Cuadernos del Audiovisual
del Consejo Audiovisual de Andalucía

Las consecuencias del uso de los medios digitales en la infancia y la adolescencia. Estado de la cuestión

The consequences of the use of digital media in childhood and adolescence. State of play

Mar España Martí
Agencia Española de Protección de Datos
secretaria.direccion@aepd.es https://orcid.org/0009-0003-2375-039X

María Angustias Salmerón Ruiz
Hospital Ruber Internacional
mangustias.salmeronr@ruberinternacional.es https://orcid.org/0009-0005-8859-9744

Recibido: 30/10/2024 | **Aceptado:** 21/11/2024

Resumen: El uso intensivo y temprano por parte de niños, niñas y adolescentes de los servicios que se proporcionan en el entorno digital tiene un enorme impacto en su funcionamiento intelectual y comportamental, al tratarse de personas vulnerables que se encuentran en desarrollo. En este artículo se analizan las consecuencias que una hiperconexión incontrolada tiene en áreas como la salud, la privacidad o el ámbito educativo. Asimismo, recoge algunas propuestas públicas para intentar frenar las consecuencias expuestas, como la puesta en marcha de un sistema de verificación de edad efectivo para acceder a determinados servicios de Internet o herramientas de ayuda para intentar frenar la difusión de contenido sensible.

Palabras clave: adolescencia; hiperconexión; infancia; salud; privacidad.

Abstract: The intensive use and early involvement of children and adolescents into the services provided in the digital environment has an enormous impact on their intellectual and behavioral performance, because they are vulnerable individuals still immature. This paper analyzes the consequences of uncontrolled hyperconnection in areas like health, privacy and education. It also includes some public proposals to try to get rid of the consequences described above, by means of the implementation of an effective age verification system for accessing certain Internet services or supporting tools to try to avoid the dissemination of sexual or violent content.

Keywords: adolescence; hyperconnection; childhood; health; privacy.

CC BY-NC-SA 4.0

Cómo citar:

España Martí, M., Salmerón Ruiz, M.A., (2025). Las consecuencias del uso de los medios digitales en la infancia y la adolescencia. Estado de la cuestión. *Cuadernos del Audiovisual del Consejo Audiovisual de Andalucía*, (13), 60-76. https://dx.doi.org/10.62269/cavcaa.XX

Junta de Andalucía ca:A Consejo Audiovisual de Andalucía

1. Introducción

El impacto del entorno digital en la infancia y la adolescencia ha supuesto un drástico cambio en su forma de informarse, comunicarse, relacionarse y hasta en su educación, en un momento clave para su desarrollo personal. Esta evolución permitió mejorar la calidad de vida en muchos ámbitos (educativo, ocio, social), pero también ha supuesto retos en materia de salud y privacidad como consecuencia del uso de las pantallas, las conductas o comportamientos inadecuados, debiendo impedir la instauración de patrones adictivos en el uso de los dispositivos digitales.

Las pantallas han causado una profunda trasformación del funcionamiento intelectual y comportamental de los jóvenes, donde la inmediatez, el paso frenético de una actividad a otra y su validación en las redes sociales forman parte esencial de su día a día.

Los niños, niñas y adolescentes (en adelante, NNA) se han convertido en uno de los grupos que más servicios y contenidos digitales consume, contenidos que en ocasiones están destinados exclusivamente a los adultos, desde edades tempranas.

2. Uso y estandarización de la tecnología

La tecnología impacta en el cerebro y en la salud a todos los niveles (físico, psicológico, social y sexual) y a cualquier edad (desde el nacimiento hasta el final de la vida). Los NNA son un grupo de edad especialmente vulnerable al estar en desarrollo.

Los datos que se recogen en diversos estudios así lo demuestran. La encuesta del Instituto Nacional de Estadística (INE) sobre equipamiento y uso de tecnologías de información y comunicación en los hogares de 2023 recoge que el 91,7 % de los niños y niñas de diez años utilizaron Internet en los tres meses anteriores, una cifra que asciende al 97,1 % con quince años. Más de un 23 % del primer grupo dispone de teléfono móvil, dándose un salto exponencial en los doce años, con más de un 72 % (INE, 2023).

Por su parte, UNICEF, en su estudio *Impacto de la tecnología en la adolescencia* recoge que la edad media del primer móvil se sitúa por debajo de los once años. El 98,5 % de los adolescentes está registrado en más de una red social, y el 61,5 % dispone de más de un perfil. El 31,5 % usa Internet más de cinco horas a diario, porcentaje que asciende al 49,6 % los fines de semana, que seis de cada diez adolescentes duermen con el móvil y uno de cada cinco se conecta a partir de la medianoche (UNICEF, 2020).

Otros datos preocupantes son los relativos al acceso de los menores de edad a contenidos *online* para adultos, en concreto a la pornografía. Save the Children, en su informe *(Des)información sexual: pornografía y adolescencia*, alerta de que los primeros contactos con la pornografía comienzan en torno a los 8-9 años. El 58 % lo ha tenido antes de los trece años y el 8,7 % antes de los diez, edades en las que su desarrollo cognitivo no les permite entender lo que están viendo. El 47,4 % confiesa que alguna vez ha imitado lo que ha visto, pero no siempre de común acuerdo con la otra parte de la relación (Save the Children, 2020).

El acceso a esos contenidos a edades tan tempranas afecta a su desarrollo integral en un momento en el que la personalidad no está formada, generando importantes

desórdenes en la concepción de las relaciones sexuales y del rol de la mujer. La Fiscalía General del Estado, en su última Memoria, alerta del alarmante incremento en los últimos cinco años de las agresiones sexuales perpetradas por menores, un 116 %. La Fiscalía señala que, si bien este incremento obedece a causas complejas y que confluyen diversos factores, apunta a la carencia de una adecuada formación ético-sexual y al visionado inapropiado y precoz de material pornográfico violento (FGE, 2022).

Otro efecto importante derivado del uso de la tecnología digital es el de la violencia digital de género. Un estudio de la Fundación ANAR refleja que las TIC tienen una implicación relevante en los casos de violencia de género entre adolescentes, un 79,7 %, que, según ANAR, ha aumentado en 11,9 puntos en la postpandemia, favorecida por el temprano acceso a los dispositivos electrónicos (Fundación ANAR, 2023).

El mismo estudio refleja un crecimiento preocupante de los comportamientos machistas entre los más jóvenes, con unos datos inquietantes: el 70,3 % de los adolescentes no denuncian la violencia que sufren ni tienen intención de hacerlo. Además, el 47,1 % no es consciente del problema.

