# Ciberacoso
## y violencia de género en redes sociales

### Análisis y herramientas de prevención

Coordinadora: María Ángeles Verdejo Espinosa

Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

# Capítulo III

# Seguridad y prevención en redes sociales. Responsabilidades legales y menores en Internet

*Juana María Morcillo Martínez*

**Resumen.** *Este trabajo de revisión analiza las cuestiones jurídicas y de normativa más relevantes y que afectan directamente al uso de las redes sociales. Además ponemos de manifiesto la importancia de una óptima labor educativa por parte de las familias y el colectivo docente que, a través de su experiencia, deben fomentar un buen uso de estos medios. Por otro lado, el imparable avance de las tecnologías de la información y la comunicación en la sociedad actual tiene que estar óptimamente regularizado. Este tratamiento masivo que las TIC posibilitan, puede acarrear riesgos para la intimidad. En este sentido, se hace necesario dotar de protección específica a los derechos del individuo, pero señalamos de forma especial los derechos de los niños y niñas.*
**Palabras clave:** *Prevención en redes sociales, Responsabilidades legales, Libertades de expresión y Menores.*

**Abstract.** *This review paper discusses the relevant legal and regulatory issues that directly affect social networks. All this must be complemented with an important educational efforts by families and teachers who, through their experience, should encourage good use of these media. In addition, the unstoppable advance of information and communications technology in today's society must be optimally regularized. This massive treatment that enable ICT can bring privacy risks. In this sense, it is necessary to provide specific protection of individual rights, but noted specially the rights of minors.*



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

**Keywords:** *Prevention on social networks, legal responsibilities, freedoms of expression, Minors.*

## 1. Introducción.

Este trabajo de revisión analiza por un lado, la normativa existente en relación a la seguridad y prevención en redes sociales y, por otro, indaga sobre como las nuevas tecnologías, ordenadores y con estos la "red de redes" [Internet] en los últimos años han entrado a formar parte de la vida cotidiana de las personas adultas que nos hemos ido adaptando al fenómeno con cierta dificultad. Sin embargo, los jóvenes, adolescentes [o preadolescentes] o incluso niños y niñas, no han precisado tal esfuerzo de asimilación.

En este sentido unos y otros a través de las nuevas tecnologías [teléfonos móviles, Internet…], nos hemos acostumbrado a comunicarnos, a divertirnos, a jugar, a encontrar nuevas vías de conocimiento de realidades o personas, a relacionarnos, etc. Pero igual que ha ocurrido con otros muchos inventos, lo que puede servir para tantas cosas positivas, puede servir para lo contrario, para desarrollar conductas negativas e incluso delictivas dirigidas hacia otras personas.

Así mismo, se ha llegado a hablar de "delincuencia informática" o "delitos cometidos a través de nuevas tecnologías", para catalogar fenómenos delictivos relativamente novedosos y en cualquier caso de reciente aparición.

Del mismo modo, la rápida emergencia de un mercado liberalizado de comunicación global, y el uso popular de Internet han traído como consecuencia el cuestionamiento de medios tradicionales de distintas normas de regulación. En esta nueva sociedad, el sector de las telecomunicaciones es crucial y lo convierte en balaustre del proceso de informati-



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

zación. La seguridad que se le exige a la red es mucho mayor que la que han ofrecido hasta ahora los medios tradicionales.

Es importante destacar que Internet implica un medio para muchos atentados contra derechos, bienes e intereses jurídicos. Su potencialidad en la difusión de imágenes e información la hace un medio rápido para atentados contra cuatro tipos de bienes básicos:

- La intimidad, la imagen, la dignidad y el honor de las personas.
- La libertad sexual.
- La propiedad intelectual e industrial, el mercado y los consumidores.
- La seguridad nacional y el orden público.
- La seguridad de la información transmitida.

Así, entre estas problemáticas podemos encontrar:

- Filtración de información confidencial: datos personales, secretos profesionales o información reservada de una empresa.
- Monitoreo de acceso o control de una persona, en la red.
- Protección contra manipulación de datos personales.
- Posibilidades de recoger datos contenidos en la información por medio de programas que se instalan.
- Intromisión a la intimidad a través del correo basura y el no deseado.
- Protección a menores contra la pornografía y obscenidad, sin violar los derechos de libertad de expresión e información de los adultos.

Añadiremos que la vida *online* trae consigo riesgos potenciales, como ciberacoso y/o exposición a contenidos inapro-



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

piados. Un aspecto clave es la confianza que niños y niñas tengan en la mediación de los padres, madres, cuidadores y docentes. La rápida diseminación de dispositivos móviles y el aumento del acceso a Internet en espacios privados, obliga a ir más allá de enfoques restrictivos, pues la mejor forma de proteger a niños, niñas y adolescentes es utilizar estrategias basadas en una activa mediación del uso de Internet.

Por lo tanto, es fundamental la configuración de unas leyes que regulen la materia y penalicen las conductas perjudiciales. Todo ello se debe complementar con una importante labor educativa por parte de las familias y los docentes que, a través de su experiencia, deben fomentar un buen uso de estos medios.

## 2. La normativa existente y su utilización para la prevención de los menores ante las nuevas tecnologías

En la actualidad Internet es una de las mayores evidencias del progreso social, económico y político de nuestros tiempos, haciendo accesible la información y la comunicación a nivel global en cualquier parte del mundo. Sin embargo, también puede ser utilizado para perpetrar acciones delictivas que atacan a valores jurídicos protegidos, como son la libertad, la intimidad personal y familiar, la propia imagen, la dignidad humana, etc.

Del mismo modo señalamos que las TIC son un aspecto importante en la vida de niños y niñas, por lo que es esencial considerar las oportunidades y los riesgos que conllevan. La Convención sobre los Derechos del Niño[1] provee aspectos

1 Para más información véase UNICEF (2015). Únete por la infancia. Disponible en http://www.unicef.es/infancia/derechos-del-nino/convencion-derechos-nino.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

importantes relacionados con los derechos de la infancia y los medios de comunicación. Particularmente, los artículos 13 y 17 establecen el derecho de los niños y niñas a acceder a información desde diferentes fuentes, incluyendo Internet. El artículo 12 remite a su habilidad para forjar sus propias opiniones y garantiza su derecho a la libertad de expresión. La naturaleza abierta de Internet configura un espacio para la socialización, participación y expresión. De hecho, niños, niñas y adolescentes pueden convertirse en autores y publicar en blogs, sitios de vídeos y otras plataformas; es decir, no son destinatarios pasivos de la información *online* sino actores que le dan forma a Internet.

En consecuencia, es esperable que las administraciones competentes y la sociedad les aseguren los recursos necesarios para que accedan a la información y aprendan a utilizarla. Un gran desafío es cómo equilibrar la protección con el empoderamiento *online* en la relación entre padres, madres, hijos e hijas.

En lo que se refiere a los/as menores, en los últimos años, esta gran herramienta educativa ha demostrado ser un arma de doble filo, ya que engendra muchos peligros para los más vulnerables. Son muchos los riesgos que corren los niños/as navegando por Internet si no siguen los consejos de una navegación segura y no han recibido una correcta información acerca de los peligros y trampas que les acechan. Este colectivo tiene que valorar la comunicación física por encima de la que pueden entablar a través de las nuevas tecnologías. Las ventajas de conocer al interlocutor frente a los riesgos de no hacerlo.

Por otro lado, su educación es la base de un futuro Internet más seguro. Así, es importante decirles que tienen que tener en cuenta que hablar habitualmente con una persona en Internet, no le convierte en conocido. La adicción a las nuevas tecnologías es un problema en alza que los padres y



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

madres no deben descuidar y darle la importancia que tiene. El tiempo que pasen sus hijos e hijas en Internet tiene que estar limitado, según sean las motivaciones de uso de la red y la edad.

