CONECTADOS RESPONSABLES

Uso de dispositivos electrónicos por parte de menores

NO CLAMES, RECLAMA!

MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

CECU

Conectados responsables: Uso de dispositivos electrónicos por parte de menores[1]

[1] **"Conectados responsables: Uso de Dispositivos Electrónicos por parte de menores"** se desarrolla dentro del marco del proyecto "No clames, reclama", que CECU viene desarrollando desde 2010, y que tiene por objetivo informar a las personas consumidoras sobre sus derechos y cómo reclamarlos.

Para ello cuenta con una página web (www.noclamesreclama.org) y una aplicación para móviles -RECLAMA, que puede descargarse de forma gratuita desde las tiendas de Google y Apple-, donde puede encontrarse toda la información relacionada, para los distintos sectores económicos (transportes, energía, seguros, vivienda, telecomunicaciones, comercio electrónico, viajes etc.).

ÍNDICE

Introducción	**2**
1. Primera parte: riesgos	**3**
a. Riesgos para la salud y el neurodesarrollo	3
b. Riesgos para la privacidad y protección de datos personales de las personas menores de edad	7
c. Riesgos técnicos y de seguridad	11
2. Segunda parte: derechos y formas de reclamación	**13**
Escenario nº1. ¿Cómo protegemos a nuestros niños/as del diseño adictivo de los servicios digitales?	13
Escenario nº2. ¿Qué podemos hacer frente al contenido inapropiado o ilícito que es recomendado a los niños/as por Internet?	14
Escenario nº3. ¿Qué hacer ante un caso de robo o suplantación de identidad de un menor, ciberacoso o grooming?	15
Escenario nº4. ¿Qué hacer si exponen información personal de un menor sin consentimiento, por ejemplo, si generan o comparten un *deepfake* o explotan sus datos personales o si un menor "vende" su iris?	17
Escenario nº5. ¿Qué protege a nuestros menores del abuso de anuncios personalizados con su información?	18
Escenario nº6. ¿Qué hacer si un ataque de *malware* o *phising* ha afectado la información de un menor?	19

INTRODUCCIÓN

La **seguridad de las niñas, niños, adolescentes y jóvenes** en relación con la utilización de **dispositivos electrónicos** y, en particular, en las **redes sociales**, es un problema apremiante. Ya en 2021 las revelaciones de los archivos de Facebook expusieron que Meta tenía conocimiento de que su algoritmo de clasificación de contenido en Instagram exacerbaba los problemas de **salud mental** entre las adolescentes, con un impacto negativo significativo en la imagen corporal[2].

Desde la Federación de Consumidores y Usuarios CECU consideramos clave sensibilizar en esta materia en España, tal y como se desprende de las prioridades del Ministerio de Derechos Sociales, Consumo y Agenda 2030 y de la agenda España Digital 2026. A través de esta guía, queremos informar a madres y padres, educadores y organizaciones interesadas de los peligros que los dispositivos electrónicos pueden presentar para los menores y sobre **cómo mitigar estos riesgos** para asegurar un **entorno digital seguro y enriquecedor**. Se trata de un instrumento de ayuda para que puedan conocer los principales **riesgos, recomendaciones y derechos** que existen frente a diferentes problemáticas que surgen en el entorno digital. En este sentido, recomendamos jugar un papel activo en la experiencia en Internet de los menores a su cargo y mantener siempre un **diálogo abierto** sobre su seguridad y privacidad.

[2] https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

1. PRIMERA PARTE RIESGOS

La era digital conlleva algunos riesgos para determinados grupos, como es el caso de los niños, niñas, adolescentes y jóvenes, que pueden encontrarse en situaciones de **vulnerabilidad digital.** En esta guía abordaremos algunos de estos riesgos, poniendo el foco en la salud y el neurodesarrollo, la privacidad y los riesgos técnicos y de seguridad.

A. Riesgos para la salud y el neurodesarrollo

El **uso excesivo de dispositivos electrónicos** puede **afectar negativamente el desarrollo físico y cognitivo** de los menores. Estudios indican que la exposición prolongada a pantallas puede conducir a **problemas de visión, trastornos del sueño y reducción en la capacidad de atención**. Hay quienes sostienen que, incluso, el uso problemático de pantallas o dispositivos electrónicos podría compararse con conductas adictivas[3]. En esta sección analizaremos algunos de los riesgos a los que están expuestos al utilizar dispositivos electrónicos en relación con su salud y el neurodesarrollo.

El diseño adictivo es la incorporación de características diseñadas para ser adictivas en detrimento de la salud y el bienestar de las personas, especialmente de los menores[4]

Las redes sociales están diseñadas para fomentar un uso frecuente y/o prolongado. Cada notificación, ya sea un mensaje de texto, un "me gusta" en Instagram o una notificación de Facebook, tiene el potencial de ofrecer un estímulo social positivo y una oleada de dopamina, lo que puede **alentar tendencias adictivas**. El comportamiento compulsivo en las redes sociales se refuerza mediante facilidades tecnológicas que permiten a los usuarios disfrutar de una experiencia de navegación sin fricciones -como *feeds* de noticias interminables, recarga automática y funciones de reproducción automática-. Estos patrones de uso adictivo plantean riesgos significativos, especialmente para los menores que atraviesan fases importantes de desarrollo.

[3] Ver. "Adicción a pantallas".

En efecto, algunas características de las conductas adictivas pueden ser:

Intoxicación: Refiere a los cambios cognoscitivos, psicológicos y conductuales, específicos y reversibles producidos por el efecto fisiológico del uso o consumo sobre los órganos blancos.

Uso problemático y/o abuso: No refiere sólo al uso excesivo sino también inadecuado, cuando la situación o contexto puede en sí mismas traer consecuencias adversas significativas, como el incumplimiento de obligaciones, las inasistencias a la escuela, el uso en lugares o circunstancias donde esto pueda resultar especialmente peligroso, los descuidos, los problemas interpersonales o, incluso, legales.

Craving: Es el deseo o impulso intenso e imperioso que tiende al consumo.

Dependencia: Ocurre cuando la vida de una persona comienza a girar de manera casi exclusiva en torno al consumo: todos los días o casi todos, sin que la voluntad sea suficiente para frenar la conducta, incluso cuando esto acarrea problemas de salud, interferencias severas o consecuencias negativas en alguna dimensión de su vida, obstaculizando el desarrollo normal de la vida cotidiana.