3. El impacto en la salud

El consumo de pornografía a edades tempranas puede producir que se normalicen conductas sexuales de riesgo. Los datos del tiempo y hábitos de uso de las pantallas y de los servicios y aplicaciones digitales que implica son preocupantes por las nocivas consecuencias que pueden producir y que, en personas vulnerables como los NNA, en pleno desarrollo de su personalidad, adquieren una mayor trascendencia.

Los efectos de la exposición a las pantallas a los dos años se relacionan con repercusiones a los cuatro años en dificultades para la comunicación y la socialización. A mayor tiempo de uso de los medios digitales menor competencia social e implicación de los padres en el uso de pantalla de sus hijos (Canadian Paediatric Society, 2023: 184-192).

Las repercusiones estudiadas a los tres años es que a mayor tiempo de pantalla más probabilidad de desarrollar problemas de conducta, retraso en los hitos del desarrollo psicomotor, dificultades para el aprendizaje y trastornos del lenguaje.

Los estudios relacionaron el tiempo que los padres pasan con sus dispositivos con la frecuencia de comportamientos para llamar la atención en sus hijos y un aumento en la dificultad de gestionar de una forma adecuada los conflictos en la familia.

El uso de un teléfono para premiar o distraer a niños de uno a cuatro años provoca que los niños exijan los dispositivos para calmarse y tengan rabietas si se les niega.

La multitarea relacionada con las pantallas se asocia con peores resultados cognitivos, disminución de la capacidad de filtrar las distracciones, aumento de la impulsividad y disminución de la memoria de trabajo. Los adolescentes que pasan demasiado tiempo frente a una pantalla tienen más probabilidades de presentar dificultades cognitivas graves (Song *et al.,* 2023).

En un estudio de seguimiento de la población durante dos años, detectaron en la resonancia magnética cerebral el impacto causal entre el uso de pantallas y la lectura en la adolescencia temprana. Tanto las puntuaciones en la interpretación de los mensajes

ISSN: 2952-6094 | e-ISSN: 2952-6116 | Núm. 13 | Enero de 2025
https://dx.doi.org/10.62269/cavcaa.XX | Consejo Audiovisual de Andalucía

verbales como la velocidad y la calidad de la lectura en voz alta se vieron afectadas significativamente por ver programas de TV o series (Li *et al.*, 2024).

La adolescencia es un período crítico para el desarrollo del córtex prefrontal y un período de máxima vulnerabilidad para la adquisición y el desarrollo de trastornos adictivos, psiquiátricos y comportamentales.

Ver películas en *streaming*, jugar a videojuegos, escuchar música, hablar por teléfono, enviar mensajes de texto, usar las redes sociales o chat antes de dormir, se asociaron con insomnio de conciliación y de mantenimiento. La falta de sueño por el uso de pantallas está relacionada con el estado de ánimo depresivo, los comportamientos externalizantes, la disminución de la autoestima, las dificultades en el afrontamiento y alteraciones en el desarrollo cerebral (Zhao *et al.*, 2024).

Las intervenciones que tienen como objetivo limitar el uso de pantallas demuestran un incremento significativo del ocio activo, reforzando el efecto de desplazamiento que produce el uso de pantallas de otro tipo de ocio más activo (Pedersen *et al.*, 2022).

En la infancia y en la adolescencia, al estar el ojo en desarrollo, se relaciona con miopía progresiva y estrabismo agudo por espasmo acomodativo. Este tipo de estrabismo cursa con visión borrosa y cefalea, que requiere atención urgente para descartar una causa neurológica (SAO, 2014).

La Agencia Española de Protección de Datos ha colaborado con la Asociación Española de Pediatría apoyando el Plan Familiar Digital que indica, desde la evidencia científica, cómo afecta el uso y el número de horas de pantallas a los NNA. La plataforma ofrece información útil sobre el uso adecuado de Internet por parte de los menores para familias y pediatras e incluye, además, un documento que las familias podrán personalizar y adaptar a sus circunstancias particulares con recomendaciones avaladas por la evidencia científica en función de la edad de sus hijos y otras generales para todos los miembros. Establece pautas sobre el número de máximo de horas de uso de pantallas por edades que incluye los tiempos de ocio y de aula. De cero a dos años se debe evitar su uso, de tres a cinco menos de una hora diaria y a partir de cinco años menos de dos horas de ocio digital al día (AEP, 2023).

Otro de los objetivos del plan es dotar a los pediatras de una herramienta sencilla que pueda usar en la consulta para informar y acompañar a las familias con el objetivo de prevenir los riesgos. Con este fin se ha desarrollado un apartado específico para profesionales, en el que se ofrecen detalles del plan, por qué es importante y cómo usarlo en la consulta.

4. Uso de medios digitales en el ámbito educativo

La UNESCO ha alertado también sobre que el tiempo que los niños pasan frente a la pantalla ha aumentado, tanto con fines educativos como por ocio. Este incremento de tiempo puede afectar negativamente al autocontrol y a la estabilidad emocional, y aumentar la ansiedad y la depresión (UNESCO, 2023).

En el informe *Perspectivas de la Educación Digital* de la OCDE se realiza un profuso análisis del impacto que el uso de medios digitales tiene en los NNA. En el mismo se recoge el impacto positivo que puede tener, y se considera que la tecnología digital,

incluida la inteligencia artificial (IA), podría mejorar la eficacia y la calidad de la educación personalizándola, ya sea mediante enseñanza y aprendizaje u otros servicios educativos, haciéndola más inclusiva y posiblemente equitativa, y mejorando la rentabilidad del sector. Sin embargo, también se afirma que la transformación digital de la educación conlleva riesgos que deben mitigarse (OECD, 2023).

Tal y como se recoge en el citado informe: «desarrollar una gobernanza de la digitalización para dar forma a una transformación digital eficaz y equitativa requiere centrarse tanto en cómo hacer posible la transformación digital como en cómo mitigar sus riesgos y desafíos. La innovación o la digitalización no son un fin en sí mismas. Tiene que ser un medio para alcanzar objetivos educativos específicos: personalización, inclusión de alumnos con discapacidad o necesidades diversidad social en la escuela, etc.».

Esto supone que desde todas las instancias hay que analizar el impacto real de la digitalización y poner el foco en proteger a los NNA, garantizando el cumplimiento de todos los derechos que les asisten.

Suecia se ha replanteado la digitalización en las aulas. En el año 2023, la ministra de Educación pidió a diferentes expertos que valoraran el Plan de Digitalización aprobado en 2022, con el objeto de estudiar el impacto que la enseñanza digital tiene en los alumnos, para poder establecer una evidencia científica de los posibles efectos que dicho proyecto pueda tener en la infancia sueca.