En este sentido y según la Agencia de Calidad de Internet [IQUA],[2] estos peligros se podrían clasificar de la siguiente manera:

1. **Personales**. Aquellos riesgos que consisten en la existencia de distintos acosadores que utilizan los foros, los chats y los programas de mensajería instantánea tipo Messenger y Skype para lograr captar a sus víctimas, menores de edad, fáciles de engañar y mucho más accesibles que cualquier otra persona.
2. **De contenido**. Estos peligros se refieren al acceso, voluntario o involuntario, a contenidos como imágenes,

2 La Agencia de Calidad de Internet (IQUA) es una entidad de ámbito estatal sin ánimo de lucro, creada el 21 de octubre de 2002, que quiere ser un referente común para la Administración, las empresas, los operadores, las asociaciones, los usuarios, tiendas y los técnicos que trabajan en la mejora y la calidad en Internet. Del mismo modo, señalamos que el objetivo principal de IQUA es la confianza y seguridad en la red, mediante la autorregulación y el otorgamiento del sello de calidad IQ. Y, los ámbitos de actuación son los siguientes: 1) Velar por la calidad de Internet; 2) Desarrollar la sociedad de la información; 3) Promover la autorregulación en Internet; 4) Otorgar un sello que acredite la calidad de las páginas web; 5) Defender los derechos de los usuarios de la red; 6) Realizar estudios e informes sobre los contenidos de la red; 7) Actuar como plataforma de debate y reflexión; 8) Tramitar quejas y sugerencias; 9) Resolver extrajudicialmente conflictos relacionados con Internet; y 10) Actuar como plataforma de mediación y arbitraje. En este sentido, el Código Deontológico de IQUA se refiere a aquellos principios generales que deben ser respetados para la defensa del interés general y de los derechos de los ciudadanos. IQUA pretende que el desarrollo de la Sociedad de la Información tenga lugar bajo el respeto de unos principios éticos que considera fundamentales. Para más información, véase: IQUA.es (2013), disponible en: http://www.iqua.es.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

vídeos o textos violentos, de carácter sexual, racista, xenófobo o sectario, no apto para todos los públicos.

3. **De adicción**. Este riesgo se refiere al comportamiento que pueden adquirir los/as menores, igual que los adultos, de dependencia del uso de Internet, también llamado "desorden de adicción a Internet".

La necesidad de conocer y saber utilizar Internet es una condición primordial en la sociedad actual, por lo que la protección, en todos sus términos, no debe privar a los/as menores de esta herramienta, imprescindible en su vida laboral. La prohibición y el control no representan el camino hacia una navegación segura y responsable de los menores. Es importante enseñarles a utilizar esta herramienta con criterio, haciendo un buen uso de los muchos beneficios que aporta, pero también es necesario darles a conocer la manera de afrontar determinadas situaciones.

Consecuentemente, los sistemas educativos no sólo están obligados a adaptarse a los cambios tecnológicos, sino que tienen un enorme protagonismo en la generación de estos cambios y en la apropiación social de las tecnologías producidas.

Esta dinámica de integración de la tecnología en el entramado social y económico debe entenderse como un proceso secuencial, caracterizado por fenómenos muy diferenciados en cada una de las fases de desarrollo. Habitualmente, en los primeros momentos de implantación de una innovación, la cultura, las actitudes y los valores de uso no están todavía bien configurados, de manera que son frecuentes los riesgos de adicción y de dependencia, la posibilidad de indefensión o desregulación ante determinados riesgos que la tecnología genera, las actitudes de rechazo o la inflación de expectativas.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

No obstante, esta política preventiva no debe caer en la tentación de la tecnofobia, o adicción a Internet y a las nuevas tecnologías,[3] en el pesimismo sobre la tecnología o la exageración de los riesgos. La idea de posponer, limitar o reducir el uso de la tecnología entre los jóvenes no es el escenario que debe orientar la actuación. El riesgo de la tecnofobia es grave, porque supone cerrarse al progreso y, además, porque es una actitud que no está justificada, se basa en estereotipos y, con frecuencia, es consecuencia de la brecha tecnológica que se establece entre las generaciones y que separa claramente a docentes y alumnos.

Frente a esta tecnofobia, se propone la tecnofilia constructiva, basada en un optimismo razonable sobre las aportaciones de las Nuevas Tecnologías y en una gestión responsable de sus posibles riesgos. Esta actitud se concreta en una educación para el uso autónomo de la tecnología, en una investigación sobre el potencial de los artefactos para el desarrollo de una educación personalizada y para el uso de todas las posibilidades que tiene la tecnología en el desarrollo profesional, ciudadano y personal de los alumnos.

3 Cuando hacemos alusión al término tecnofobia nos referimos a la adicción a Internet y a las nuevas tecnologías. La tecnofobia puede manifestarse de diferentes maneras que van desde un impulso irracional por adquirir todo aquello que está en la punta del avance tecnológico, hasta aquellos que han encontrado en las tecnologías una forma de resignificar un entorno vacío y carente de experiencias valiosas. En el primer grupo podemos encontrar a muchas personas que llegan a obsesionarse con acceder a "lo último" en conexiones a Internet, móviles, videojuegos o electrodomésticos, por nombrar sólo algunos. En cambio el segundo grupo está conformado por personas que son reflejo de unas carencias psicológicas primarias como, la falta de objetivos, las dificultades para establecer relaciones interpersonales, la pobreza en las habilidades sociales, la timidez, la soledad o la baja autoestima. No está claro si estos rasgos son la causa o la consecuencia del uso abusivo.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Hoy en día, la población joven está utilizando la tecnología de muchas formas, enriqueciendo así sus conocimientos con la variedad de instrumentos que se ofertan en la red. Con la aparición de las tecnologías Web 2.0 [tecnologías web que fomentan la colaboración *online* y el intercambio entre los usuarios], la población joven ya no es sujeto pasivo en el intercambio de la información virtual, sino que se transforman en creadores de contenidos digitales, utilizando así los instrumentos de software social.

El informe realizado por el Observatorio de las Telecomunicaciones y de la Sociedad de la Información,[4] en el año 2011 y relativo a la infancia y la adolescencia en la sociedad de la información, determina una relación muy positiva entre los menores de 18 años y las Nuevas Tecnologías. En comparación con la relación que tiene la población adulta con estas tecnologías, los menores de 18 años se ven más animados/as a probar los nuevos avances, se sienten más identificados con las tecnologías, a las que no consideran una barrera para la comunicación, y no les frena su posible complejidad de uso. Además, las consideran una herramienta útil en su desarrollo personal, ven más clara su utilidad que los adultos y muestran más interés por las mismas, aunque las consideren caras.

Otro estudio, elaborado por INTECO,[5] concluye que el primer contacto con Nuevas Tecnologías, y más concretamente con Internet, se produce entre los 10 y 11 años. Este dato reivindica la tan utilizada y conocida expresión "nativos digitales", que fue acuñada por Marc Prensky y que describe

4 Para más información véase: Fundación Orange-E-spaña (2011): Informe anual sobre el desarrollo de la sociedad de la información en España.

5 Para más información véase: INTECO (2009): Estudio sobre los hábitos seguros en el uso de las nuevas tecnologías por niños y adolescentes y e-confianza de sus padres. Observatorio de la Seguridad de la Información.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

a los/as estudiantes, menores de 30 años, que han crecido con la tecnología y que desarrollan una habilidad innata en el lenguaje y en el entorno digital. Para esta nueva generación, las Nuevas Tecnologías representan una parte central y clave en sus vidas, ya que dependen de ellas para realizar muchas actividades cotidianas como estudiar, relacionarse, comprar, informarse o divertirse.