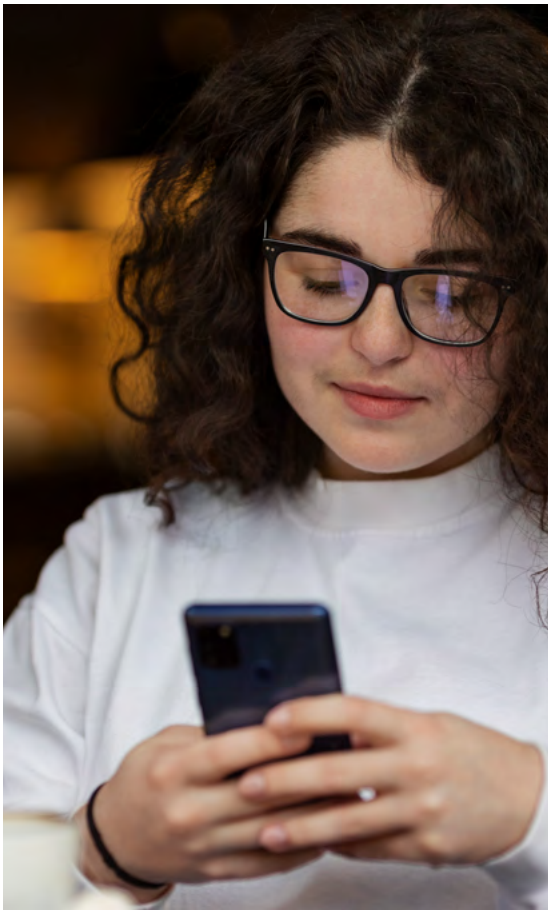
Abstinencia: Son las manifestaciones que aparecen -cargadas de malestar- ante la interrupción o la disminución abrupta del uso o consumo.

[4] https://panoptykon.org/sites/default/files/2023-08/Panoptykon_ICCL_PvsBT_Fixing-recommender-systems_Aug%202023.pdf

El uso excesivo y problemático de las redes sociales está también vinculado a **problemas de sueño y atención**. Por ejemplo, un estudio realizado a cientos de adolescentes holandeses mostró que este problema estaba significativamente ligado a la aparición de efectos cognitivos serios, como la atención reducida, el aumento de la impulsividad y una mayor hiperactividad. Asimismo, otro estudio lo vinculó con la mala calidad del sueño, la reducción de la duración del sueño, las dificultades para dormir, lo que puede repercutir en síntomas depresivos y ansiosos, neuroticismo y pensamientos y comportamientos suicidas.

Exposición a contenido inapropiado o ilícito

El **contenido inapropiado** es toda **imagen, vídeo o texto violento u ofensivo que circule en redes sociales e Internet sin ser adecuado para la edad y el desarrollo psicológico y emocional** tanto de niños/as como de adolescentes. Estos contenidos no tienen por qué ser ilegales, es decir, implicar un delito, como es el caso de la pornografía infantil, la apología del terrorismo, incentivar el consumo de drogas, promover el racismo o distribuir material que vulnera la dignidad humana. Los **contenidos inapropiados** pueden ser legales, pero podrían ser **nocivos** para los niños/as y adolescentes. Sería el caso de páginas o videojuegos con contenido violento y retos virales que desafían a realizar pruebas extremas, arriesgadas o dolorosas.



Al exponerse a estos contenidos, los niños/as y adolescentes podrían:

(i) formarse **percepciones erróneas** sobre relaciones afectivas, adoptando comportamientos denigrantes, sexistas o estereotipos negativos;

(ii) ser **más vulnerables** ante riesgos *online,* como *sexting* y *grooming*, y

(iii) exponerse a problemas como desórdenes alimenticios, autolesiones, consumo de drogas o adicción a juegos online[5].

[5] En concreto, tal y como se desprende de la iniciativa Internet Segura para Niños (is4k.es) del Instituto Nacional de Ciberseguridad (INCIBE), entre los daños potenciales que conlleva la exposición de menores a contenido inapropiado e ilícito se destacan los siguientes:

- Daños psicológicos y emocionales. Por ejemplo, contenido pornográfico o violento.
- Desinformación, manipulación y construcción de falsas creencias. Son especialmente peligrosos cuando tratan temáticas relacionadas con la salud y la seguridad.
- Establecimiento de conductas peligrosas o socialmente inapropiadas. Por ejemplo, sexismo, machismo, homofobia, racismo, etc.
- Daños para la salud física. Por ejemplo, la promoción de desórdenes alimenticios (anorexia y bulimia), conductas de autolesión o consumo de drogas.
- Inclusión en grupos y colectivos dañinos. Por ejemplo, colectivos extremistas, violentos o racistas, así como sectas de carácter ideológico o religioso, grupos políticos radicales, etc.
- Adicciones. Por ejemplo, contenidos inapropiados sobre drogas, sexo y juegos de azar puede favorecer trastornos de adicción.
- Gastos económicos. Por ejemplo, fraudes o intentos de engaño destinados a estafar a los usuarios para hacerse con su dinero o sus datos.

Retos virales

Son una invitación para realizar **acciones extremas, arriesgadas o dolorosas** que, a menudo, carecen de sentido. Suelen ser promovidos por *influencers*, celebridades o *youtubers,* que se graban a sí mismos y cuentan con millones de seguidores. Los participantes comparten en redes sociales fotos o vídeos mostrando que han completado el desafío.

Para muchas personas, participar en estos desafíos es una forma de sentirse parte de un grupo, ganar popularidad y unirse a tendencias virales en las redes sociales**.** Sin embargo, **también pueden tener consecuencias negativas, como el robo de datos personales, sextorsión, suicidio, daños físicos y psicológicos, *grooming* y muerte accidental[6].**

Recomendaciones

- ✔ **Educa sobre riesgos**: Informa a los menores sobre los peligros para su privacidad y seguridad al usar dispositivos móviles e Internet.
- ✔ **Reflexiona sobre los propios hábitos** con los dispositivos electrónicos. Educa con el ejemplo.
- ✔ **Fomenta el diálogo y la confianza**, conversando con los menores habitualmente para guiarles hacia contenidos positivos y constructivos. Esto es fundamental para que:
  - Establezcan acuerdos sobre cómo y cuándo usar los dispositivos.
  - Desarrollen criterios para seleccionar contenido apropiado para su edad.
  - Aprendan a usar las redes sociales e internet de manera responsable.
  - Configuren y gestionen su privacidad y seguridad online.
- ✔ **Presta atención a la terminología** que los menores usan en línea para entender sus intereses y las comunidades donde interactúan.
- ✔ **Presta atención a cambios** radicales en la vestimenta, hábitos de sueño, alimentación, estado de ánimo y comunicación de los menores: puede ser indicativo de problemas.
- ✔ Asegúrate de que cumplen con la **edad mínima recomendada** para crear perfiles en redes sociales.

Más allá de ello, **en España la legislación establece que los menores de 14 años no pueden acceder a las redes sociales**, excepto si lo hacen con consentimiento de los padres o tutores legales.