Se preguntó a cerca de sesenta organismos dedicados a la investigación en diferentes campos, uno de los cuales es el Instituto Karolinska, que llegó a la conclusión de que el cerebro en niños muestra que no se benefician de la enseñanza basada en pantallas.

En China, el Ministerio de Educación limitó el uso de dispositivos digitales como herramientas educativas a un 30 % del tiempo de enseñanza global.

En Estados Unidos, las plataformas educativas han demandado a las principales empresas de internet por los daños en la salud mental a la juventud. Estas consecuencias llevaron el año pasado a la Agencia Española de Protección de Datos a proponer a las administraciones educativas que se encuentran en su ámbito de competencia que valorasen la adopción escolar pues, según los estudios realizados en aquellas comunidades autónomas en las que se había restringido el uso de los dispositivos electrónicos en los centros escolares, se demostró que había disminuido significativamente el riesgo de ciberacoso y aumentado el rendimiento escolar.

Esta propuesta se ha seguido por comunidades autónomas como Madrid, Aragón, Cataluña, Valencia o Murcia, entre otras. En las etapas de Infantil y Primaria la restricción es prácticamente total, excepto en casos individuales por razones muy justificadas, de salud o razones personales o familiares debidamente acreditadas, y en Secundaria se incluye una amplia limitación, permitiéndose únicamente su uso para actividades didácticas.

El uso inadecuado o problemático y adictivo de Internet por los NNA tiene unos efectos perjudiciales que afectan gravemente a su desarrollo personal, además de en su salud física, mental, psicosocial y sexual, como ya se ha mencionado, en su neurodesarrollo, su aprendizaje, la adquisición de las medidas cognitivas, las relaciones familiares y sociales, los hábitos de consumo o la monetización de sus datos.

Además, la sobreexposición de información personal los hace más proclives a las situaciones de riesgo que el consumo intensivo de tecnología puede causar, como el

ISSN: 2952-6094 | e-ISSN: 2952-6116 | Núm. 13 | Enero de 2025
https://dx.doi.org/10.62269/cavcaa.XX | Consejo Audiovisual de Andalucía

ciberacoso, el *sexting* o el *grooming*, con consecuencias en algunos casos lamentablemente irreparables.

La relación actual entre educación y comunicación ha sido objeto de análisis, por cuanto «este entramado alienta la construcción de andamiajes y la mediación entre la información que el alumnado recibe, la presión de las relaciones en la sociedad y lo que puede darle la institución educativa». De ahí el hecho de que el docente se valore «desde una mirada educomunicativa, pasando de su criticado rol bancario hacia acciones y actitudes de un auténtico mediador y guía, considerándose a los actores de la educación en todo su potencial comunicativo» (Narváez Garzón y Castellanos Noda, 2018).

5. El impacto en la privacidad

El derecho fundamental a la protección de datos se constituye como una garantía de los derechos y libertades de las personas en lo que respecta al tratamiento que se realiza de sus datos personales, al asegurarles su control y disposición. Se trata de un derecho instrumental para la salvaguarda del conjunto de nuestros derechos y libertades, que se pueden ver afectados por el tratamiento de los datos: derecho a la salud, educación, a la no discriminación, daños y perjuicios físicos, psíquicos, materiales e inmateriales, influir en comportamientos y decisiones, usurpación de identidad, fraude, pérdidas financieras, reputación, confidencialidad, perjuicios económicos y sociales, comportamentales, etc.

La Agencia Española de Protección de Datos (AEPD) es la autoridad administrativa independiente, de carácter público, que vela por la observancia del derecho a la protección de datos y se configura como la garante de dicho derecho.

En el año 2019, la AEPD constituyó un grupo de trabajo, Menores, salud digital y privacidad, dedicado a analizar las situaciones que afectan a los derechos de los NNA en el ámbito digital, que aglutina a los diferentes actores implicados en su defensa y bienestar.

Resultado del trabajo desarrollado por ese grupo, se ha transmitido a la sociedad cuáles son las consecuencias que en diversos ámbitos: educativo, sanitario, del derecho de los consumidores y usuarios o del alcance de la responsabilidad penal, pueden derivar del uso de tecnologías digitales y cuál es la protección aplicable desde el punto de vista de la privacidad. La atención que la AEPD presta a la protección de los NNA en el ámbito digital ha llevado a diseñar una Estrategia global sobre menores, salud digital y privacidad, que recoge sus líneas de actuación prioritarias para fomentar la protección efectiva de la infancia y adolescencia en el uso que realizan de Internet y sus servicios (AEPD, 2024).

Las actuaciones desplegadas por la Agencia en los últimos años, cooperando con cada vez más actores públicos y privados, han puesto de manifiesto el reto pluridisciplinar que supone la protección de los NNA en un mundo tecnologizado. La Estrategia de la Agencia sobre menores, salud digital y privacidad contiene un total de diez actuaciones prioritarias y 35 medidas que se agrupan en tres grandes ejes: la colaboración regulatoria para la protección integral de los NNA en Internet, el refuerzo para garantizar sus derechos en un plano nacional e internacional y el ejercicio de las potestades de investigación y sanción contra las prácticas ilícitas y nocivas para la infancia y adolescencia.

Con el análisis de los diferentes datos se puede llegar a la conclusión de que se ha fomentado la monetización de los datos del menor, su inmersión prematura en el entorno digital como usuario y, por parte de la industria de Internet, la creación de patrones adictivos de satisfacción inmediata en los contenidos de Internet. En este sentido, la AEPD ha realizado un estudio en el que expone que, en muchos casos, los proveedores de servicios de Internet implementan patrones de diseño engañosos y adictivos en sus plataformas, aplicaciones y servicios. Ya el Comité Stigler concluyó en 2019 que el modelo de negocio de las principales plataformas en línea se basa en interfaces de usuario adictivas diseñadas para mantener la atención de dichos usuarios. Los beneficios que obtienen los proveedores dependen, en gran medida, de la cantidad de usuarios, la cantidad de tiempo que cada usuario pasa conectado y su grado de compromiso, y la cantidad de datos que un usuario comparte, directa o indirectamente. Investigaciones recientes acuñan el término «imperativo de atención a los datos» (Elettra, 2024, p. 66).

Los patrones engañosos se consideran interfaces y experiencias de usuario que llevan a los usuarios a tomar decisiones no intencionadas, involuntarias y potencialmente dañinas con respecto al tratamiento de sus datos personales y que se centran en los mismos aspectos: engaño, manipulación, influencia, toma de decisiones en contra de los propios intereses, daño o consecuencias negativas potenciales, falta de alternativas e información, etc. (EDPB, 2023; Cara, 2019).

