de la red en adolescentes de la provincia de Ourense* (Tesis doctoral). Universidad de Vigo.

Bermejo, B., Saul, L. Á. y Jenaro, C. (2011). La anorexia y la bulimia en la red: Ana y Mía dos «malas compañías» para las jóvenes de hoy. *Acción Psicológica*, *8*(1), 71-84. https://gredos.usal.es/handle/10366/123299

Bevilacqua, L., Shackleton, N., Hale, D., Allen, E., Bond, L., Christie, D. y Viner, R. M. (2017). The role of family and school-level factors in bullying and cyberbullying: a cross-sectional study. *BMC Pediatrics*, *17*. https://doi.org/10.1186/s12887-017-0907-8

Calderón-Cañola, S. (2010). Redes sociales virtuales: un medio efectivo en la prestación y distribución de servicios en línea. *Primer Simposio Brasileño de Ciencia de los Servicios*. https://docplayer.es/1715862-Redes-sociales-virtuales-un-medio-efectivo-en-la-prestacion-y-distribucion-de-servicios-en-linea.html

Castañeda Quintero, L., González Calatayud, V. y Serrano, J. L. (2011). Donde habitan los jóvenes: precisiones sobre un mundo de redes sociales. En F. Martínez e I. Solano, *Comunicación y relaciones sociales de los jóvenes en la red* (pp. 47-63). Marfil. https://www.researchgate.net/publication/255716910_Donde_habitan_los_jovenes_precisiones_sobre_un_mundo_de_redes_sociales

Cereceda Fernández-Oruña, J., Sánchez Jiménez, F., Herrera Sánchez, D., Martín Moreno, F., Rubio García, M., Gil Pérez, V., Santiago Orozco, A. M.ª y Gómez Martín, M. Á. (2018). *Estudio sobre la cibercriminalidad en España*. Ministerio del Interior. Gobierno de España. http://www.interior.gob.es/documents/10180/8736571/Informe+2018+sobre+la+Cibercriminalidad+en+E%20spa%C3%B1a.pdf/0cad792f-778e-4799-bb1f-206bd195bed2

Cerezo Ramírez, F. (2015). Bullying homofóbico. El papel del profesorado. *International Journal of Developmental and Educational Psychology*, *1*(1), 417-424.

Cerezo Ramírez, F. y Rubio Hernández, F. J. (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), 113-126.

Defensor del Pueblo. (2000). Violencia escolar: el maltrato entre iguales en la educación secundaria obligatoria. *Informes, Estudios y Documentos.*

Defensor del Pueblo. (2007). Violencia escolar: el maltrato entre iguales en la educación secundaria obligatoria 1999-2006 (nuevo estudio y actualización del informe 2000). *Informes, Estudios y Documentos.*

Del Rey Alamillo, R. y Ojeda Pérez, M. (2018). Claves para prevenir el acoso y el ciberacoso: la mejora de la convivencia y «ciberconvivencia» en los entornos escolares. *Participación Educativa*, *5*(8), 131-141.

DeSmet, A., Aelterman, N., Bastiaensens, S., Cleemput, K. van., Puels, K., Vandebusch, H., Gordon, G. y De-Bourdeaudhuij, I. (2015). Secondary school educators´ perceptions and practices in handling cyberbullying among adolescents: a cluster analysis. *Computers & Education*, *88*, 192-201. https://doi.org/10.1016/j.compedu.2015.05.006

Ditrendia. (2016). *Informe Ditrendia: mobile en España y en el mundo*. https://www.amic.media/media/files/file_352_1050.pdf

Fanjul Díaz, J. M. (2012). Visión jurídica del acoso escolar (bullying). Avances en supervisión educativa. *Revista de la Asociación de Inspectores de Educación de España*, *17*, 1-8.

García-Collantes. A. y Garrido, M. J. (2021). *Violencia y ciberviolencia de género*. Tiran lo Blanch.

Giménez-Gualdo, A. M., Galán-Casado, D. A. y Moraleda-Ruano, A. (2021). Competencias clave para la mejora de la ciberconvivencia escolar: el programa «Alumnos ayudantes TIC». *Education in the Knowledge Society (EKS)*, *22*, 1-11. https://doi.org/10.14201/eks.22168

Guadaño Narganes, Á. (2016). *El nuevo delito de acoso o acecho obsesivo («delito de stalking») del artículo 172 ter del Código Penal* (Trabajo de fin de grado). Universidad de Salamanca. http://hdl.handle.net/10366/135296

Iglesias, E. (2018). Inauguración del congreso. En E. Iglesias (Presidencia). *II Congreso Nacional de Violencia de Género Digital*. Asociación Stop Violencia de Género Digital, Madrid.