Sin embargo, y a pesar de la aparente familiaridad de los/as jóvenes con esta nueva tecnología y de la sensación de control o inocuidad que experimentan, la red se desarrolla cualitativa y cuantitativamente en direcciones no siempre deseables, y a una velocidad que hace difícil el establecimiento de medidas mitigadoras de los posibles impactos perjudiciales sobre el crecimiento emocional y personal de los adolescentes. El informe INTECO, antes mencionado, determina también que 84,5% de los/as menores de 18 años son capaces de dar una respuesta, en cuanto a las medidas que toman, ante la incidencia de un riesgo de las Nuevas Tecnologías. El 15,5% restante ofrece respuestas como cerrar la conexión o salirse de la web o chat, negarse a hacer lo que le piden y pedir ayuda a sus padres o madres [sólo un 1,1% de los/as niños/as declara esta opción].

En cuanto a los padres, ellos y ellas siguen principalmente medidas de tipo físico o técnico entendiendo por medidas físicas aquellas que implican una actuación sobre el equipo). En mucha menor medida, los padres mencionan medidas educativas y coercitivas. Las medidas educativas engloban aquéllas que implican el diálogo, la advertencia o la formulación de recomendaciones. Las medidas coercitivas implican el establecimiento de algún tipo de limitación o control [horario, supervisión...]. Por último, sólo un 0,3% de los padres inicia acciones de denuncia ante las autoridades oportunas. Un 3% no hace nada, y más de un 16% no es capaz de dar una respuesta.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Sin duda, estas Nuevas Tecnologías conllevan nuevos riesgos, pero es importante tener en cuenta que esta nueva generación también es capaz de auto regularse si está bien informada sobre los distintos niveles de riesgo. Las escuelas tienen el deber de enseñar a su alumnado a permanecer seguros cuando navegan en Internet, ya sea dentro del centro educativo o fuera. Si los centros educativos empiezan a utilizar cada vez más estas Nuevas Tecnologías, reconociendo que sus beneficios educativos y sociales son mucho mayores que los peligros que engendran, la flexibilidad de su currículo se aumentará cada vez más eficaz y eficientemente.

Por otro lado, el imparable avance de las tecnologías de la información y la comunicación en la sociedad actual tiene que estar regularizado. Este tratamiento masivo que las TIC posibilitan, puede acarrear riesgos para la intimidad, lo que hace necesario dotar de protección específica a este ámbito de los derechos del individuo. En este sentido, y en una primera aproximación al tema nos encontramos con las siguientes:

## 2.1. La normativa de marco general

- Declaraciones Universales:
  - Declaración Universal de los Derechos Humanos [art12]. "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

## 2.2. A nivel internacional

- **La Resolución de 27 de febrero de 1996 del Consejo de Telecomunicaciones de la Unión Europea** para impedir la difusión de contenidos ilícitos de Inter-



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

net, especialmente la pornografía infantil, que propone medidas para intensificar la colaboración entre los estados miembros, independientemente de que cada uno de ellos aplique la legislación que exista en su país sobre la materia.

- **El Libro Verde sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información (1996)** de la Unión Europea tiene por objeto profundizar el debate sobre las condiciones necesarias para la creación de un marco coherente para la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información.

  De la misma manera, plantea diferentes posibilidades para reforzar la cooperación entre las diferentes administraciones nacionales: intercambio de informaciones, análisis comparado de sus legislaciones, cooperación en los marcos de la justicia y de los asuntos interiores.

  Por las características de Internet no cabe duda que aplicar soluciones globales es difícil, pero no debe abandonarse el empeño por buscar las que sean más compatibles para los Estados Miembros.
- **La Recomendación 98/560/CE del Consejo de la Unión Europea** es el primer instrumento jurídico elaborado para la protección de los menores antes los contenidos perjudiciales o ilegales de Internet. Esta Recomendación se ideó a raíz del Libro Verde de 1996 sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información, que fue el inicio de un debate a escala europea sobre la dimensión ética de la sociedad de la información y sobre la forma en que el interés general puede protegerse en los nuevos servicios.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

- **La Recomendación 2006/952/CE**, que completa la Recomendación 98/560/CE, invita a dar un paso más hacia la instauración de una cooperación eficaz entre los Estados miembros, la industria y las demás partes interesadas en materia de protección de los menores y de la dignidad humana en los sectores de la radiodifusión y de los servicios de Internet.
- **La Directiva 95/46/CE** se aprueba con la voluntad de acercar las legislaciones estatales de protección de datos personales de los Estados Miembros de la Unión. La transposición de esta directiva en los distintos Estados debe establecer, entre otros aspectos, el régimen de infracciones y sanciones que habrá que aplicar en caso de incumplimiento de las disposiciones adoptadas en la materia. Por otra parte, la legislación penal protege también ciertos ámbitos del derecho a la intimidad en los ordenamientos jurídicos de los diferentes Estados.

## 2.3. A nivel estatal

- **La Constitución Española** regula la protección de los menores en diferentes artículos. Así, el artículo 20.4 limita la libertad de expresión, de información y de cátedra, *"… en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia".* Por su parte, el artículo 39.4 del mismo texto determina que; *"… los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos".*

  Del mismo modo, El Art. 18 de la "Constitución española de 1978" establece que: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la*



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

*propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas.*

- **La Ley Orgánica 2/2006, de 3 de mayo, de Educación**, establece el marco de los derechos y deberes en materia de educación. Tres son los principios que presiden esta Ley, el primero la exigencia de proporcionar una educación de calidad a todos los ciudadanos, al mismo tiempo garantizar una igualdad efectiva de oportunidades, el segundo la necesidad de que todos los componentes de la comunidad educativa colaboren para conseguir ese objetivo. El tercer principio consiste en un compromiso decidido con los objetivos educativos planteados por la Unión Europea para los próximos años, dirigidos hacia una cierta convergencia de los sistemas de educación y formación.
- **La Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor**, impone la obligación a toda persona o autoridad de comunicar a la autoridad o sus agentes las situaciones de riesgo que puedan afectar a un menor sin perjuicio de prestarle el auxilio inmediato que precise. Esta Ley aborda una reforma en profundidad de las tradicionales instituciones de protección del menor reguladas en el Código Civil, pretende construir un amplio marco jurídico de protección que vincula a todos los Poderes Públicos, a las instituciones específicamente relacionadas con los menores, a los padres y familiares y a los ciudadanos en general. En esta Ley, también se manifiesta la preocupación por agilizar y clarificar los trámites de los procedimientos administrativos y judiciales que afectan al menor, con



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

la finalidad de que éste no quede indefenso o desprotegido en ningún momento.

Concluimos este apartado exponiendo que la protección legal representa el paso inicial fundamental para asegurar unos hábitos adecuados de uso de Internet. En este sentido, la mayor parte de los problemas que podemos encontrarnos en Internet se producen básicamente como consecuencia de no respetar toda una serie de normas básicas de seguridad.

## 3. Consejos de prevención en el uso de redes sociales: ¿qué datos tengo que proteger?

En la Ley de Protección de Datos se define dato personal toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Actualmente, la privacidad alcanza una dimensión especial y distinta como resultado del uso masivo de las nuevas tecnología, Internet y más en concreto, las redes sociales. Estas últimas se han convertido en grandes fuentes de información sobre todos sus miembros y usuarios. Por este motivo, insistimos en tener precaución cuando hacemos públicos nuestros datos personales.

En España, la edad de acceso de los usuarios a las redes sociales se ha establecido en los 14 años, tomando como base lo establecido en el Código Civil y la Ley de Protección de Datos, que otorgan la capacidad de los mayores de 14 años de poder facilitar sus datos personales de forma directa. El problema es que en la práctica, hay considerables menores de 14 años que ingresan o acceden en distintas redes sociales de forma irregular, sencillamente falsificando su fecha de na-



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

cimiento. Lamentablemente, hasta la fecha no existen sistemas de control de edad eficaces y objetivos. Los mecanismos de control empleados en la actualidad son:

1. Las denuncias de otros usuarios.
2. Rastreos de perfiles llevados a cabo por la propia red social.
3. Control parental.