Los patrones adictivos se pueden definir como «cualquier sistema de información que afecte proactivamente el comportamiento humano, en favor o en contra de los intereses de sus usuarios». Estos son características, atributos o prácticas de diseño que determinan una forma particular de utilizar las plataformas, aplicaciones y servicios digitales destinados a que los usuarios dediquen mucho más tiempo a su uso o con un mayor grado de compromiso del esperado, conveniente o saludable para ellos. El desarrollo de los patrones adictivos comienza con el concepto de tecnología persuasiva. El diseño persuasivo, cuando se aplica a las plataformas, aplicaciones y servicios, convierte a estos en adictivos (Kampik, 2018; Fogg, 1998; Chen *et al.*, 2023).

Patrones engañosos y adictivos tienen como propósito prolongar el tiempo que los usuarios permanecen en sus servicios, además de incrementar su nivel de compromiso, lo que conlleva que se aumente la cantidad de datos personales que se recogen sobre ellos. Ello es especialmente relevante por el impacto que estas estrategias adictivas tienen cuando se utilizan para tratar datos personales de personas vulnerables, como es el caso de la infancia y adolescencia, influyendo en las preferencias e intereses de los NNA, y afectando en última instancia a su autonomía y a su derecho al desarrollo.

Diferentes países y organismos internacionales han reconocido también el impacto de las prácticas adictivas. Por ejemplo, las Naciones Unidas han destacado la necesidad de abordar la adicción digital y proteger los derechos de la infancia en el entorno digital. Sin embargo, las regulaciones varían y son específicas según el país. Algunos han implementado directrices o leyes relacionadas con las características adictivas de la tecnología, mientras que otros todavía están explorando enfoques prácticos. Por ejemplo, la ley Stop Addictive Feeds Exploitation (SAFE) for Kids, aprobada por la Legislatura de Nueva York en junio de 2024, prohibirá que las plataformas de redes sociales ofrezcan contenido a usuarios menores de dieciocho años basándose en algoritmos de

ISSN: 2952-6094 | e-ISSN: 2952-6116 | Núm. 13 | Enero de 2025
https://dx.doi.org/10.62269/cavcaa.XX | Consejo Audiovisual de Andalucía

recomendación cuando se den unas circunstancias concretas. Estas plataformas tendrán que proporcionar *feeds* cronológicos inversos en esas circunstancias (ONU) (The New York State Senate, 2023-2024).

El Parlamento Europeo adoptó una resolución en diciembre de 2023, que aborda explícitamente el diseño adictivo de los servicios y la protección del consumidor en el mercado único de la UE. La resolución exigió prohibir prácticas adictivas como el desplazamiento (*scrolling*) infinito o la reproducción automática que fomentan la conexión prolongada, pasar de la economía de la atención al diseño ético, introducir un derecho digital a «no ser molestado» y empoderar a los usuarios para controlar sus experiencias en línea y garantizar que todas las plataformas, aplicaciones y servicios en línea sean seguros para la infancia, así como la introducción de nueva legislación para la protección de los consumidores dirigida específicamente a las prácticas adictivas (European Parliament, 2023).

Los usuarios con diferentes antecedentes mentales, sociales, tecnológicos y de comportamiento pueden reaccionar de manera diferente ante una misma característica de diseño. El adaptarse a las distintas circunstancias personales de cada usuario concreto, conocidas a través de la recogida masiva de datos, incentiva a los proveedores de plataformas, aplicaciones y servicios a diseñar sus productos de manera que funcionen bien en términos de beneficios y métricas relevantes para su modelo de negocio. Según estas métricas, y dada la presión actual del mercado, pueden obtener mejores resultados al emplear patrones adictivos (Sindermann *et al.*, 2022; Narayanan *et al.*, 2022).

Los tratamientos de datos personales de los usuarios que tienen lugar a partir de estos patrones incluyen operaciones específicas, todas ellas engañosas, de manera que se influya en sus decisiones y que se utilicen sus datos personales con este fin o para generar nuevos datos y realizar perfilado. En función de cómo se adaptan dichos patrones, se pueden establecer tres niveles en los que pueden clasificarse los patrones adictivos: de alto, medio y bajo. Dicha clasificación se puede realizar a partir de patrones identificados y analizados en investigaciones previas centrándose en su tendencia adictiva dada la evidencia disponible (analizada realizando una revisión sistemática siguiendo el método PRISMA-ScR) (AEPD, 2024).

En ese sentido, los denominados patrones de alto nivel son estrategias generales independientes del contexto y de la aplicación, y se han identificado cuatro: acción forzada, ingeniería social, interferencia en la interfaz y persistencia. Los patrones de nivel medio describen enfoques más específicos que explotan las debilidades o vulnerabilidades psicológicas de los usuarios. Finalmente, los patrones de bajo nivel corresponden a la ejecución específica de los diferentes enfoques y, a menudo, son específicos del contexto o de la aplicación.

La incorporación de patrones adictivos a los tratamientos de datos personales tiene importantes implicaciones para la protección de datos de los usuarios, como la responsabilidad proactiva, la aplicación efectiva de las obligaciones de protección de datos desde el diseño y por defecto, la transparencia, la licitud, la lealtad, la limitación de la finalidad, la minimización de datos o el tratamiento de categorías especiales de datos. Asimismo, implica un riesgo para los derechos y libertades de todos los usuarios y, en particular, para el derecho a la integridad física y psíquica de la infancia y adolescencia.

La toma de decisiones automatizada también debería evaluarse cuidadosamente en este contexto por las prohibiciones normativas y por el impacto que puedan tener en el menor, la escala a la que se aplican los patrones adictivos obliga a los proveedores a automatizarlos, que, además de impactos a la integridad física y mental, por su naturaleza automática presentan riesgos adicionales de discriminación, exclusión, manipulación, socave de la autonomía individual, influencia en su proceso de pensamiento, sus emociones, su comportamiento, limitar su libertad de información y expresión, generar autocensura y afectar a la autonomía y desarrollo de los menores (EDPB, 2021).

En este sentido, la AEPD va a promover que el Comité Europeo de Protección de Datos incluya los patrones adictivos en las directrices que se están preparando sobre la interrelación entre el Reglamento General de Protección de Datos y la DSA, debido al elevado impacto que estas prácticas poseen sobre el derecho a la protección de datos en los entornos digitales.