[6] Algunos ejemplos incluyen:

- El reto Momo: consiste en agregar a "Momo" -una foto con un personaje aterrador de ojos saltones, piel pálida y sonrisa tenebrosa- como contacto de WhatsApp. El delincuente usa el contacto Momo para robar información, cometer ciberdelitos, incitar al suicidio o a la violencia, acosar, extorsionar o generar algún trastorno psicológico.
- El reto de la Ballena Azul: propone realizar cincuenta pruebas que concluyen con el suicidio de la persona que está jugando.
- El reto de la pastilla: Este peligroso reto viral consiste en consumir ansiolíticos y ser el último en dormirse.
- La cicatriz francesa: Esta tendencia consiste en hacerse moratones horizontales en los pómulos a base de pellizcos fuertes, hasta que aparezcan las marcas faciales.
- El desafío de las 48 horas: Anima a irse de la casa y desaparecer durante 48 horas sin avisar a nadie, ni familia ni conocidos y sin dejar forma de comunicarse, con el objetivo de crear alarma inmediatamente.
- Quien duerma el último, gana: Reta a los menores a tomar el ansiolítico Rivotril (clonazepamha), que produce somnolencia extrema.

Recomendaciones

- ✔ **Fomenta relaciones positivas**, animándolos a interactuar y compartir información con personas que aporten valor, desde compañeros de clase hasta profesionales reconocidos por sus habilidades en distintos campos.
- ✔ **Ayúdales a crear contenido de calidad,** que refleje lo mejor de ellos sin comprometer su privacidad o seguridad y que sea respetuoso con otros usuarios.
- ✔ **Inculca un pensamiento crítico**, especialmente respecto a retos y contenidos que puedan ser perjudiciales o peligrosos. Discute abiertamente sobre los peligros de actividades como bromas pesadas, violencia y cualquier forma de autolesión o comportamiento riesgoso.
- ✔ **Fomenta la responsabilidad digital**: Enséñales la importancia de no participar en la difusión de material dañino o peligroso y aliéntalos a denunciar cualquier contenido que consideren inapropiado o ilegal.
- ✔ **Informa y explica qué es el acoso** y el ciberacoso para que puedan identificarlo y abordarlo eficazmente.
- ✔ **Ofrece apoyo** y busca la ayuda de otros adultos, como profesores, entrenadores, psicólogos u otras madres y padres, para abordar y resolver situaciones de ciberacoso de manera rápida y eficaz.
- ✔ **Denunciar.** En casos graves, es crucial denunciar los hechos ante la autoridad competente para garantizar la seguridad y el bienestar de los menores afectados.
- ✔ **Implementa controles parentales** que ofrecen los sistemas operativos y proveedores de internet, para filtrar contenido, limitar el uso de aplicaciones, gestionar horarios y monitorear actividades como el uso de redes sociales. Selecciona cuidadosamente estas herramientas de forma que se ajusten a tus necesidades y que ofrezcan seguridad sin introducir nuevos riesgos:
  - No instales la aplicación sin informar a los jóvenes. Explícales que es una medida de protección.
  - Establece acuerdos claros sobre el uso de dispositivos. Si necesitan ajustes, modifícalos según sea necesario.
  - Predica con el ejemplo en el uso que haces de tus propios dispositivos.
  - Discute la importancia de los filtros y las precauciones online, así como los riesgos y beneficios de internet.
  - Prioriza su privacidad y asegúrate de que se sientan respetados, no vigilados.
- ✔ Restablece los "*feeds*". Por ejemplo, el "Para Ti" de TikTok o la página de exploración de Instagram, limpiando el historial de búsqueda.
- ✔ Establece límites de tiempo de pantalla para controlar el *scrolling* infinito.
- ✔ **Evita bloqueos** excesivos, ya que puede ser contraproducente.

ENCUENTRA AQUÍ ALGUNOS RECURSOS ÚTILES:

- Guía sobre controles parentales del Internet Segura For Kids (is4k) del INCIBE
- Tipos de control parental - INCIBE
- Servicios para educadores, familias y jóvenes del is4k del INCIBE
- Contenido inadecuado – INCIBE
- Retos virales - INCIBE
- Recomendaciones para padres y tutores para la protección del menor en Internet de la Agencia Española de Protección de Datos (AEPD).
- Decálogo de principios. Verificación de de edad y protección de personas menores ante contenidos inadecuados - AEPD
- Patrones adictivos en el tratamiento de datos personales - AEPD

B. Riesgos para la privacidad y protección de datos personales de las personas menores

La **huella digital**, o identidad online, es esencialmente el **registro de nuestra actividad en Internet**. Se compone de la información que compartimos voluntariamente, como nombres, edad, profesiones y correos electrónicos, además de datos sobre nuestras acciones y preferencias recopiladas cada vez que interactuamos online, a través de acciones como enviar correos, publicar fotos y comentarios o registrarnos en sitios web. Estos datos, que pueden parecer efímeros, en realidad **se almacenan y conforman una imagen duradera de nuestra identidad digital**. **Reflexionar sobre la creación consciente de nuestra huella digital desde una edad temprana es crucial.**

Además, es importante considerar los riesgos relacionados con la privacidad y la seguridad de los datos personales, que se enumeran a continuación.

Robo o suplantación de identidad [7]

La suplantación de identidad consiste en **hacerse pasar por otra persona de forma malintencionada**, para obtener beneficios económicos, información privada para dañar a esa o a otra persona, por ejemplo, con insultos, burlas, chantajes o amenazas. Puede perseguir diferentes fines: objetivo económico, robo de cuentas e información, hacerse pasar por el menor, difundir fraudes y *malware, grooming*[8] o ciberacoso[9].

[7] https://www.incibe.es/menores/tematicas/suplantacion-de-identidad

[8] Se refiere al acoso sexual a niños, niñas y adolescentes a través de medios digitales, consistente en acciones desplegadas generalmente por personas adultas, de cara a establecer contacto con fines sexuales

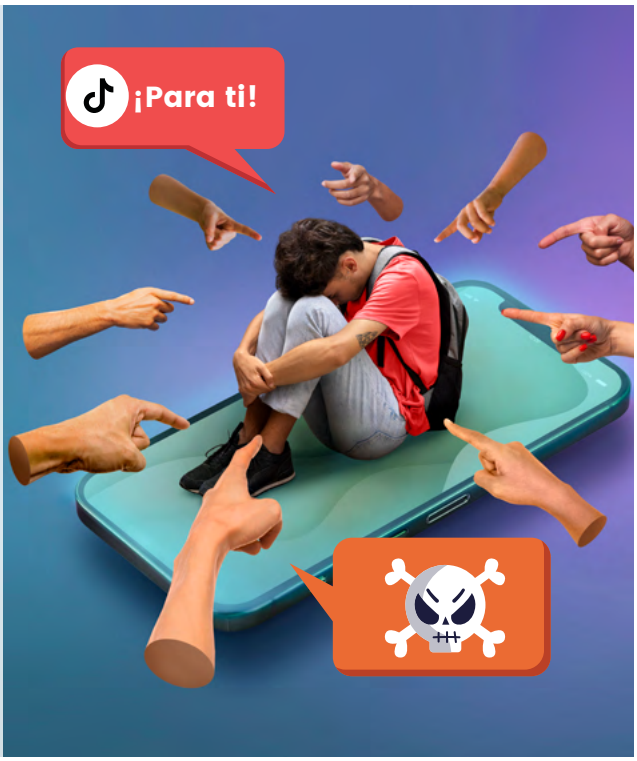
[9] Tipo de acoso que afecta a niños, niñas y adolescentes, que consiste en que uno o varios menores hagan daño (verbal y/o psicológico) a una víctima, también menor, conscientemente y de manera repetida a través de los medios digitales.