Instituto Andaluz de la Mujer. (2018). https://www.juntadeandalucia.es/institutodelamujer/index.php/inicio

Kemp, S. (2018). *Digital in 2018: World's Internet Users Pass the 4 Billion Mark: We are Social*. https://wearesocial.com/blog/2018/01/global-digital-report-2018

Labrador Encinas, F., Requesens Moll A. y Helguera Fuentes, M. (2015). *Guía para padres y educadores sobe el uso seguro de internet, móviles y videojuegos.* Fundación Guadium.

LeBon, G. (1896). *Psicología de las masas*. https://upcndigital.org/~ciper/biblioteca/Filosofia%20moderna/Psicologia-de-las-masas-G.-Le-Bon.pdf

Martínez Otero, J. (2017). La difusión de sexting sin consentimiento del protagonista: un análisis jurídico. *Derecom.* Nueva Época, *12*(2), 1-16.

Megías, I. y Rodríguez, E (2014). La imagen de los jóvenes en los medios de comunicación. Percepciones desde los propios jóvenes. En J. A. Alcoceba Hernando, I. Megías Quirós, T. Menéndez Hevia, B. Pueyo Ruiz y E. Rodríguez San Julián, *Jóvenes y medios de comunicación: el desafío de tener que entenderse* (pp. 10-19). Centro Reina Sofía sobre Adolescencia y Juventud. Fundación de Ayuda contra la Drogadicción (FAD).

Méndez-Lois, M. J., Villar-Varela, M. y Barreiro-Fernández, F. (2015). Estudio de los espacios virtuales como soportes para la violencia de género en la adolescencia. *Revista de Estudios e Investigación en Psicología y Educación*, *13*, 172-175. https://doi.org/10.17979/reipe.2015.0.13.525

Ministerio del Interior. (2021). *Estudio sobre la cibercriminalidad en España 2020*. http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3

Miró Llinares, F. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Montoro Fernández, E. y Ballesteros Moscosio, M. Á. (2016). Competencias docentes para la prevención del ciberacoso y delito de odio en secundaria. *Relatec*, *15*(1), 131-143. https://doi.org/10.17398/1695-288X.15.1.131

Nocentini, A., Zambuto, V. y Menesini, E. (2015). Anti-bullying programs and information and Communication Technologies (ICTs): A systematic review. *Aggression and Violent Behavior*, *23*, 52-60. https://doi.org/10.1016/j.avb.2015.05.012

Ortega Ruiz, R. (2008). *Malos tratos entre escolares: de la investigación a la intervención*. Ministerio de Educación, Política Social y

Deporte; Dirección General de Educación, Formación Profesional e Innovación Educativa; Centro de Investigación y Documentación Educativa (CIDE); Secretaría General Técnica.

Ortega Ruiz, R. y Núñez, J. C. (2012). Bullying and cyberbullying: research and intervention at school and social contexts. *Psicothema*, *24*(4), 603-607.

Pérez Orozco, A. y Cifuentes Bernal, B. (2008). Las madres comunitarias del Instituto Colombiano de Bienestar Familiar comprometidas con la atención integral de los niños en condiciones de pobreza y/o situación vulnerable. *Lumen. Instituto de Estudios en Educación*, *6*, 1-6. https://issuu.com/wilmarandresmartinezvalencia/docs/madrescomunitarias

Pozas Rivera, J., Morales Reynoso, T. y Martínez-Vilchis, R. (2018). Efectos de un programa de ciberviolencia en la prevención de ciberbullying. *Psychology, Society &* Education, *10*(2), 239 250.

Roberts, L. D. (Enero 2008). Jurisdictional and definitional concerns with computers-mediated interpersonal crimes: an anaysis on cyberstalking. *Internationational Journal of Cyber Criminology*, *2*(1), 271-285. https://bit.ly/2tWcZrr

Rodríguez-Álvarez, J. M., Cabrera-Herrera, M.ª C. y Yubero Jiménez, S. (2018). Los riesgos de las TIC en las relaciones entre iguales. Cyberbullying en educación primaria y secundaria. *Innoeduca. International Journal of Technology and Educational Innovation*, *4*(2), 185-192. https://doi.org/10.24310/innoeduca.2019.v5i1.3505

Sánchez Pardo, L., Crespo Herrador, G., Aguilar Moya, R., Bueno Cañigral, F. J., Aleixandre Benavent, R. y Valderrama Zurián, J. C. (2016). *Los adolescentes y el ciberacoso. Plan Municipal de Drogodependencias*. Unitat de Prevenció Comunitaria de Conductes Adictives (UPCCA).