6. El acceso de menores a contenidos inadecuados

Como se ha comentado, en cuanto al acceso *online* por los menores a contenidos para adultos, en especial a la pornografía, estudios e informes de organizaciones especializadas señalan que se viene produciendo a edades muy tempranas y a gran escala, en un momento en el que su desarrollo cognitivo no les permite entender lo que están viendo, pues su personalidad no está formada, generando importantes desórdenes en la concepción de las relaciones sexuales y del rol de la mujer.

Los resultados del *Estudio sobre pornografía en las Islas Baleares: acceso e impacto sobre la adolescencia, derecho internacional y nacional aplicable y soluciones tecnológicas de control y bloqueo* son preocupantes. Así, el estudio destaca que más del 90 % de los jóvenes reconoce que en los últimos años ha mirado pornografía (91,7 % hombres y 89,3 % mujeres). Además, un 93,3 % ha tenido los primeros contactos con la pornografía antes de los catorce años. En cuanto a la edad de inicio de la visualización habitual de pornografía, la edad mediana en chicos son 12,7 años y 12,98 en chicas. Sobre el tipo de pornografía que miran habitualmente, un 76,25 % de la muestra responde que ve sobre todo pornografía *hardcore* o cruda (Milano *et al.*, 2023).

Según datos del *Barómetro del Centro de Investigaciones Sociológicas* (CIS) de febrero de 2024, un 93,9 % de los encuestados está a favor de «restringir o prohibir» el acceso de las personas menores de edad a páginas web pornográficas. A este respecto, la verificación de la edad para acceder a esos contenidos es uno de los elementos clave para proporcionar un entorno seguro y saludable de Internet a los menores, para lo que son necesarios sistemas que lo realicen de manera eficaz y plenamente respetuosos con los derechos y libertades de las personas, en particular con la protección de sus datos personales y su privacidad (CIS, 2024).

Los sistemas de verificación de edad que se emplean actualmente en Internet (autodeclaración, compartir credenciales con el proveedor de contenidos, que sea este el que estime la edad o que exista una entidad intermediaria entre el usuario y el proveedor)

ISSN: 2952-6094 | e-ISSN: 2952-6116 | Núm. 13 | Enero de 2025
https://dx.doi.org/10.62269/cavcaa.XX | Consejo Audiovisual de Andalucía

han demostrado riesgos claros para los derechos de las personas y en particular a los NNA: localización de menores de edad a través de Internet, falta de certidumbre sobre la edad declarada, exposición de la identidad a múltiples intervinientes en la Red, perfilado masivo, o recopilación y tratamiento de datos no necesarios, entre otros. Estos perfiles se pueden utilizar para publicidad dirigida, análisis de comportamiento o prácticas discriminatorias (EDRi, 2023).

Los esfuerzos de investigación se han centrado en explorar formas de superar algunos de estos desafíos. Sin embargo, la mayoría de los trabajos se centran en discutir si es el enfoque más adecuado en diferentes casos de uso o en aspectos éticos y de política pública (Bertrand *et al.*, 2024; Egan *et al.*, 2023; Brennen y Perault, 2023; CNIL, 2022; Jarvie, 2021; Pasquale *et al.*, 2020; Yar, 2020; Nash *et al.*, 2012).

Además, el British Standards Institute (BSI) y la Digital Policy Alliance desarrollaron un código de prácticas para los proveedores de servicios de verificación de edad en línea, llamado PAS 1296:2018 [10], que aplica a los proveedores que deben realizar procesos de aseguramiento de la edad para determinar si un ciudadano puede o no acceder a bienes, contenidos o servicios con restricción de edad. La Organización Internacional de Normalización (ISO) está trabajando actualmente en el desarrollo de la norma ISO/IEC 27566. Uno de los principales impulsores de este esfuerzo es el creciente acuerdo de que un método sencillo para explicar los niveles de confianza alcanzados por los diferentes componentes de aseguramiento beneficiaría a los proveedores de servicios, las partes que confían en él y los reguladores (ISO, 2023; BSI, 2018).

Entre las iniciativas europeas se puede señalar el Proyecto euCONSENT. Este trabaja sobre la propuesta de ampliaciones de la operación de la infraestructura eIDAS (electronic IDentification, Authentication and trust Services) para ofrecer una verificación de la edad interoperable paneuropea, de sistema abierto, segura y certificada y el consentimiento de los padres para acceder a los servicios de la sociedad de la información. El segundo es el Grupo de Trabajo sobre Verificación de la Edad en virtud de la Ley de Servicios Digitales, creado en 2024 para avanzar hacia un enfoque armonizado de la UE para la verificación de la edad.

En este marco, la AEPD presentó en diciembre de 2023 una propuesta de sistema de verificación de edad y protección de las personas menores de edad en Internet ante el acceso a contenidos para adultos (AEPD, 2023).

El objetivo es proteger al menor del acceso a contenidos para adultos y que estos contenidos, a su vez, puedan ser accesibles para aquellas personas que puedan demostrar su edad sin necesidad de hacer visible su identidad. No se trata de que los proveedores de contenidos o terceros conozcan que la persona que está accediendo es menor (lo que supondría una exposición o señalamiento de un usuario como menor y se multiplicarían los riesgos), sino que tengan la garantía de que la persona que accede a los contenidos para adultos puede hacerlo, demostrando su condición de «persona autorizada a acceder» (AEPD, 2023).

En la propuesta se identifica un aspecto de capital importancia: la verificación de la edad de la persona usuaria es solo el primer paso en un sistema cuyo objetivo sea proteger a personas menores de edad ante contenidos inadecuados. Este sistema estará formado básicamente por los siguientes elementos:

- Por un mecanismo de verificación de edad, que proporcionará una información cierta sobre la autorización de acceso a contenidos orientados a personas adultas.
- Unas políticas de calificación de sitios y contenidos por razones de edad, que permitirán tener un criterio de qué sitios en Internet, o qué contenidos en sitios generalistas, son considerados contenidos orientados a personas adultas o tienen establecidos unos requisitos de limitación de acceso por edad.
- Una calificación de los sitios, o de los contenidos, en función y aplicación de las políticas previamente establecidas. Esta calificación supone la aplicación de las políticas anteriores.
- Una ejecución de las políticas de acceso en función de las políticas establecidas, la calificación de los contenidos y de la autorización de acceso de la persona usuaria, que realizará el filtrado de los contenidos. Esta ejecución debe implicar no solo a las entidades responsables de los sitios web y de las redes sociales, sino también a los buscadores en Internet, las empresas de telefonía móvil y los fabricantes de videojuegos o dispositivos, entre otros.