Por otro lado, y en lo que respecta a la protección de datos, los usuarios de servicios de redes sociales deben tener en cuenta que pueden incurrir en los siguientes riesgos:

Al darse de alta:

- Nos solicitan excesivos datos de carácter personal.
- Damos consentimiento al administrador para usar nuestros datos.
- No restringir la visibilidad de nuestros datos. Perfiles privados.

Mientras se está en la red:

- No controlar la información e imágenes que se publican.
- Cuando publicamos imágenes (fotografías y videos) cualquiera puede copiarlas, manipularlas y distribuirlas.
- Las imágenes dan mucha información que puede poner en riesgo al menor, a sus conocidos/as y familiares: Permiten localizar al menor.
- La información que se publica puede permanecer toda la vida.
- En perfiles púbicos o en aquellos en los que existen un gran número de amigos o agregados, es necesario solicitar autorización para publicar imágenes de terceras personas.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Al darse de baja:

- Eliminar perfil no es lo mismo que desactivarlo.
- Conservación de datos por parte del administrador Red.

Y, como protocolo de actuación en casos de vulneración del derecho a la intimidad, es importante:

- Guardar pruebas de los hechos o de las evidencias electrónicas existentes: Imprimiendo pantallazos.
- Grabando la información en un disco, *pen-drive*, etc.
- Tomando imagen de la pantalla mediante una cámara fotográfica, donde aparezcan fechadas las fotografías.
- Ponerse en contacto con los Administradores de la red social para solicitar la salvaguarda de la información a efectos de posibles denuncias. Del mismo modo, solicitar cancelaciones de datos personales, comentarios o textos.
- Ponerse en contacto con los posibles buscadores que hayan indexado los contenidos solicitando su bloqueo o retirada.
- Denunciar ante la Agencia Española de Protección de Datos.
- Emprender acciones judiciales, Civiles y/o Penales.

Conjuntamente, a lo anteriormente expuesto, tenemos que:

- Utilizar siempre un antivirus para la seguridad de tu ordenador y analiza con él cualquier archivo que te descargues. Es importante actualizar con frecuencia el antivirus.
- Utilizar también un programa anti-*spyware* para evitar la entrada de programas espías o troyanos.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

- Cuando accedas a tus redes o correo electrónico desde algún lugar público, asegúrate de desactivar las casillas de "recordar contraseña", "recordarme" y/o "no cerrar sesión", y de cerrar la sesión antes de cerrar las ventanas.
- Nunca te fíes de los extraños, un desconocido/a, no es tu amigo o amiga, aunque mantengas una relación *online* con él/ella, sigue siendo un desconocido/a, no puedes comprobar que es quien dice ser.
- No acuerdes nunca citas con personas desconocidas, si tienes mucho interés en hacerlo, hazlo en un lugar público (nunca en un domicilio privado), y siempre ve acompañado/a por algún amigo/a, o mejor, por una persona adulta de confianza.
- No grabes ni publiques imágenes o vídeos sin el consentimiento de las personas que aparecen y mucho menos las etiquetes sin su consentimiento. Cuando publicas una foto o escribes en los muros, puedes estar incluyendo información sobre otras personas. Respeta sus derechos y sé consciente de tu responsabilidad, personal y jurídica.
- Garantiza tu seguridad mediante una configuración adecuada de tu privacidad, la privacidad más segura es aquella en la que sólo personas a las que tú has aceptado como "amigos" o "usuarios" pueden ver tu perfil: privacidad "amigos de amigos". Utiliza contraseñas adecuadas. Busca una contraseña que sólo sepas tú y no sea fácil de encontrar para las demás personas (nunca tu fecha de nacimiento, el nombre de tu mascota, tu pueblo…), es mejor cuanto más larga sea y si se compone de número y letras. Si alguien sabe tu contraseña se puede hacer pasar por ti.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

- No publiques en tus perfiles de las redes sociales excesiva información personal y familiar (ni datos que permitan la localización física).
- No aceptes solicitudes de contacto de forma compulsiva, sino únicamente a personas conocidas o con las que tengas una relación previa.
- Revisa periódicamente tu lista de contactos, a lo mejor sigues teniendo contactos con los que ya no tienes ninguna relación y no quieres seguir compartiendo cosas.
- ¡Precaución! en Internet no todo el mundo es quien dice ser. Si solicitan tus datos y no te dicen para qué los van a usar, o no entiendes lo que le dicen: nunca des tus datos.
- Ten especial cuidado al publicar información relativa a los lugares en que te encuentras o un tercero se encuentra. Podría poneros en peligro.
- No utilices datos de otras personas para elaborar un perfil en una red social, piensa que estarías suplantando la identidad de otra persona, y eso es un delito.
- Piensa la imagen que quieres dar de ti mismo y hasta dónde puede llegar, puede ocurrir que se difunda a muchas más personas de las que en principio tenías previsto. Recuerda que aunque subas imágenes tuyas voluntariamente, esas imágenes dejan de ser sólo tuyas y las pueden controlar muchas más personas.

Por lo tanto, nuestros datos personales conforman nuestro derecho a la intimidad y, consecuentemente, forman parte de nuestra vida privada. Nadie puede obtener nuestros datos personales sino es porque nosotros mismos los facilitamos de forma voluntaria.

En este sentido y en función de la cantidad y el tipo de datos personales que facilitemos, así expondremos en mayor o menor medida nuestra vida privada e intimidad.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

## 4. Seguridad y libertades de expresión e información en Internet versus amenazas y garantías en las redes sociales

Las redes sociales son parte de los hábitos cotidianos de navegación de gran cantidad de personas. Cualquier usuario de Internet hace uso de al menos una red social y muchos de ellos participan activamente en varias de ellas. Para muchos usuarios (especialmente los más jóvenes), las redes sociales son el principal motivo para conectarse a Internet. Sin embargo, a partir de su uso, los usuarios se ven expuestos a un conjunto de amenazas informáticas, que pueden atentar contra su información, su dinero o incluso su propia integridad.

Ante la creciente tendencia de los ataques informáticos a utilizar las redes sociales como medio para su desarrollo, se vuelve de vital importancia para el usuario, estar protegido y contar con un entorno seguro al momento de utilizarlas.

Así mimo, es importante:

- **Prestar atención cuando publiquemos y subamos material:**
  - Pensar muy bien qué imágenes, vídeos e información escogemos para publicar.
  - No publicar nunca información privada.
  - Usar un seudónimo.

- **Escoger cuidadosamente a nuestros amigos:**
  - No aceptar solicitudes de amistad de personas que no conozcamos.
  - Verificar todos nuestros contactos.

- **Proteger nuestro entorno de trabajo y no poner en peligro nuestra reputación:**



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

- Al registrarnos en una red social, usar nuestra dirección de correo personal (no el correo de la empresa).
- Tener cuidado de cómo representamos en Internet a nuestra empresa u organización.
- No mezclar nuestros contactos de trabajo con nuestros amigos/as.
- No dejar que nadie vea nuestro perfil o nuestra información personal sin permiso.
- No dejar desatendido nuestro teléfono móvil.
- No guardar nuestra contraseña en nuestro móvil.

Del mismo modo, la cantidad de información personal disponible en Internet, procedente tanto de las comunicaciones de los ciudadanos en las redes sociales como de aquellas que realizan las administraciones, está generando que la identidad digital casi importe más que la identidad personal. La presencia digital de las personas y las empresas, y el papel que tienen en el ámbito del derecho al olvido grandes empresas como Google o Facebook, se ponen de manifiesto a través de los mecanismos de indexación, que convierten a estas plataformas en grandes contenedores de información personal.