Explotación de datos personales para personalizar contenido de manera que dañe la salud y el bienestar, especialmente de menores[10]

Para personalizar la experiencia en línea de sus usuarios, los sistemas de recomendación de las redes sociales dependen de **patrones de comportamiento**, que **pueden revelar vulnerabilidades** individuales como adicciones, trastornos alimenticios, complejos corporales, ansiedad o trastornos depresivos. Como resultado de esto, los sistemas de recomendación terminan explotando tales vulnerabilidades para maximizar el compromiso ("*engagement*") de las personas usuarias. También crean **bucles de retroalimentación** que conducen a las usuarias hacia selecciones de contenido más acotadas, que se corresponden con sus vulnerabilidades.

Un determinado contenido puede no ser peligroso en sí mismo y de forma aislada, pero se vuelve dañino si lo consumen personas vulnerables, como es el caso de personas menores. Caer en la trampa del "***doomscrolling***" (por ejemplo, exposición excesiva a contenido relacionado con autolesiones, dietas o imágenes corporales idealizadas) desencadena un "*engagement* insalubre", que puede impactar negativamente en su bienestar y **agravar problemas de salud mental preexistentes**.

Existen casos reales que evidencian esta cuestión[11]. Los resultados de una investigación técnica desarrollada por Amnistía Internacional muestran que los niños, niñas y jóvenes que ven contenidos relacionados con la salud mental en la página "Para ti" de TikTok se ven rápidamente abocados a una espiral de contenidos potencialmente nocivos, incluidos vídeos que idealizan y fomentan el pensamiento depresivo, las autolesiones y el suicidio[12].



[10] https://panoptykon.org/sites/default/files/2023-08/Panoptykon_ICCL_PvsBT_Fixing-recommender-systems_Aug%202023.pdf

[11] Por ejemplo, en octubre de 2022, tras una investigación sobre la muerte de Molly Russell, de 14 años, el Sr. Coroner Andrew Walker encontró que Russell "murió por un acto de autolesión mientras sufría de depresión y los efectos negativos del contenido en línea". El forense encontró que los motores de recomendación de Instagram y Pinterest finalmente llevaron a Russell a su muerte. Y concluyó que Russell tenía acceso a contenido para adultos que no debería haber estado disponible para que lo viera una niña de 14 años. En el informe de prevención de futuras muertes, dijo: "la forma en que operaban las plataformas significaba que Molly tenía acceso a imágenes, videoclips y textos relacionados con autolesiones y suicidio, o que de otra manera eran negativos o deprimentes en su naturaleza. La plataforma operaba de tal manera, usando algoritmos, que en algunas circunstancias resultaba en períodos de atracones de imágenes, videoclips y texto, algunos de los cuales fueron seleccionados y proporcionados sin que Molly los solicitara. Estos períodos de atracones, si involucraban este contenido, probablemente habrían tenido un efecto negativo en Molly. Parte de este contenido romantizaba los actos de autolesión por parte de los jóvenes".

Por otro lado, un estudio realizado por un centro italiano para trastornos alimentarios en la infancia y la adolescencia entre 78 pacientes investigó el uso de TikTok entre jóvenes con trastornos alimentarios. Se encontró que el algoritmo de TikTok frecuentemente mostraba a los usuarios contenido relacionado con trastornos alimentarios sin que ellos tuvieran que buscarlo. A su vez, un análisis realizado por el Centro para Contrarrestar el Odio Digital (CCDH) encontró que los videos recomendados por TikTok sobre salud mental o imagen corporal se mostraban a "cuentas estándar de adolescentes" cada 39 segundos. El contenido recomendado incluía dietas peligrosamente restrictivas, contenido pro-autolesión y contenido que romantiza el suicidio a usuarios que muestran una preferencia por el material, incluso si están registrados como menores de 18 años. En igual sentido, una investigación de The Wall Street Journal encontró que el algoritmo de TikTok expone a los usuarios a contenido dañino, incluyendo videos sobre autolesiones, dietas extremadamente dañinas y suicidio.

[12] https://www.amnesty.org/es/latest/news/2023/11/tiktok-risks-pushing-children-towards-harmful-content/

Exposición de información personal sin consentimiento o con consentimiento inválido: el caso de los deepfakes o de la "venta de iris"

El **uso de la tecnología para generar y distribuir contenido sexual sin consentimiento** es un problema que arrastra en particular la tecnología ***deepfake***. Por ejemplo, una persona toma una foto de una compañera de clase sin su permiso y utiliza una aplicación de IA para modificar su imagen, creando versiones alteradas o comprometedoras. Estas imágenes modificadas luego son compartidas en redes sociales, exponiendo a su compañera y potencialmente dañando su reputación. Las investigaciones sobre el tema apuntan a que la grandísima mayoría de víctimas (el 96%) son mujeres[13]. Si este contenido afecta a un menor, puede dañar gravemente su bienestar y salud mental, perjudicar su imagen y reforzar la problemática del abuso y explotación sexual contra menores.

Otra práctica puesta en marcha por algunas empresas es el **escaneo de iris a cambio de "criptomonedas"**. El iris es un dato sensible, ya que se trata de un dato biométrico. Como tal, tiene un régimen de protección especial y su uso debe estar muy justificado y constar de un consentimiento válido. Cabe recordar que solo a partir de los 14 años se puede dar dicho consentimiento y que, para que el mismo sea válido, debe ser libre e informado. No sería el caso de vender tu iris sin comprender las políticas de privacidad de la empresa.

Publicidad dirigida a menores[14]

La **publicidad** es tan **omnipresente** en Internet que a menudo es difícil distinguir entre contenido genuino y anuncios. Los menores son especialmente susceptibles a técnicas invasivas de recolección de datos, frecuentemente empleadas para la publicidad dirigida o fines más dañinos.

En el ámbito digital, la publicidad se manifiesta en formas diversas como *banners* llamativos, *pop-ups* que interrumpen la navegación y resultados patrocinados que a veces **se camuflan como contenido orgánico** bajo etiquetas como "anuncio" o "patrocinado". Además, en plataformas de redes sociales, *influencers* y creadores de contenido discuten temas populares entre los jóvenes, como videojuegos o juguetes, donde sus publicaciones, aunque no siempre marcadas como publicidad, pueden influir significativamente en las percepciones y decisiones de compra de los menores.

Las empresas **compilan perfiles detallados de los intereses de los usuarios** basándose en sus actividades online para **dirigir anuncios personalizados**. En las redes sociales, el fenómeno de la publicidad personalizada es aún más relevante, dado el elevado grado de conocimiento que tienen de sus usuarios. A pesar de que la legislación europea prohíbe la publicidad personalizada a menores, existen brechas y situaciones en las que estos perfiles se utilizan para influir en las decisiones de compra de los menores o para promover productos no adecuados para su edad.