Para comprender cómo la verificación de edad puede ayudar a proteger a los menores en línea primero es necesario comprender de qué hay que protegerlos exactamente. En esta nota se emplea la clasificación de la OCDE, de manera que se tienen en cuenta cinco categorías de riesgos, las denominadas cinco Cs (OECD, 2021):

1) Contenido: el contenido de odio (por raza, género, religión, orientación sexual, etc.), el dañino (pornografía, violencia extrema, consumo de sustancias, extremismo, desórdenes alimenticios, etc.), el ilegal (abuso sexual, terrorismo, etc.) y la desinformación pueden provocar impactos en la salud mental y en desarrollo afectivo de los menores.
2) Conducta: de nuevo se observan los cuatro tipos de riesgos ya mencionados, pero en este caso se refieren al comportamiento del propio menor cuando utiliza Internet, que puede colocarle en una posición vulnerable por participar en conductas de odio (ciberacoso, etc.), dañinas (*sexting*, etc.), ilegales o participar en la distribución de desinformación.
3) Contacto: se producen riesgos en categorías similares, pero en este caso los NNA son contactados por alguien que interactúa con ellos gracias a Internet y les hace objeto de mensajes de odio, dañinos, ilegales o problemáticos por otros motivos. Algunos ejemplos claros son la sextorsión, el *grooming*, o las situaciones en las que los NNA proporcionan datos suficientes para pasar del contacto en el entorno real al contacto en el entorno físico, con riesgo para su derecho a la integridad. La diferencia con los riesgos de conducta es que en este caso el NNA es objeto o víctima directa en lugar de actor o parte activa.
4) Consumo (contrato o consentimiento): se producen cuando el NNA es un cliente o consumidor, principalmente porque recibe publicidad de productos que no son adecuados (como tabaco, alcohol o servicios de citas), porque recibe publicidad que no puede identificar como tal (por ejemplo, por *product placement* o a través de un *influencer*), porque se aprovecha su credulidad, inexperiencia o falta de madurez

ISSN: 2952-6094 | e-ISSN: 2952-6116 | Núm. 13 | Enero de 2025
https://dx.doi.org/10.62269/cavcaa.XX | Consejo Audiovisual de Andalucía

para que consienta con acuerdos o contratos que no son beneficiosos para él o ella (por ejemplo, empleando patrones engañosos) o porque, directamente, no le corresponde al NNA tomar las decisiones sobre consumo, contrato o consentimiento (UNESCO, 2024).

5) Corte transversal: en esta categoría entran riesgos bastante heterogéneos que no se pueden clasificar en las categorías anteriores, principalmente:
   a) Riesgos para la privacidad: como la sobreexposición provocada por ellos mismos, el *sharenting*, los tratamientos asociados a las tecnologías y plataformas educativas, etc.
   b) Riesgos asociados a las nuevas tecnologías: como los asociados al uso de inteligencia artificial (por ejemplo, herramientas que producen fotografías falsas de desnudos que se ofrecen en chats de videojuegos), internet de las cosas (por ejemplo, relojes inteligentes infantiles que permiten la geolocalización), al tratamiento de neurodatos (por ejemplo, para jugar a videojuegos o monitorizar la atención en clase) o la autenticación biométrica (por ejemplo, para pagar en los comedores de los colegios o para acceder a un evento deportivo).
   c) Riesgos asociados a la salud mental y física: como los asociados a los patrones adictivos empleados por algunos servicios y aplicaciones o al tiempo excesivo de pantalla.

Una vez comprendidos los riesgos principales que sufre la infancia en Internet, se puede establecer cuál es el papel que juega la verificación de edad en la protección del menor:

- Las soluciones de verificación de edad, con el modelo adecuado, pueden ser de gran ayuda para evitar o mitigar gran parte de estos riesgos desde el diseño y por defecto.
- La selección del modelo adecuado para la verificación de edad, así como su diseño e implementación, deberían partir de una evaluación de impacto para los derechos de la infancia (Child Rights Impact Assessment [CRIA]). La gestión de los riesgos para la infancia en Internet no debe realizarse a ciegas ni de una manera rígida o estándar, sino tras una evaluación sistemática y específica las cinco categorías de riesgos ya mencionadas en el caso de una aplicación o servicio concreta, tanto por su funcionalidad como por su público objetivo, contexto de uso, etc.
- La verificación de edad puede emplear, para gestionar todos estos riesgos, el enfoque habilitador que comprueba que el usuario supera el umbral de edad requerido para realizar cambios en la configuración, permitir acceso a la comunicación con terceros, instalar aplicaciones para adultos, etc.
- Esto permite gestionar los riesgos de manera proactiva, y devolver a familiares y tutores la capacidad de ejercer su deber de cuidado y el resto de sus obligaciones.
- La verificación de edad no necesita verificar una edad concreta ni una fecha de nacimiento, solo la superación de dicho umbral. Umbral que puede ser distinto en función del tipo de actividad o elemento al que se desea acceder en Internet.
- La verificación de edad resulta inútil si todo el ecosistema (aplicaciones, herramientas, interfaces, etc.) no se adapta para la protección del menor por

defecto y para comprobar que los usuarios que realizan ciertas solicitudes tienen la edad requerida para ello de forma que se garantice el anonimato, la no trazabilidad y que no se detecta a NNA.

En cuanto a los procedimientos llevados a cabo por la AEPD para la protección de los NNA en su acceso a contenidos para adultos hay que destacar los siguientes procedimientos sancionadores contra empresas titulares de páginas de pornografía por la falta de exactitud en la verificación de la edad y de privacidad desde el diseño (AEPD, 2023 y 2021).

En el caso de la titularidad de empresas de webs dedicadas a la pornografía que han sido sancionadas por ello existía un riesgo cierto de que los NNA accedieran directamente y sin limitaciones a un contenido perjudicial para ellos. Las limitaciones o cautelas previstas en las páginas web resultaban claramente insuficientes para evitar el acceso a los NNA, tanto de forma directa a la página web (usuarios no registrados), como en aquellos supuestos en los que era preciso un registro. Si bien había presentes mecanismos para declarar la edad, no existía ninguno para comprobarla ulteriormente, ni ninguno para verificarla.

Los riesgos a los que están afectos los NNA, inherentes a su desarrollo, han de ser considerados por los responsables del tratamiento, y no solo por aquellos que dirigen servicios directa y específicamente a los niños, sino por todos aquellos que realizan tratamientos de datos personales dirigidos a otros colectivos en los que los NNA puedan interactuar o intervenir, como sucede con la pornografía en Internet.