En el Reglamento europeo, el responsable de haber publicado los datos personales deberá adoptar todas las medidas razonables, incluidas medidas técnicas, para informar a los terceros que estén tratando dichos datos de que el titular de los mismos les solicita que supriman cualquier enlace a esos datos personales o cualquier copia o réplica de ellos.

Por ello la irrupción de las redes sociales y el hecho de que cualquiera pueda convertirse en emisor de información de utilidad pública y la exposición digital de la vida privada de las personas son fenómenos que obligan a reforzar la protección de datos *online*.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

## 5. Responsabilidad de los prestadores de servicios de Internet: Amenazas y garantías en Internet

Iniciamos este capítulo exponiendo que para que se pueda hablar de responsabilidad de los prestadores de servicios de Internet es necesaria la concurrencia de cuatro supuestos:

1. Un acto u omisión.
2. El daño que supone una pérdida o lesión que sufre un sujeto como consecuencia del acto, consiste en un deterioro que afecta a bienes personales o patrimoniales del sujeto.
3. El nexo causal: entre el daño y la acción debe haber un vínculo de causalidad, es decir la acción tuvo que provocar el daño.
4. La culpa: mayor o menor conciencia de inobservancia del deber de actuar con la diligencia exigible.

Así mismo, cuando la información se convierte en objeto de apropiación indebida, se ven afectados valiosos bienes jurídicos como la intimidad, el orden socioeconómico y la seguridad del estado, entre otros.

El tema de la informatización y la garantía de las libertades individuales es uno de los que debe enfrentar el derecho y, dentro de éste, por supuesto, el Derecho Penal. El principal aspecto que se discute es el del acceso y utilización de la información privada de las personas. Las normatividades se basan fundamentalmente en acuerdos internacionales sobre telecomunicaciones, comunicaciones vía satélite, protección de software, construcción de equipos y otras.

En un principio, se observaba una reacción a nivel privado frente a las primeras manifestaciones de invasión no autorizada, pero simultáneamente se producía de parte de los transgresores un perfeccionamiento en sus técnicas de intro-



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

misión. Posteriormente, ante esta realidad se consideró muy necesaria la participación del Estado y sus organismos, para consolidar la adecuada complementación de los mecanismos de seguridad privados con normativas que establecieran una clara regulación y sanción de estas conductas tipificándolas en los diversos códigos penales como delitos.

El bien jurídico que se pretende tutelar, es precisamente, la Seguridad Informática. La Seguridad Informática es la seguridad de la operación de los sistemas de información, la cual debe proporcionar integridad, disponibilidad y confidencialidad de la información.

Cuando usamos el término integridad, hacemos alusión a que la información debe ser fidedigna y completa, nadie que no sea el usuario tiene derecho a cambiarla. En este sentido, utilizamos el término disponibilidad, para referirnos a que el usuario debe tener la información en el momento en que la necesite y confidencialidad porque sin consentimiento del usuario nadie debe tener acceso ni divulgar su información.

Los delitos informáticos se clasifican según el perjuicio causado, el papel que el computador desempeñe en la realización del mismo, el modo de actuar, el tipo penal en que se encuadren y la clase de actividad que implique según los datos involucrados.

Quizás la modalidad más conocida de delitos contra la Seguridad Informática, y la más difundida, sea el sabotaje electrónico, el que se presenta en diversas modalidades que van desde la manipulación de los datos antes de su entrada a la máquina, la modificación de un programa para que realice funciones no autorizadas, el redondeo de cuentas, el uso no autorizado de programas, programa de ejecución sujeta a determinadas condiciones, hasta el acceso a líneas de transmisión de datos y el uso de la computadora en la planificación, ejecución o control de la comisión de algún otro delito.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Dentro de este tipo de conductas comúnmente podemos encontrar:

1. Phreaking o acceso no autorizado. Es el usual "pinchazo" de redes o teléfonos, donde el individuo se aprovecha ilícitamente del servicio, evitando realizar pago alguno.
2. Hacking: Esta conducta se refiere al acceso no autorizado que realiza el sujeto activo a un sistema de información atentando contra el sistema de seguridad que este tenga establecido. Usualmente un hacker realiza estas acciones para satisfacer su curiosidad y aumentar su autoestima.
3. Cracking: Un cracker, a diferencia de un hacker, usualmente ingresa en redes ajenas con fines ilícitos o para dañar a los mismos.
4. Atentados contra la propiedad intelectual y de marcas.

Del mismo modo, en la responsabilidad por servicios de alojamiento tenemos el riesgo creado y el deber de garantía o de seguridad. El servicio ofrecido por el proveedor de la red se basa en la confianza que sus clientes tienen de la seguridad de sus redes hace que éste tipo de servicio contenga obligaciones tanto de resultado como de seguridad.

Los operadores de redes, por ello, no están normalmente expuestos a responsabilidades penales o civiles por el contenido transmitido por sus redes, aunque pueden ser requeridos a dar los pasos adecuados respecto a sus clientes (los proveedores de acceso) si estos últimos usan algunos recursos para transmitir contenidos ilegales o para realizar actos ilícitos.

El principio general de la normativa que regula los requisitos de seguridad que debe cumplir un servicio informático se basa en trasladar a los proveedores la responsabilidad



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

sobre el control de la calidad y seguridad de los servicios que brindan.

En el caso de responsabilidad no imputable al administrador de redes, el responsable será la empresa, o el propietario de la red. Serán responsables de los daños que se causen por la indebida destrucción, apoderamiento, modificación, o utilización de archivos que pertenezcan a los usuarios de modo personal. Sólo serán excluidos de la responsabilidad los Administradores de redes de cómputo, y las empresas o dueñas de la red, si se demuestra que era imposible la prevención del ilícito cometido, a pesar de la debida preparación de los Administradores de la red, así como de que se contaba con los programas actualizados para detección de virus, etc.

Por otro lado, señalamos que los contenidos nocivos son aquellos que significan una ofensa a los valores o sentimientos de algunas personas y están íntimamente relacionados con el concepto de honor, pudor, intimidad y moralidad. Los contenidos ilícitos prohibidos contemplan también apología a algún delito. Así, contempla también a:

a. La difusión de instrucciones sobre preparación de bombas, las actividades terroristas, la producción y tráfico de drogas, y el activismo político, lo que atenta contra la seguridad nacional y mundial.
b. La oferta de servicios sexuales y pornografía relacionada con niños (pedofilia).
c. El envío de mensajes que incitan al odio y la discriminación racial o religiosa.
d. Las conductas de hurto y destrucción de datos que atentan contra la seguridad y confidencialidad de la información.
e. Los delitos de "piratería" de software, que vulneran la propiedad intelectual.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

f. Los delitos contra la propiedad industrial: apropiación de logotipos, marcas, diseños originales, etc.
g. El mal uso de tarjetas de crédito ajenas.
h. La recolección, procesamiento y transmisión no autorizada de datos personales.
i. El envío de mensajes difamatorios o injuriantes.

Exponemos que existen diversas teorías respecto a la responsabilidad de los proveedores de servicios frente a los contenidos transmitidos por sus usuarios a través de la red. Una que sostiene que como medio de comunicación social Internet debe de ser regulada y se debe impedir en ella la transmisión de contenidos nocivos o ilícitos.

Y, la otra teoría es la de la autorregulación la cual exime de toda culpa a los proveedores de servicios en cuyas redes o servidores fluya dicho tipo de contenidos, siempre y cuando el proveedor haya advertido a su usuario del carácter de dichos mensajes o publicaciones.