Sastre, A. (Coord.). (2016). *Yo a eso no juego: bullying y ciberbullying en la infancia*. Save the Children. https://www.savethechildren.es/sites/default/files/imce/docs/yo_a_eso_no_juego.pdf

Solberg, M. y Olweus, D. (2003). Prevalence estimation of school bullying wiht the Olweus Bully/Victim Questionnaire. *Aggressive Behavior*, *29*, 239-268.

Streeter, C. L. y Gillespie, D. F. (1992). Social network analysis. En D. F. Gillespie y C. Glisson (Eds.), *Quantitative Methods in Social Work: State of the Art*. The Haworth Press.

UNICEF. (2006). *Convención de Naciones Unidas sobre los Derechos del Niño*. https://www.un.org/es/events/childrenday/pdf/derechos.pdf

Urueña, A. (Coord.). (2011). *Las redes sociales en internet*. ONTSI. https://www.ontsi.es//sites/ontsi/files/redes_sociales-documento_0.pdf

Viana-Orta, M.ª I. (2013). La mediación escolar en los planes y programas institucionales de convivencia en España. *Revista Complutense de Educación*, *25*(2), 271-291. http://dx.doi.org/10.5209/rev_RCED.2014.v25.n2.41458

Wasserman, S. y Faust, K. (1999). *Social Network Analysis: Methods and Applications*. Cambridge University Press.

ANEXO 1

FIS para profesionales de la educación (diferentes tipos de violencia)

Violencia *online*

Educadores, profesores y progenitores deben promover el uso responsable de las nuevas tecnologías al objeto de proteger la seguridad y la ciberseguridad de los menores.

Al igual que en otras disciplinas y campos, la importancia de la FIS se convierte en algo fundamental para evitar comportamientos delictivos en algunas ocasiones y preocupantes en otras muchas.

Tecnoconceptos → Tecnoadicción

- *Vamping* → Uso de dispositivos durante la noche.
- Nomofobia → Miedo irracional a estar sin el teléfono móvil.
- *Gambling* → Participar en juegos de azar a través de la red.
- *Infosurfing* → Navegar de forma continuada y prolongada sin un objetivo claro.
- *Hikikomori* → Casos extremos de aislamiento, como no salir de la habitación refugiándose en el mundo virtual.

Todos → forman parte de las llamadas «tecnoadicciones».

Constituyen

Atentados a derechos fundamentales:

- **Derecho a la intimidad.** Lee correos o mensajes.
- **Derecho al secreto de las comunicaciones.** Lee correos o mensajes antes de que la víctima lo haga.
- **Suplantación de identidad.** El victimario se hace pasar por la víctima en el ciberespacio.
- **Derecho a la libertad.**
- **Derecho a la propia imagen, dignidad, honor…**

¡Recuerda! Si una persona lee tu correo electrónico, una vez que está abierto es violación del secreto de correspondencia. Si no está abierto, es violación del derecho a la intimidad.

Cyberstalking

El *cyberstalking* o ciberacoso consistiría en una agresión psicológica, sostenida y repetida en el tiempo, perpetrada por los sujetos del artículo 1.1 de la Ley orgánica 1/2004 contra su pareja o expareja, utilizando para ello las nuevas tecnologías por medio de cualquier plataforma o escenario virtual.

Sextorsión es el chantaje, la coacción o el acoso que sufre cualquier persona víctima de las amenazas de una tercera persona al hacer público determinado material explícito de la misma.

Amenazas, control, desconfianza, etcétera. + TIC = *Cyberstalking*

Comportamientos *online*	
Hacking (piratería)	Uso de la tecnología para tener acceso ilegal o no autorizado a determinados sistemas o páginas con el propósito de obtener información personal, alterar o modificar información, calumniar o denigrar.
Suplantación de identidad	Uso de la tecnología para asumir la identidad de la víctima con el propósito de acceder a información privada, avergonzar o culpar a la víctima, o crear falsos documentos de identidad.
Surveillance/ tracking (vigilancia/rastreo)	Uso de la tecnología para acosar y monitorizar a la víctima y sus actividades.
Harassment/ spamming (acoso *spam*/ *cyberstalking*)	El uso de la tecnología para contactar continuamente con la víctima, molestarla, amenazarla o asustarla.
Recruitment (reclutamiento)	El uso de la tecnología para reclutar víctimas potenciales como se hace con el tráfico de seres humanos; por ejemplo, usando *chat rooms* y determinadas páginas web para comunicar o advertir los diferentes actos.
Doxing	Manipular y distribuir información difamatoria relacionada con la víctima, sin su consentimiento, que puede incluir contenidos con connotación erótica o sexual.
Phising	Recogida de datos necesarios para estafar al usuario.
Pharming	Manipular direcciones electrónicas para engañar al usuario y cometer fraude.