Resultando que estas entidades deciden que las categorías de interesados se limitan a los mayores de edad, les corresponde implementar las medidas técnicas y organizativas apropiadas para que el tratamiento se efectúe únicamente respecto de interesados mayores de edad. Ello conlleva que también implemente las medidas técnicas y organizativas apropiadas para que los datos de los NNA no sean tratados.

Además de la legislación sobre protección de datos, otras regulaciones establecen disposiciones para proteger a los menores en el acceso a contenidos *online*. El Reglamento de Servicios Digitales recoge que los prestadores de servicios y motores de búsqueda deben tener en cuenta el interés superior de los menores a la hora de adoptar medidas, como adaptar el diseño de su servicio, en especial cuando se dirijan principalmente a menores o sean utilizados predominantemente por ellos, y adoptar medidas para protegerlos de contenidos que puedan perjudicar su desarrollo físico, mental o moral.

Por su parte, la Ley General de Comunicación Audiovisual obliga a las plataformas de intercambio de vídeos a establecer sistemas de verificación de edad con respecto a contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores y que, en todo caso, impidan el acceso de estos a los contenidos audiovisuales más nocivos, como la violencia gratuita o la pornografía.

7. Contenidos sensibles y prioritarios

Los NNA son capaces de aprender de forma intuitiva cómo funcionan las herramientas digitales, pero falta mucho por hacer para enseñarles a ser conscientes de la magnitud de los riesgos, las consecuencias que puede tener, por ejemplo, el envío de fotos o vídeos

ISSN: 2952-6094 | e-ISSN: 2952-6116 | Núm. 13 | Enero de 2025
https://dx.doi.org/10.62269/cavcaa.XX | Consejo Audiovisual de Andalucía

sexuales o cómo puede afectar al desarrollo de la personalidad el acceso a contenidos que no pueden gestionar por sí mismos.

El Canal Prioritario de la Agencia es una iniciativa pionera a nivel mundial que permite solicitar la retirada urgente de contenidos publicados que pongan en grave riesgo los derechos y libertades o la salud física o mental de los afectados. Ello incluye, entre otros, los contenidos sexuales o violentos publicados en páginas web sin el permiso de las personas que aparecen en ellos, en particular, en casos de acoso a menores o violencia sexual contra las mujeres, pero también en situaciones de violencia digital de todo tipo.

Las nuevas tecnologías han propiciado nuevas amenazas, en parte causadas por la velocidad de difusión de información e imágenes, la facilidad de acceso a las mismas a través de los motores de búsqueda y las dificultades para eliminarlas de Internet. La violencia ha pasado de ser física o psicológica a incluir el ciberacoso y la vulneración de la privacidad de las víctimas con acciones como la grabación y distribución de imágenes con contenido sensible en las redes sociales. Aunque todo ciudadano puede ser una víctima, los NNA son el principal blanco de estas conductas. Esta violencia digital puede tomar formas muy distintas: acoso en redes sociales; amenazas, sextorsión y ataques a la reputación a través del correo electrónico, las redes o cualquier medio digital; suplantación de la identidad; seguimiento de los distintos dispositivos digitales mediante programas espías, etc.

El Canal Prioritario de la AEPD para comunicar la difusión ilícita de contenido sensible y solicitar su retirada pretende ofrecer una respuesta rápida en situaciones excepcionalmente delicadas. Establece una vía en la que las reclamaciones recibidas son analizadas de forma prioritaria, permitiendo que la Agencia, como autoridad independiente, pueda adoptar medidas urgentes para evitar que esos contenidos continúen publicados *online*.

Si los afectados por las imágenes son menores de edad, pero tienen más de catorce años, podrán acudir directamente al canal prioritario por una vía especialmente habilitada para ello. Si las imágenes afectan a menores de catorce años serán los padres, madres o tutores quienes deban presentar la solicitud de retirada.

La AEPD ha ordenado la retirada de contenidos a diferentes páginas web en más de una treintena de casos en 2023, que se suman a las 51 intervenciones de urgencia que se realizaron en 2022. Entre esas órdenes de retirada se encuentran la difusión de vídeos o fotografías de contenido sexual grabadas con consentimiento, pero publicadas sin permiso, la grabación de agresiones y humillaciones y la publicación de perfiles falsos de mujeres en páginas web pornográficas utilizando su imagen real y su número de teléfono. El porcentaje de efectividad del Canal Prioritario para retirar los contenidos ha alcanzado el 100 % de efectividad en 2023 y, en general, la retirada se produce en un plazo de 72 horas, cuando el responsable de la plataforma se encuentra en España.

En tales casos, se requiere a los proveedores de servicios correspondientes la retirada de los contenidos sensibles con la mayor inmediatez posible. La retirada de estos contenidos supone una gran ayuda para las personas afectadas y es uno de los principios en los que se basa la responsabilidad social de la Agencia. Pero con independencia de la retirada urgente de los contenidos sensibles, la Agencia puede determinar que procede depurar responsabilidades a través de un procedimiento sancionador.

Nos encontramos en una situación que requiere trabajar y rápido si se quiere ayudar a las generaciones de jóvenes actuales y venideras y proporcionarles un marco de protección para navegar por la Red, que ha de involucrar a todos los sectores y agentes implicados.

Contribución autoría

— Estructura del trabajo, metodología, edición, revisión del manuscrito, análisis, coordinación, supervisión: Mar España Martí y María Angustias Salmerón Ruiz.

Financiación

La presente investigación no ha recibido ayudas específicas provenientes de agencias del sector público, sector comercial o entidades sin ánimo de lucro.

8. Referencias

Agencia Española de Protección de Datos (AEPD) (2019). *Canal Prioritario.* Disponible en: https://acortar.link/gMvoZ9

Agencia Española de Protección de Datos (AEPD) (2021). PS/00554/2021. Disponible en: https://acortar.link/6kQSab

Agencia Española de Protección de Datos (AEPD) (2021). PS/00555/2021. Disponible en: https://acortar.link/KtpmYc

Agencia Española de Protección de Datos (AEPD) (2023). *Decálogo de principios que debe cumplir un sistema de verificación de edad*. Disponible en: https://acortar.link/WXxanW

Agencia Española de Protección de Datos (AEPD) (2023). *Nota técnica. Descripción de las pruebas de concepto sobre sistemas de verificación de edad y protección de personas menores ante contenidos inadecuados*. Disponible en: https://acortar.link/LEsKAw

Agencia Española de Protección de Datos (AEPD) (2023). Verificación de edad y protección de menores ante contenidos inadecuados. *YouTube vídeo*. Disponible en: https://acortar.link/Yu8Upq