[13] **https://cecu.es/wp-content/uploads/2023/06/Abordar-los-danos-a-las-personas-consumidoras-de-la-IA-generativa_CECU.pdf**

[14] **https://www.incibe.es/menores/blog/menores-de-edad-y-la-publicidad-en-internet**

Recomendaciones:

- ✔ **Establece métodos de desbloqueo seguros** y evita que otros vean las contraseñas al ingresarlas. No dejes dispositivos desbloqueados y sin vigilancia.
- ✔ **Utiliza contraseñas largas y únicas** para cada cuenta y servicio. Puedes utilizar un gestor de contraseñas.
- ✔ Añade una capa extra de seguridad con la **autenticación de doble factor**, que requiere un código temporal después de ingresar la contraseña.
- ✔ En **equipos de uso compartido**, navega en modo privado, evita guardar credenciales, cierra sesión después de usar y borra los datos de navegación.
- ✔ **Mantén actualizado el software** y utiliza **antivirus**. Sé cauteloso con enlaces o archivos en mensajes de redes sociales, chats de videojuegos o emails, y analízalos con un antivirus online.
- ✔ **Mantén tu navegador actualizado** y activa las configuraciones de **protección antirrastreo**. Utiliza la opción *"Do not track"* si está disponible y considera bloquear las *cookies* de terceros, especialmente en modo privado.
- ✔ **No instales aplicaciones innecesarias**: puede aumentar los riesgos de seguridad.
- ✔ **Privacidad y gestión de exposición en Internet**: Configura las cuentas en modo privado, utiliza configuraciones de privacidad avanzadas y acepta solo a contactos conocidos personalmente. Publica de manera consciente y crítica y rechaza compartir información personal bajo cualquier circunstancia.
- ✔ **Activa alertas en buscadores** a modo de *egosurfing* (buscar el nombre del menor en Internet) para detectar posibles suplantaciones, comentarios relacionados o información confidencial.
- ✔ **Identifica perfiles falsos.** Desconfía de perfiles con poca actividad o contenido sospechoso, discrepancias en el lenguaje, insistencia en obtener información personal o coincidencias excesivas con los intereses del menor.
- ✔ Utiliza navegadores, *launchers,* aplicaciones y versiones **diseñadas específicamente para niños/as**, ya que suelen ser menos intrusivas y más seguras.
- ✔ **Presta atención a todos los dispositivos conectados.** Recuerda que dispositivos como *Smart TVs* y videoconsolas también están expuestos a riesgos similares y requieren configuraciones de seguridad adecuadas.
- ✔ Asegúrate de entender y **controlar cómo se retienen y utilizan los datos** personales de los menores para evitar usos no autorizados o inapropiados.
- ✔ **Evita el "*shareting*"** -compartir imágenes online de personas menores de edad- o hazlo de forma responsable.
- ✔ **Dialoga sobre *deepfakes*:** Comparte impresiones intercambiando puntos de vista sobre qué opinan de estos contenidos. Enseña claves que les ayuden a reconocer que existe una alteración del contenido o a identificar *fake news.*
- ✔ **Fomenta el pensamiento crítico** en los menores ayudándoles a reconocer y entender las estrategias publicitarias.
- ✔ **Utiliza bloqueadores de anuncios** en navegadores y ordenadores para limitar la cantidad de publicidad que se muestra.
- ✔ **Elige espacios en Internet con menos publicidad invasiva**, con contenidos de calidad y fuentes fiables.
- ✔ **Configura y gestiona los ajustes de anuncios** en redes sociales y plataformas online para evitar publicidad personalizada.
- ✔ **Enseña a no compartir datos** personales innecesariamente.
- ✔ **Promueve el consumo responsable**, evitando compras impulsivas y evaluando la necesidad real de los productos.
- ✔ **Limita el tiempo frente a pantallas** para reducir la exposición a publicidad, estableciendo acuerdos familiares sobre el uso compartido de dispositivos y empleando herramientas de control parental.

ENCUENTRA AQUÍ ALGUNOS RECURSOS ÚTILES:

- Configuración de privacidad en redes sociales - INCIBE
- ¿Qué hacer frente a un caso de suplantación de identidad en menores? - INCIBE
- Grooming – INCIBE
- Ciberacoso - INCIBE
- Alfabetización mediática para proteger a los y las menores frente a los deepfakes – INCIBE
- Una empresa escanea el iris a menores a cambio de criptomonedas en un centro comercial - INCIBE
- La publicidad en las plataformas de vídeo en Internet – is4k - INCIBE
- Menores de edad y la publicidad en Internet - INCIBE
- Los niños ante la publicidad - Cátedra de Marketing y Comunicación Infantil y Adolescente, Universidad Complutense de Madrid
- Medidas para minimizar el seguimiento en Internet – AEPD.
- 10 consejos para realizar un *'sharenting'* responsable – AEPD y Pantallas Amigas

C. Riesgos Técnicos y de Seguridad [15]

Malware

El ***malware*** es cualquier programa malicioso diseñado para **infectar, dañar o acceder a sistemas informáticos** con el fin de engañar y de que no se detecte su ejecución. Existen distintos tipos de *malware* con objetivos distintos, como los virus, los gusanos o los troyanos.

El *malware* puede llegar a los dispositivos de las personas menores a través del uso que hacen de sus redes sociales, donde están más expuestos a perfiles o contenidos falsos y donde se difunden archivos infectados o enlaces maliciosos. En el ámbito de los videojuegos también pueden ser atraídos a descargar juegos, trucos o extras desde fuentes no confiables, que pueden contener *malware* que se instala en su dispositivo.

Phishing

Es un método utilizado por los ciberdelincuentes para engañar a las personas y **hacer que revelen información personal**, como contraseñas o datos bancarios para el robo de cuentas. Se suelen utilizar los chats internos de las aplicaciones y videojuegos, el envío de SMS al teléfono móvil, mensajes de correo electrónico, o mensajes privados de las redes sociales, con excusas alarmistas para que hagan clic en un enlace malicioso donde se captura el usuario y contraseña de la víctima.