## 6. Ciber derechos. Los e-derechos de la infancia en el nuevo contexto TIC

La brecha digital exacerba desigualdades en el acceso a información y conocimiento, socialización con pares, visibilidad y manejo de herramientas básicas para desempeñarse en la sociedad. Reducir esta brecha permite sinergias virtuosas de inclusión social y cultural entre niños, niñas y adolescentes, con impactos positivos en el desarrollo de capacidades y generación de oportunidades para toda su vida. Si bien las nuevas generaciones están conectadas y sus miembros son nativos digitales, es obvio que persisten desigualdades entre grupos socioeconómicos.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Especialistas en la materia[6] coinciden en los efectos positivos de Internet en distintos ámbitos de la vida de niños y niñas, ya que incide en el desarrollo de sus capacidades digitales y en las oportunidades de su vida adulta. En el abanico de posibilidades que ofrecen las TIC hay ventajas y riesgos que van de la mano. El desafío está en la provisión de capacidades digitales y estrategias de seguridad en línea y de autocuidado.

Las TIC, puestas al servicio de los derechos fundamentales de la infancia, son una herramienta que fortalece el ejercicio del derecho a dar su opinión y fomentar la participación ciudadana, así como su libertad de expresión e información. Con los avances tecnológicos de la web 2.0, los usuarios dejan de ser receptores pasivos, teniendo la posibilidad de crear y difundir sus propios contenidos.[7] Se trata de un uso que posibilita que los niños, niñas y adolescentes accedan a mensajes de los medios masivos y de otros individuos, lo que les permite compartir opiniones e información y promocionar diálogos, donde se cultivan relaciones interpersonales en una gran variedad de formatos, incluyendo textos, fotografías, audio y vídeo. La horizontalidad de estas prácticas democratiza la producción e intercambio de opiniones, ideas y contenidos, y aumenta la participación y diversidad en la red. Este ejercicio aporta a los niños y niñas sociabilidad, comunicación, creatividad e interactividad.

6 Véase UNICEF (2015). "Convención sobre los derechos del niño". URL http://www.unicef.es/infancia/derechos-del-nino/convencion-derechos-nino.

7 Web 2.0 es un concepto que hace referencia a la masificación de una serie de herramientas que alimentan la interactividad de las plataformas digitales y que permite a los usuarios crear contenidos y hacerlos públicos en la web (OCDE, 2007).



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

El derecho a la intimidad personal y familiar, al honor y a la propia imagen, es inherente a toda persona, inalienable y concreta el valor de la dignidad humana en un Estado social y democrático de derecho. De hecho, el derecho a la intimidad está perfectamente regulado en distintos tipos de legislaciones, tanto a nivel internacional como nacional, teniendo, en todos los casos, tratamiento de derecho fundamental de las personas.

Al igual que ocurre con el resto de derechos fundamentales, el derecho a la intimidad se convierte en un deber para con los demás. En consecuencia, al mismo tiempo que podemos exigir el respeto a nuestra intimidad, debemos respetar el derecho a la intimidad de terceros. Esta premisa es trasladable al entorno de las nuevas tecnologías: los usuarios deben respetar la privacidad de los demás.

En muchos casos, la vulneración del derecho a la intimidad o privacidad de cualquier persona podría ser constitutivo de distintos tipos de delitos. Así pues, pasamos a detallar algunas de las conductas delictivas más frecuentes:

1. **Descubrimiento y revelación de secretos:** Aquel que con el fin de descubrir o vulnerar la intimidad de otro, sin su consentimiento, se apodere de su correo electrónico o cualesquiera otros documentos o efectos personales, o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación.
2. **Injurias:** Acción o expresión que lesiona la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación. Ej.: Difusión de vídeos o imágenes íntimas, insultos, difundir montajes fotográficos de una persona, etc.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

3. **Falsedad en documento privado:** suscribir a un tercero, a infinidad o multitud de listas de correo, haciéndonos pasar por él, y remitiendo infinidad de correos de suscripción suplantando la identidad de otro.
4. **Estafa:** Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. Ej.: Manipulación de datos o programas para la obtención de un enriquecimiento ilícito.

Del mismo modo, exponemos que El 6 de febrero de 2004 UNICEF celebró el Día Internacional para una Internet Segura. En esta oportunidad la oficina nacional de España presentó un decálogo con los derechos y deberes relacionados con las TIC, donde se expresa la importancia de incentivar el uso y acceso para fines informativos y recreativos, pero con responsabilidad, y siendo éstos los siguientes:

1. Derecho al acceso a la información sin discriminación por sexo, edad, recursos económicos, nacionalidad, etnia o lugar de residencia. Este derecho se aplicará en especial a los niños y niñas discapacitados/as.
2. Derecho a la libre expresión y asociación. A buscar, recibir y difundir informaciones e ideas de todo tipo por medio de la red. Estos derechos solo se restringirán para garantizar la protección de los niños y niñas frente a informaciones perjudiciales para su bienestar, desarrollo e integridad; y para garantizar el cumplimiento de las leyes, la seguridad, los derechos y la reputación de otras personas.
3. Derecho de los niños y niñas a ser consultados y a dar su opinión cuando se apliquen leyes o normas a Internet que les afecten.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

4. Derecho a la protección contra la explotación, el comercio ilegal, los abusos y la violencia de todo tipo.
5. Derecho al desarrollo personal y a la educación, y a todas las oportunidades que las nuevas tecnologías puedan aportar para mejorar su formación.
6. Derecho a la intimidad de las comunicaciones por medios electrónicos. Derecho a no proporcionar datos personales por Internet, a preservar su identidad y su imagen de posibles usos ilícitos.
7. Derecho al esparcimiento, al ocio, a la diversión y al juego, mediante Internet y otras tecnologías. Derecho a que los juegos y las propuestas de ocio no contengan violencia gratuita, ni mensajes racistas, sexistas o denigrantes y que respeten los derechos y la imagen de los niños y niñas y otras personas.
8. Los padres y madres tendrán el derecho y la responsabilidad de orientar y acordar con sus hijos e hijas un uso responsable.
1. Los gobiernos de los países desarrollados deben comprometerse a cooperar con otros países para facilitar el acceso de estos y sus ciudadanos, y en especial de los niños y niñas, a Internet y otras tecnologías para promover su desarrollo y evitar la creación de una nueva barrera entre los países ricos y los países pobres.
10. Derecho a beneficiarse y a utilizar en su favor las nuevas tecnologías para avanzar hacia un mundo más saludable, pacífico, solidario, justo y respetuoso con el medioambiente, en el que se respeten los derechos de todos los niños y niñas.[8]

8 Para más información véase: Internetsegura.net. Decálogo de los derechos de la infancia en Internet, (2004): http://www.redescepalcala.org/inspector/DOCUMENTOS%20Y%20LIBROS/TIC/Internet%20Segura.pdf.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

## 7. Responsabilidades penales de los menores

La facilidad de conexión, la inmediatez y la generalización de redes sociales para estar en contacto están suponiendo nuevos modelos de expresión en los menores así como una particular manera de comunicarse. Sin embargo, que los menores hagan un uso frecuente de Internet y en general de las nuevas tecnologías, no significa que sepan hacerlo de forma segura. Ni tampoco que lo hagan de forma responsable o conociendo las consecuencias que para ellos puede tener una utilización que resulte dañina para terceros. Este uso inadecuado puede hacer que queden expuestos a muchos riesgos, de entre los cuales, destacaríamos los siguientes:

1. Los derivados de la falta de privacidad en Internet.
2. Los posibles conflictos de relación que surgen entre los/as menores y que trascienden a la Red.

A través de Internet y concretamente de las Redes Sociales, los/as menores comparten todo tipo de información: facilitan datos personales, cuelgan sus fotografías y las de amigos/as y familiares, hablan de sus gustos y preferencias, de lo que están haciendo, de los planes que tienen e incluso de sus sentimientos y preocupaciones. Lo que antes se quedaba en su grupo de amigos, ahora puede ser visto por millones de personas. Esta situación, lógicamente, puede generar situaciones de riesgo.