¡Ojo! → ***Sexting*** (envío de material con connotación sexual) **no es delito**.

Sí lo es el delito de *sexting* (envío de este material sin consentimiento).

Fuente: elaboración propia.

ANEXO 2

FIS para profesionales de la educación (medidas y recursos de ciberseguridad para las víctimas)

Conductas frecuentes de alarma

- Recepción de cartas, *e-mails*, mensajes y llamadas telefónicas a todas horas.
- En las redes sociales, el acechador vigilia, comenta o llega incluso a hackear la cuenta de la víctima con el fin de conocer cualquier cambio en su vida diaria.
- La víctima también puede sufrir allanamientos de morada.
- Y en los casos más graves y extremos puede recibir amenazas y sufrir algún tipo de delito de violencia.

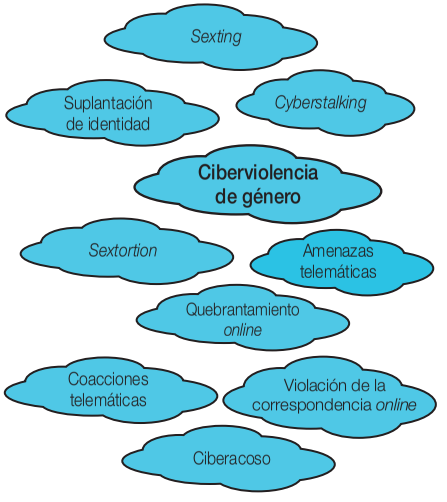
Consejos sobre la protección de la intimidad digital

- Desconecte los programas o aplicaciones de geolocalización.
- Use claves conocidas solamente por usted.
- Cambie claves cada tres meses.
- No suba a la red datos personales.
- Use antivirus que detecten la existencia de programas espía.
- Haga copias de seguridad diariamente.
- Actualice periódicamente el *software* del sistema para reducir la vulnerabilidad.
- Cierre siempre las sesiones al abandonar las redes sociales.
- Active el Firewall del sistema para bloquear accesos no autorizados.
- Proteja la red wifi.
- No comparta la cuenta de usuario con nadie. En el móvil se puede instalar App Lock para crear contraseñas en las aplicaciones.
- Consulte con expertos en seguridad informática por si el dispositivo personal presenta geolocalizadores, aplicaciones espía o similares.
- Desconecte de su dispositivo móvil la opción de «permitir ubicación».
- No suba información personal en las aplicaciones para búsqueda de trabajo.
- No se etiquete en las fotos compartidas y pida que no la etiqueten.
- Uso de contraseñas seguras:

Teléfonos y recursos urgentes

- Guardia Civil → https://www.guardiacivil.es
- Cuerpo Nacional de Policía → https://policia.es/_es/index.php
- Grupo de Delitos Telemáticos → https://www.gdt.guardiacivil.es
- Agencia Española de Protección de Datos → https://www.agpd.es
- Oficina de Seguridad del Internauta → https://www.osi.es/es
- Asociación Protégeles → http://www.protegeles.com
- Servicio Orientación Jurídica: 91 72 06 247
- 012
- Unidad de Atención a Víctimas con Discapacidad Intelectual (UAVDI): 900 335 533
- https://www.pantallasamigas.net
- Internet Segura for Kids: https://www.is4k.es/

Ciberviolencia de género y cibercontrol



¿Qué son? y ¿cómo protegernos?

La violencia de género se encuadra dentro de diferentes tipos penales en el Código Penal: delito de lesiones (art. 153.1), amenazas (art. 171.4), coacciones (art. 172.2) y contra la integridad (art. 177). Se le suma el agravante de parentesco si el victimario es pareja o expareja. De esta manera, la violencia de género es un delito transversal del Código Penal. Con las TIC, se cometen en el ciberespacio ciberamenazas, cibercoacciones, etc., además de nuevos tipos: *sextortion*, *cyberstalking*, etc.

Fuente: elaboración propia.