[15] https://www.incibe.es/menores/blog/como-puede-llegar-el-malware-los-dispositivos-de-tus-hijosas

Recomendaciones:

- ✔ **Descarga** las aplicaciones y *software* desde **fuentes oficiales** para evitar *malwares*.
- ✔ **Mantén actualizados los sistemas operativos y aplicaciones**, incluyendo el antivirus, para fortalecer las defensas contra ataques.
- ✔ **Verifica los enlaces** mediante analizadores de URL antes de hacer clic, especialmente aquellos acortados que ocultan la dirección completa.
- ✔ **Crea contraseñas seguras y únicas** para cada cuenta y enseña a los menores a no compartirlas.
- ✔ **Implementa herramientas de control parental** para restringir el acceso a sitios web peligrosos o inapropiados –con las precauciones señaladas más arriba-.
- ✔ **Configura las opciones de seguridad y privacidad** presentes en los dispositivos, perfiles y cuentas de las que haga uso el/la menor.
- ✔ **Sé escéptico con ofertas** de descuentos o regalos en línea y verifica siempre la autenticidad de cualquier solicitud de datos personales.
- ✔ **Evita la ejecución de ventanas emergentes**, el acceso a enlaces desconocidos o archivos adjuntos en mensajes.
- ✔ **Evita conexiones inseguras.** Utiliza los datos móviles antes que redes Wi-Fi públicas para reducir el riesgo de interceptación de datos.
- ✔ **Realiza copias de seguridad** regulares para facilitar la recuperación de información en caso de infección por *malware*.

ENCUENTRA AQUÍ ALGUNOS RECURSOS ÚTILES:

- Protege a los menores frente al robo de cuentas - INCIBE
- ¿Cómo puede llegar el malware a los dispositivos de tus hijos/as? - INCIBE
- Virus y Malware - INCIBE
- Phishing – INCIBE

2. SEGUNDA PARTE DERECHOS Y FORMAS DE RECLAMACIÓN

En esta sección veremos los principales **marcos regulatorios**, los **derechos** reconocidos y las distintas **formas de reclamar** o actuar frente a diferentes escenarios que puedan poner en riesgo la salud, la privacidad, la protección de datos personales o la seguridad de nuestros niños, niñas, adolescentes y jóvenes.

Escenario Nº 1 ¿Cómo protegemos a nuestros niños/as del diseño adictivo de los servicios digitales?

Si bien no existe aún una normativa que aborde el diseño adictivo de los servicios digitales, es necesario conocer alguna de las pautas que establece la **Ley de Servicios Digitales (DSA, por sus siglas en inglés)**. Esta norma reconoce una serie de obligaciones y derechos que pueden contribuir a proteger a los menores frente este tipo de diseños, en caso de que sea aplicada efectivamente por las plataformas y las autoridades de control. Entre las obligaciones a cargo de los intermediarios en Internet, que incluye a las plataformas de redes sociales, destacamos:

- ✔ **La moderación de contenido:**
  - Las plataformas ya podían restringir contenido en función de sus **términos y condiciones**, por eso, la DSA exige que sean **públicos, accesibles** y que publiquen un **resumen** claro y compresible en los idiomas de la UE. Esto incluye publicar en formato legible por máquina y de forma fácilmente accesible, al menos una vez al año, informes sencillos sobre cualquier actividad de moderación de contenidos que hayan realizado durante el período pertinente.
  - Posibilidad de **impugnar** las decisiones de contenido, ya sea ante la plataforma o ante órganos extrajudiciales y, eventualmente, ante la justicia.
- ✔ **Explicación clara de las condiciones generales** y de cualquier restricción del uso del servicio, de manera que los menores lo puedan comprender.
- ✔ **Garantizar un elevado nivel de privacidad, seguridad y protección** de los menores en su servicio.
- ✔ **Prohibición de patrones oscuros:** No diseñar, organizar, ni gestionar sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio o que distorsionen u obstaculicen la capacidad de tomar decisiones libres e informadas.
- ✔ **Sistemas de recomendación y perfilado:** Hasta el momento había muy poca transparencia sobre cómo funcionan (a lo que se deben sumar los avances de la inteligencia artificial). Con la DSA, las plataformas tienen que ser más transparentes sobre cómo funcionan y dar más opciones de elección y control a los usuarios.
- ✔ En el caso de las **grandes plataformas y motores de búsqueda** (VLOPs/VLOSEs por sus siglas en inglés), que incluye, por ejemplo, a TikTok, Instagram, Facebook, Youtube, etc.:
  - Deben realizar **evaluaciones de riesgos sistémicos** en sus plataformas, incluidos los derivados del diseño o del funcionamiento de su servicio y los sistemas relacionados, como los sistemas algorítmicos; o del uso de sus servicios, para abordar los efectos negativos sobre los menores y en relación con sus derechos.
  - **Sistemas de recomendación:** Ofrecer una opción para cada sistema que no se base en la elaboración de perfiles.

Conocer estas obligaciones permitirá estar atento/a para denunciar su incumplimiento frente a las autoridades. En el caso de España, la autoridad de aplicación de la DSA es el **Coordinador de Servicios Digitales,** función a cargo de la **Comisión Nacional de los Mercados y la Competencia (CNMC**), que, dependiendo del caso, podrá llevar adelante la reclamación o deberá remitirla a la Comisión Europea, que es la autoridad de aplicación de las VLOPs/VLOSEs.

Escenario Nº 2 ¿Qué podemos hacer frente al contenido inapropiado o ilícito que es recomendado a nuestros hijos/as a través de Internet?

La exposición por parte de los niños, niñas, adolescente y jóvenes a contenido inapropiado e ilícito en Internet es un tema no resuelto. Las **redes sociales permiten denunciar contenido** por una variedad de razones, destinadas a mantener un entorno en línea seguro, respetuoso y legalmente conforme. Se pueden denunciar casos de acoso, injurias, calumnias, discriminación, odio, ciberdelitos, violencias, etc. para que esos contenidos sean retirados. Cada red social establece sus propias normas y políticas de uso que prohíben ciertos tipos de contenidos.

Ahora bien, bajo la DSA, las plataformas digitales **tienen que abordar el contenido ilegal**[16]. A tal fin, deben facilitar la denuncia de este tipo de contenidos y darle trámite y prioridad a la denuncia de los "alertadores fiables"[17]. Además, deben ser transparentes sobre las medidas que tomen y publicar informes. Esto incluye:

- ✔ **Mecanismos de notificación y acción** para que cualquier persona física o entidad les alerte de la presencia de elementos que esa persona o entidad considere ilícitos. Información para denunciar contenido ilícito en: Instagram, TikTok, Snapchat, X
- ✔ Dar una **declaración de motivos** clara y específica a cualquier destinatario del servicio afectado por restricciones impuestas si su contenido es ilegal o incompatible con sus condiciones generales.
- ✔ **Sistema interno de gestión de reclamaciones** que permitan reclamar contra las decisiones tomadas por el prestador de la plataforma.
- ✔ **Resolución extrajudicial de litigios:** Se puede elegir cualquier órgano de resolución que haya sido certificado para resolver litigios relativos a esas decisiones.
- ✔ Posibilidad de **reclamar** al Coordinador de Servicios Digital (la CNMC en España) por incumplimientos a la DSA.
- ✔ **Derecho a ser indemnizado** por cualquier daño o perjuicio sufrido por incumplimientos a la DSA.
- ✔ **Derecho a ser representado** por un organismo, organización o asociación para ejerza sus derechos en tu nombre.
- ✔ **Derecho a ser representado en una acción colectiva** por incumplimientos de la DSA.