Por otra parte, hay que ser conscientes de que en la actualidad muchos de los conflictos que se producen en las aulas trascienden a Internet y viceversa, y éstos pueden degenerar en un acoso sistemático a través de las nuevas tecnologías, lo que se ve favorecido por el supuesto anonimato del que los jóvenes creen disfrutar en la Red.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Del mismo modo es importante destacar que las nuevas tecnologías no suponen un problema en sí mismas, y para los menores se han convertido, además, en algo irrenunciable. Las consideran básicas y su utilización está perfectamente integrada en su vida cotidiana. Se hace necesario pues prevenir las situaciones de riesgo, para lo cual disponemos de dos poderosas herramientas: la información y la educación.

Si la población menor conoce los riesgos y las consecuencias de hacer un mal uso de las TIC, y saben también cómo actuar y a quién dirigirse en caso de necesidad, la navegación por Internet será para la mayoría de ellos/as tan satisfactoria como cualquier otra actividad saludable.

Si bien existen pautas y consejos específicos para el uso correcto de las TIC, que reproducimos a continuación, tanto los padres/madres y educadores, como la sociedad en su conjunto, debemos partir de que no existe una vida real y otra virtual, transcurriendo en paralelo. Ambas están totalmente interrelacionadas y lo que sucede en la una repercute en la otra. En consecuencia, las mismas recomendaciones y pautas que transmitimos a los menores para su vida cotidiana, son totalmente extrapolables a la Red desde las normas básicas de educación.

Por lo tanto, conviene que hagamos una referencia breve y simplificada a lo que son las principales conductas delictivas (y por lo tanto proseguibles desde las Fiscalías de Menores). Por sistematizar de manera muy simple los podemos dividir en dos categorías:

1. Delitos contra las personas ya sean lesiones, malos tratos, etc. y que se fotografían o graban y donde se utiliza la nueva tecnología para su difusión a través de Internet o por SMS. La potencialidad lesiva está en la difusión.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

2. Delitos cometidos propiamente a partir de nuevos medios tecnológicos:
   - Contra el honor y libertad y seguridad (injurias, amenazas, coacciones...). Puede ser al ordenador de la víctima por e-*mail*, o usando messenger, a través de chats, por medio de SMS. En su modalidad más grave y continuada integrará el llamado "ciberbullying". Esto último consiste en "el uso de medios telemáticos (Internet, telefonía móvil, videojuegos *online*) para ejercer el acoso psicológico entre iguales".
   - Tenencia, descargas y distribución de pornografía infantil (en la Memoria de la Fiscalía General del Estado de 2008 se refieren numerosas denuncias de difusión de desnudos grabados por cámara web.
   - Delitos patrimoniales y/o estafas en la Red: tarjetas, obtención de crédito fraudulento en tarjetas prepago de móviles. Esas son, en esencia, algunas de las principales conductas detectadas y, como decía, la sensación de impunidad, de que "no pasa nada", es ilusoria.

En primer lugar, todo este tipo de tecnologías dejan siempre un "rastro" de su procedencia y por hablar sólo de Internet, cada vez que se realiza un acceso a través de nuestro ordenador (a una página web, a una red de intercambio, a una red social, chat, etc), dejamos una huella a través del IP (Internet Protocol), número de identificación diferenciado y asignado a cada ordenador, y que es fácilmente detectado por las Fuerzas y Cuerpos de Seguridad del Estado que cuentan tanto la Policía nacional y Guardia Civil como las diversas Policías Autonómicas, con equipos de agentes altamente especializados y cualificados para el descubrimiento y persecución de esta clase de conductas delictivas.



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

Y respecto a la segunda cuestión, por el hecho de ser menor **¿no va a pasar nada?** Como decíamos antes, nada más lejos de la realidad. Es cierto que, a consecuencia de un enfoque equivocado del tema por parte de los medios de comunicación se ha generalizado el tópico de que los delitos cometidos por menores quedan impunes, pero tal creencia es por completo falsa.

El menor de catorce a dieciocho años **tiene una responsabilidad** por los hechos delictivos que comete, distinta, cierto, a la de un adulto, pero debe responder desde el punto de vista de la sanción como desde el punto de vista patrimonial o de indemnización.

La regulación legal está recogida básicamente en la Ley Orgánica de Responsabilidad Penal del Menor (LO 5/00 de 12 de enero) que atribuye la labor de instrucción e investigación de los delitos y faltas cometidos por menores a las Fiscalías de Menores y el enjuiciamiento de las conductas ilícitas a los Jueces de Menores. En dicha Ley se establecen las **medidas tanto judiciales como extrajudiciales** que se le pueden imponer a un menor responsable de un delito o falta, que ciertamente, no será la prisión o una multa, por citar penas que sólo son imponibles para las personas adultas, pero sí se le podrá imponer al menor medidas como la prestación de servicios en beneficio de la comunidad, la libertad vigilada, el alejamiento de la víctima o privarle incluso de libertad con permanencias de fin de semana en un centro o internamientos en centros en régimen semiabierto o cerrado, según los casos.

Pero; ¿qué pasa con las conductas delictivas que antes mencionábamos cometidas por menores a través de medios tecnológicos? Pues nos merecen especial cuidado, porque hablando, por ejemplo, del primer grupo mencionado, de las agresiones a personas que se graban para luego difundirlas, lo que merece más reproche a veces que la propia conducta



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

(y con independencia de la sanción que ésta merezca) es **el hecho de grabarla y difundirla**, que hace que se extienda mucho más el agravio sufrido por la víctima. Por eso, la acusación y la sanción es muchas veces la misma -si no más grave- para quien maltrata o insulta que para quien estuviere grabando o "cuelga" y distribuye el vídeo o imagen, pudiendo ser muchas veces perseguido como un delito contra la integridad moral del artículo 173 del Código Penal. Este artículo que habla del que "inflingiere a otra persona un trato degradante menoscabando gravemente su integridad moral..." lo venimos aplicando para sancionar frecuentemente las conductas conocidas como de acoso escolar, respecto a cuya persecución tenemos órdenes estrictas en las Fiscalías emanadas de la Fiscalía General del Estado (Instrucción 10/05), pudiendo aplicarse tanto ese artículo como esas directrices a los supuestos en que ese acoso se materializa a través de medios telemáticos (*ciberbullying*).

¿Cuáles son, entonces, las medidas a aplicar a menores ante tales conductas? Existe una cierta flexibilidad a la hora de decantarse por la medida adecuada, que dependerá en buena parte de la mayor o menor gravedad de la conducta y de la actitud que muestre el menor.

Ante este tipo de hechos no pocas veces podemos intentar encauzarlos a través de una **solución extrajudicial** del artículo 19 de la Ley de Responsabilidad Penal del Menor, evitando así a la víctima y a los propios menores infractores tener que acudir a juicio. Es necesario primero que se trate de faltas o delitos menos graves, siempre que la violencia o intimidación ejercidas sobre la víctima no fuesen graves. En tales casos se puede obviar el juicio, siempre que el infractor asuma su responsabilidad, a través de una conciliación, pidiendo disculpas el menor al ofendido (aparte de retirar, por ejemplo, el contenido injurioso o vídeo ultrajante de la red...) y/o una reparación extrajudicial, en la que, además de las



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

consiguientes disculpas, el menor infractor realice una tarea en beneficio de la víctima o de otras personas o colectivos: así realizando tareas en beneficio de personas desasistidas o en situación de precariedad (residencias de ancianos) o tareas medio ambientales, asumiendo así las consecuencias de su acción.