En el caso de que exista un daño como consecuencia de un contenido ilícito, la plataforma no será responsable, a menos que:

- ✔ **Tenga conocimiento efectivo de una actividad o contenido ilícito** y, en lo que se refiere a una acción por daños y perjuicios, tenga conocimiento de hechos o circunstancias por los que la actividad o el contenido revele su carácter ilícito.
- ✔ Conociendo estos puntos, **no actúe con prontitud para retirar el contenido ilícito o inhabilitar el acceso al mismo.**

Es importante entender que, en principio, las plataformas digitales no son responsables del contenido que se sube a las mismas, pero podrán serlo si no actúan correctamente frente a la toma de conocimiento de una actividad o un contenido ilegal. **Por eso es muy importante denunciar los contenidos que se consideren ilegales.**

[16] Definición de contenido ilícito: toda información que, por sí sola o en relación con una actividad, incluida la venta de productos o la prestación de servicios, incumpla el Derecho de la Unión o el Derecho de cualquier Estado miembro.

[17] Condición otorgada por el Coordinador de Servicios Digitales a cualquier entidad que lo desee que tenga conocimientos y competencias para detectar contenido ilícito.

Escenario Nº 3 ¿Qué hacer frente a un caso de robo o suplantación de identidad de un menor, ciberacoso o *grooming*?

En este caso podría tratarse de delitos penales propiamente dichos, que también pueden dar lugar a acciones civiles o reclamaciones administrativas. Es importante actuar rápidamente para minimizar los daños y seguir los siguientes pasos:

✔ **Vía penal - Denunciar a las Fuerzas y Cuerpos de Seguridad** (Guardia Civil y Dirección General de la Policía), o ante **los tribunales de justicia**, por delitos como:

- La **usurpación de identidad** se considera un delito según el Código Penal, denominado "usurpación de estado civil" (art. 401). Las consecuencias pueden variar desde multas hasta penas de prisión de hasta tres años.
- El ***grooming*** se encuentra tipificado en el artículo 183 del Código Penal, que prevé penas de prisión de uno a tres años o multas coercitivas.
- La **distribución** o difusión pública a través de Internet de **contenidos destinados a promover, fomentar o incitar a la autolesión** de menores de edad o personas con discapacidad necesitadas de especial protección conlleva penas de prisión de seis meses a tres años (art. 156 ter. del Código Penal).

✔ **Consejos para presentar denuncias:**

- Guarda todas las pruebas necesarias (imágenes, conversaciones, vídeos, correos o mensajes, etc.).
- Presenta la denuncia inmediatamente y no realices investigaciones por tu cuenta.

✔ **Otros Recursos disponibles:**

- Contacta con La Linea de Ayuda del INCIBE 017, donde te ofrecerán asesoramiento técnico, en cuestiones de ciberseguridad, psicosocial y legal.

✔ **Vía civil:**

Reclamar una compensación por los daños causados. La cantidad de la indemnización será determinada en función de los daños y perjuicios sufridos:

- Esta reclamación se puede **interponer contra el responsable directo** de la acción que nos ha causado el daño (difusión de contenido sin consentimiento, por ejemplo) **y/o contra la propia plataforma** si no ha adoptado las medidas legalmente previstas para evitar, o para no permitir que se siga produciendo, la comisión de un acto ilegal o delito. Las plataformas te ofrecen canales información y denuncia para que puedan adoptar tales medidas:

  | Ciberacoso: TikTok, Instagram, Facebook, X

  | Suplantación de identidad: TikTok, Instagram, Facebook, X

  | Cuentas pirateadas o hackeadas: TikTok, Instagram, Facebook

  | Contenido inapropiado/ilegal: Instagram, TikTok, X

- **Tribunales de justicia.** Podremos acudir a los tribunales para reclamar una compensación por daños y perjuicios sufridos si nuestra reclamación previa no ha sido debidamente atendida.

✔ **Frente a las plataformas, puedes acudir a la vía administrativa:**

- **AEPD:** En caso de incumplimientos del Reglamento General de Protección de Datos (RGPD) o de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

  En casos de difusión de contenido sexual o violento, si la plataforma no retira ese contenido después de haberlo solicitado, realiza una denuncia a través de Canal prioritario de la AEPD.

- **CNMC:** En caso de incumplimiento de la DSA, por ejemplo, inacción de una plataforma frente a una denuncia de contenido ilegal.

Si son viables, puedes optar por todos estos caminos.

Escenario Nº 4

¿Qué hacer si exponen información personal de un menor sin consentimiento, por ejemplo, si generan y comparten un *deepfake* o explotan sus datos personales o si un menor "vende" su iris?

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, contempla la necesidad de otorgar una protección real a las personas menores de edad en Internet, a cuyo fin obliga a los padres, madres, tutores, cuidadores o representantes legales a procurar que **hagan un uso equilibrado y responsable de los dispositivos digitales** y de los servicios de la sociedad de la información, al objeto de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales (artículo 84).

Es importante conocer los derechos que asisten a las personas menores –y a las personas en general- en relación con la protección de sus datos personales. Para ello, es necesario conocer algunas pautas relevantes del RGPD:

- ✔ **El consentimiento:** es una base legal crucial para el tratamiento de datos personales. Se trata de cualquier manifestación **de voluntad libre, específica, informada e inequívoca** por la que la persona interesada acepta, mediante declaración o acción afirmativa, el tratamiento de datos personales que le conciernen. Lamentablemente, en el entorno digital, pocas veces nos encontramos frente a un consentimiento dado de tal forma, ya que la propia vulnerabilidad y asimetría digitales hace que no seamos conscientes de cómo somos inducidos –a través de técnicas de manipulación- a dar consentimientos que no son ni libres, ni específicos ni inequívocos.

- ✔ **La edad para brindar el consentimiento está establecida a partir de los 14 años.** Para menores de esta edad, cualquier tratamiento de datos basado en el consentimiento solo es válido si lo otorgan los titulares de la patria potestad o tutela. No obstante, la política de privacidad de la empresa puede imponer una edad mayor, por lo que es recomendable revisarla. Por otro lado, según la legislación de protección de datos, la clave es la información y transparencia para que un consentimiento pueda considerarse válido.

- ✔ **Derechos específicos bajo el RGPD.** Además del derecho a ser informados, los menores pueden ejercer derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento de sus datos, así como oponerse a decisiones automatizadas, incluida la elaboración de perfiles. Para menores de 14 años, estos derechos deben ser ejercidos por los titulares de la patria potestad o sus tutores legales. Los mayores de 14 años pueden ejercer estos derechos por sí mismos.

Frente a un caso en el que se **expone información personal** de un menor sin consentimiento dado –o siendo el mismo inválido-, existen varias vías de actuación:

1. **Denunciar ante la propia plataforma**. Recursos por difusión de contenido sin consentimiento: Facebook, Instagram, TikTok, Twitter, YouTube y en buscadores Google y Bing

2. En el resto de los casos, dirígete al responsable del tratamiento de datos de la entidad (por ejemplo, en el caso de la venta de iris o cualquier otro tratamiento de datos biométrico).

3. Dirigirte a la **AEPD** para presentar denuncia o reclamación, en caso de que la plataforma no retire el contenido denunciado o el responsable del tratamiento no acepte la reclamación. Modelos de reclamaciones aquí. Para retirada inmediata de contenido sexual o violento frente a la inacción de plataforma, acude al Canal Prioritario de la AEPD.

4. Si consideras que alguna actuación ha podido ser constitutiva de **delito**, ponte en contacto el Grupo de Delitos Telemáticos de la Guardia Civil o la Brigada de Investigación Tecnológica de la Policía Nacional**.** También puedes reclamar una compensación por daños y perjuicios al responsable de los hechos o a la plataforma por incumplimiento de la normativa.

Escenario Nº 5 ¿Qué protege a nuestros menores del abuso de anuncios personalizados con su información?

Que un anuncio se identifique claramente como "publicidad" es un requisito básico, aunque también deberá cumplir con el resto de las normas aplicables. En nuestro país, coexisten múltiples normativas y códigos de autorregulación en materia de publicidad, Internet y menores, lo que añade complejidad al cumplimiento legal y a su verificación[18]. La pregunta de cómo debe ser la publicidad dirigida a niños/as no es sencilla de responder, pues dependerá del producto, del medio en el que se difunda el anuncio y de la edad a la que se dirige. Para empezar, la publicidad debe:

- ✔ **Respetar la ley**.
- ✔ **Diferenciarse como publicidad**.
- ✔ **Identificarse como anunciante** o mensaje publicitario. El anunciante se mostrará sin equívocos ante el menor, de modo que incluso se pueda contactar con él.
- ✔ Mostrarse **veraz**, lo que significa que debe evidenciar cómo son los productos que ofrece y sus características y no llevar a confusión sobre sus prestaciones.
- ✔ Ser **leal respecto de sus competidores**, sin denigrar o imitar características de otros productos y marcas de forma que pueda provocar confusión.

Ahora bien, en el ámbito digital a menudo es más **difícil distinguir entre contenido genuino y anuncios**, especialmente debido a la existencia de *influencers* y creadores de contenido que pueden condicionar las percepciones y decisiones de compra de los menores.

En tal sentido, y más allá de que existe un gran cúmulo de regulaciones y autorregulaciones, que no terminan de abordar la complejidad del entorno digital, resulta relevante al menos conocer algunas disposiciones de dos normas:

- ✔ **Ley General de Comunicación Audiovisual (LGCA):** Esta norma establece que las **plataformas de intercambio de vídeos** -en las que pueden incluirse las redes sociales- tendrán que adoptar medidas que **limiten el acceso del menor a la publicidad de riesgo para el desarrollo físico, mental o moral,** y otras restricciones para *influencers* o usuarios de especial relevancia. Para ello, será necesario establecer mecanismos transparentes y sencillo que permitan:
  - **Notificar** al prestador los contenidos que vulneren las obligaciones.
  - **Explicar** el curso que se ha dado a las notificaciones.
  - **Calificación** por parte de los usuarios de los contenidos que puedan vulnerar las obligaciones.
  - **Verificar la edad** con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores e impedir el acceso a los contenidos más nocivos, como la violencia o la pornografía.

[18] La problemática reside en que no hay una única norma específica y unívoca sobre publicidad y los menores. Hay leyes generales que aunque no hablan de menores les son aplicables (como la Constitución o el Código Civil), normas de menores que no hablan de publicidad pero incluyen ciertos principios que deben ser tenidos en cuenta (Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor), leyes generales de publicidad que mencionan a los niños (Ley 34/1988, de 11 de noviembre, General de Publicidad o Ley 3/1991, de 10 de enero, de Competencia Desleal); otras que se centran en determinados sectores publicitarios (alcohol y tabaco) y otras; en medios (Ley 13/2022, de 7 de julio, General de la Comunicación Audiovisual y Ley 55/2007, de 28 de diciembre, del Cine). De otro lado existen Códigos de Autorregulación sectoriales como juguetes, juegos de azar y alimentación, entre otros.

Y por si esto no fuera suficientemente complicado, debemos asumir que conviven normas europeas, nacionales y autonómicas que pueden no coincidir e incluso parecer contradictorias.

- **El control parental**, con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores.
- **La resolución de reclamaciones,** en relación con la aplicación de estas medidas.
- **La resolución extrajudicial de conflictos** mediante procedimientos alternativos de litigios de consumo.

✔ **DSA:** Bajo esta ley, las plataformas en línea, como las redes sociales, tienen ciertas obligaciones para proteger a las personas frente a la publicidad excesiva que se encuentra en Internet y, en especial, a los menores:

- **Anuncios menos personalizados y más transparentes.** Las personas deben poder conocer quién realiza el anuncio y quién ha pagado por el mismo. Además, las grandes plataformas tienen que poner a disposición de los usuarios una biblioteca de anuncios para encontrar información sobre ellos. Por ejemplo, biblioteca de anuncios de Meta, biblioteca de contenido comercial de TikTok, depósito de anuncios de X.
- **Prohibición de presentar anuncios basados en elaboración de perfiles mediante el uso de datos personales de menores** cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor.

Si detectas infracciones a estas normativas:

1. **Reclama ante la propia plataforma**.
2. Si no se resuelve, reclama ante la **CNMC** (si trata de incumplimientos a la LGCA o a la DSA) o a la **AEPD** (si trata de incumplimientos al RGPD o la LOPDGDD).

Escenario Nº 6 ¿Qué hacer si un ataque de *malware* o *phishing* ha afectado la información de un menor?

En primer lugar, puedes ponerte en contacto con el INCIBE en el 017, donde podrán ayudarte y asesorarte en materia de ciberseguridad. También disponen de un servicio de asistencia psicosocial y asesoramiento legal. Con esta información, también podrían verificar los hechos y alertar al resto de ciudadanos

A su vez, es recomendable denunciar el incidente para que se investigue el origen del delito. Así, colaboras en las labores de prevención a otras empresas y en las acciones para capturar al ciberdelincuente. La denuncia se puede realizar ante la Guardia Civil – Grupo de Delitos Telemáticos o ante la Brigada Central de Investigación Tecnológica de la Policía Nacional. En su caso, también podrás dirigirte a los tribunales de justicia para denunciar la comisión de un delito y reclamar la compensación correspondiente.

noclamesreclama.org

2024

Más información en nuestra web

www.noclamesreclama.org

Y en nuestra app RECLAMA

Android Apple

Síguenos también en:

Redes sociales

Facebook: noclamesreclama

X: @NOCLAMESRECLAMA

Youtube: noclamesreclama

info@noclamesreclama.org

MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

FEDERACIÓN DE CONSUMIDORES Y USUARIOS CECU

www.cecu.es

El presente proyecto ha sido subvencionado por el Ministerio de Derechos Sociales, Consumo y Agenda 2030, siendo su contenido responsabilidad exclusiva de CECU. 2024