Pero puede que lo anterior no sea posible ya fuere por la propia gravedad de la conducta o porque el menor no admitiera su responsabilidad o porque hubiera ya cometido otros delitos o faltas de esa misma o de diferente clase. Entonces se acudiría a una *audiencia* o **juicio** en el que, luego de celebrado y en sentencia se podrán imponer al menor alguna o varias de las medidas previstas en la Ley en el artículo 7. Esas medidas, aunque son muy diversas, podrían consistir usualmente en el alejamiento o prohibición de comunicarse con la víctima; en prestación de servicios en beneficio de la comunidad (hasta 100 horas que podrían ampliarse hasta 200); libertad vigilada, consistente en un seguimiento del menor, imponiéndole además reglas determinadas de conducta (hasta dos años, aunque pueden ampliarse por más tiempo); pero también, y en función de la tipología y gravedad del caso puede privarse de libertad al menor con permanencias de fin de semana en centro o domicilio (hasta ocho fines de semana, ampliables a dieciséis) o internamientos en centro cerrado o semiabierto hasta dos años, ampliable en función de la gravedad del caso. Algunas de estas medidas como los alejamientos, libertad vigilada o internamientos pueden adoptarse por el Juez de menores a petición de Fiscalía, en casos graves y si la gravedad de la situación lo requiriese, cautelarmente y sin esperar a juicio (art. 28 de la Ley). Por último, decir que todo lo anterior es en cuanto a la faceta sancionadora. Pero la patrimonial no es menos importante, pues el menor infractor —salvo que la víctima renuncie— está obligado a indemnizar al ofendido de los daños de todo tipo, incluidos los morales, que le haya causado y de



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

la indemnización responderán con el menor solidariamente, o sea juntamente con él, sus *padres, tutores, acogedores y guardadores legales o de hecho* (art. 61-3 de la Ley)

## 8. Conclusión

Las TIC son herramientas que posibilitan el desarrollo de capacidades cognitivas ámbitos sociales, políticos y económicos. Los dispositivos tecnológicos son parte de la cotidianidad de niños y niñas y han modificado las relaciones entre pares, lo que puede resultar positivo o nocivo según se utilice.

Es necesario reflexionar acerca del papel de la escuela en la entrega de pautas y protocolos para un uso seguro de Internet que permita aprovechar sus beneficios y minimizar sus riesgos. Si bien faltan datos respecto de cómo actúan los padres y madres frente al uso de Internet en los hogares, es posible estimar que los conocimientos mediáticos y tecnológicos de niños y niñas superan a los de sus progenitores, por lo que estos no están a la par para orientarlos.

La escuela debe convertirse en un agente en la entrega de herramientas para avanzar en este ámbito. Las políticas de informática educativa han contribuido a equilibrar las brechas digitales, posibilitando el acceso a las y los estudiantes de sectores sociales más postergados. Una meta importante es alfabetizar digitalmente a los docentes para que aprovechen la tecnología en los procesos de enseñanza.

Del mismo modo señalamos que la creciente exposición tecnológica de las nuevas generaciones impone grandes desafíos al sistema educativo. Hay que formar habilidades para navegar sin riesgos aprovechando lo que la tecnología ofrece para el desarrollo y el ejercicio de los derechos de la infancia. Estas habilidades superan lo que se ha denominado la alfabetización digital, pues son habilidades cognitivas y éticas que



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

permitirán a las nuevas generaciones construir e insertarse de modo pleno en la sociedad que les toca vivir.

En este sentido, a través de las nuevas tecnologías nos hemos acostumbrado a comunicarnos, a divertirnos, a jugar, a encontrar nuevas vías de conocimiento de realidades o personas, a relacionarnos, etc. Pero igual que ha ocurrido con otros muchos inventos, lo que puede servir para tantas cosas positivas, puede servir para lo contrario, para desarrollar conductas negativas e incluso delictivas dirigidas hacia otras personas.

Así mismo, se ha llegado a hablar de "delincuencia informática" o "delitos cometidos a través de nuevas tecnologías", para catalogar fenómenos delictivos relativamente novedosos y en cualquier caso de reciente aparición.

Por lo tanto, la rápida emergencia de un mercado liberalizado de comunicación global, y el uso popular de Internet han traído como consecuencia el cuestionamiento de medios tradicionales de distintas normas de regulación. En esta nueva sociedad, el sector de las telecomunicaciones es crucial y lo convierte en balaustre del proceso de informatización. La seguridad que se le exige a la red es mucho mayor que la que han ofrecido hasta ahora los medios tradicionales.

La necesidad de conocer y saber utilizar Internet es una condición primordial en la sociedad actual, por lo que la protección, en todos sus términos, no debe privar a los menores de esta herramienta. La prohibición y el control no representan el camino hacia una navegación segura y responsable de los menores. Es importante enseñarles a utilizar esta herramienta con criterio, haciendo un buen uso de los muchos beneficios que aporta, pero también es necesario darles a conocer la manera de afrontar determinadas situaciones.

Concluimos exponiendo que es importante destacar que las nuevas tecnologías no suponen un problema en sí mismas, y para los menores se han convertido, además, en algo



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

irrenunciable. Las consideran básicas y su utilización está perfectamente integrada en su vida cotidiana. Se hace necesario pues prevenir las situaciones de riesgo, para lo cual disponemos de dos poderosas herramientas: la información y la educación.

Y, la protección legal representa el paso inicial fundamental para asegurar unos hábitos adecuados de uso de Internet. En este sentido, la mayor parte de los problemas que podemos encontrarnos en Internet se producen básicamente como consecuencia de no respetar toda una serie de normas básicas de seguridad.

## 9. Bibliografía.

Bru cuadrada, E. (2009) "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas". Url: http://www.redescepalcala.org/inspector/DOCUMENTOS%20Y%20LIBROS/TIC/Inter net%20Segura.pdf [25/05/15]

Cotino Hueso, l (2011). *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, Valencia: Publicaciones de la Universitat de València.

E-LEGALES (2014). Url: http://www.e-legales.net/responsabilidad-penal-de-los-menores.shtml [29/04/15]

Fundación Orange España (2008). "Informe anual sobre el desarrollo de la sociedad de la información en España", Madrid, octubre 2008.

García Ingelmo, f.m. (2008). "Guía para Internet". Url: http://www.elegales.net/responsabilidad-penal-de-los-menores.shtml [10/06/15]

IQUA.es (2013). URL http://www.iqua.es/ [21/06/15]

Internet segura (2015). Url: http://www.educa.jcyl.es/ciberacoso/es/plan-prevencion-ciberacoso-navegacion-segu-



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528

ra/proteccion-legal-menores-frente-ciberacoso/normativa-existente-utilizacion-prevencion-acoso-escolar-me [20/06/15

Lara, JC., vera, f (2010). «Responsabilidad de los prestadores de servicio de Internet», *Policy Papers* 3 pp. 18-23

Lasén, A. (2010). "Mediaciones tecnológicas y transformaciones de la intimidad entre jóvenes". Congreso Internacional Jóvenes Construyendo Mundos, Madrid, junio 2010.

Manual prevención de delitos (2011). Url: http://www.unodc.org/documents/justiceandprisonreform/crimeprevention/Handbook__the_Crime_Prevention_Guidelines_Spanish.pdf [19/05/15]

Plan de prevención del ciberacoso y la navegación segura (2014). Url: http://www.educa.jcyl.es/ciberacoso/ es/plan-prevencion-ciberacoso-navegacion-segura [29/04/15]

Pérez L, Enrique, A. (1998) "Internet y el Derecho". *Revista Iberoamericana de Derecho Informático.* I, pp 721-734.

UNICEF (2015). "Convención sobre los derechos del niño". Url. http://www.unicef.es/infancia/derechos-del-nino/convencion-derechos-nino [27/05/15]



Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención.
María Ángeles Verdejo Espinosa (Coordinadora).
Sevilla: Universidad Internacional de Andalucía, 2015. ISBN: 978-84-7993-281-7. Enlace: http://hdl.handle.net/10334/3528