Agencia Española de Protección de Datos (AEPD) (2023). *Gráfico Riesgos de sistemas de verificación de edad*. Disponible en: https://acortar.link/ohqvdV

Agencia Española de Protección de Datos (AEPD) (2023). PS/00308/2023. Disponible en: https://acortar.link/qpP6IL

Agencia Española de Protección de Datos (AEPD) (2024). *Estrategia global sobre menores, salud digital y privacidad.* Disponible en: https://acortar.link/PMMRYQ

Agencia Española de Protección de Datos (AEPD) (2024). *Informe sobre las implicaciones de los patrones adictivos en el tratamiento de datos personales*. Disponible en: https://acortar.link/l1DLzI

Asociación Española de Pediatría (AEP) (2023). *Plan Digital Familiar.* Disponible en: https://acortar.link/VMKKKJ

Bertrand, A. *et al.* (2024). Easy access: identification verification and shipping methods used by online vape shops. *Tobacco Control.*

Bietti, E. (2024). The Data-Attention Imperative. *Northeastern University School of Law Research Paper*, 473, p. 66.

Brennen, S. y Perault, M. (2023). *Keeping kids safe online: how should policymakers approach age verification?* The Center for Growth and Opportunity.

ISSN: 2952-6094 | e-ISSN: 2952-6116 | Núm. 13 | Enero de 2025
https://dx.doi.org/10.62269/cavcaa.XX | Consejo Audiovisual de Andalucía

British Standards Institute(BSI) (2018). *PAS 1296:2018. Online age checking. Provision and use of online age check services. Code of Practice*. Disponible en: https://acortar.link/daByG8

Canadian Paediatric Society (2023). Screen time and preschool children: Promoting health and development in a digital world. *Paediatr Child Health*, 28, pp. 184-192. Disponible en: http://dx.doi.org/10.1093/pch/pxac125

Cara C. (2019). Dark patterns in the media: A systematic review. *Network Intelligence Studies*, 7(14), pp. 105-113.

Centro de Investigaciones Sociológicas (CIS) (2024). *Barómetro de febrero de 2024.* Disponible en: https://acortar.link/i4i9Lp

Chen, X., *et al.* (2023). Do persuasive designs make smartphones more addictive? A mixed-methods study on Chinese university students. *Computers in Human Behavior Reports*, 10, 00299.

Comisión Nacional de Informática y de las Libertades (CNIL) (2022). *Online age verification: balancing privacy and the protection of minors.* Disponible en: https://acortar.link/WqkToO

Egan, K.L., Villani, S. y Soule, E.K. (2023). Absence of age verification for online purchases of cannabidiol and delta-8: implications for youth access*. J. Adolesc. Health* 73(1), pp. 195-197.

Elettra B. (2024). The Data-Attention Imperative. *Northeastern University School of Law Research Paper*, 473, pp. 66.

European Digital Rights (EDRi) (2023). *Online age verification and children's rights.* Disponible en: https://acortar.link/sK0TPi

European Data Protection Board (EDPB) (2023). *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them.* Version 2.0. Adopted on 14 February 2023. Disponible en: https://acortar.link/TIAB4F

European Data Protection Board (EDPB) (2021). Directrices 8/2020 sobre la focalización de los usuarios de medios sociales Versión 2.0 Adoptadas el 13 de abril de 2021, párrafos 9-18. Disponible en: https://acortar.link/v9RTO7

European Parliament (2023). Resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI). Disponible en: https://acortar.link/r8yVEY

Fiscalía General del Estado (FGE) (2022). *Memoria 2022.* Disponible en: https://acortar.link/r4j2Zx

Fogg, B. J. (1998). Persuasive computers: perspectives and research directions. En: *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 225-232.

Fundación ANAR. (2023). Estudio longitudinal sobre la Evolución de la Violencia contra las Mujeres en la Infancia y Adolescencia en España (2018-2022). Disponible en: https://acortar.link/XPzfMm

Instituto Nacional de Estadística (INE) (2023). *Equipamiento y uso de TIC en los hogares, 2023.* Disponible en: https://acortar.link/MPvXtU

Jarvie, C. y Renaud, K. (2021). Are you over 18? A snapshot of current age verification mechanisms. En: *Dewald Roode Workshop*.

Kampik, T., Nieves, J. C. y Lindgren, H. (2018). Coercion and deception in persuasive technologies. En: *Proceedings of the 20th International Trust Workshop (co-located with AAMAS/IJCAI/ECAI/ICML 2018),* pp. 38-49.

Li M. *et al.* (2024). Causal Relationships Between Screen Use, Reading, and Brain Development in Early Adolescents. *JAMA Pediatr*, 11:2307540. Disponible en: https://acortar.link/hsUJ6Z

Milano, Valentina y Brage *et al.* (2023). *Estudio sobre pornografía en las Illes Balears: acceso e impacto sobre la adolescencia, derecho internacional y nacional aplicable y soluciones tecnológicas de control y bloqueo.* Disponible en: https://acortar.link/DD5wd4

Narayanan, A. *et al*. (2020). Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces. *Queue*, 18(2), pp. 67-92.

Narváez Garzón, A. M. & Castellanos Noda, A. V. (2018). Educomunicación hoy: un reto necesario. *Revista de Ciencias Humanísticas y Sociales (ReHuSo)*, 3(2), pp. 25-34. Disponible en: https://doi.org/10.33936/rehuso.v3i2.1372

Nash, V. *et al.* (2012). Effective age verification techniques: lessons to be learnt from the online gambling industry. Disponible en: SSRN 2658038.

Organización de Naciones Unidas (ONU) (s.f.). *Child and Youth Safety Online*. Disponible en: https://acortar.link/c1WJjl

Organización Internacional de Normalización (ISO) (2023). Framework. *ISO/IECWD 27566-1 Information security, cybersecurity and privacy protection–Age assurance systems..* Disponible en: https://www.iso.org/standard/88143.html

Organización para la Cooperación y el Desarrollo Económico (OECD) (2021). Children in the digital environment: revised typology of risks, 302. *OEDC Digital Economy Papers*. Disponible en: https://acortar.link/SqEjv0

Organización para la Cooperación y el Desarrollo Económico (OCDE) (2023). Towards an Effective Digital Education Ecosystem. *Digital Education Outlook.* Disponible en: https://doi.org/10.1787/c74f03de-en

Pasquale, L. *et al.* (2020). Digital age of consent and age verification: can they protect children? *IEEE Softw.* 39(3), pp. 50-57.

Pedersen J. *et al.* (2022). Effects of Limiting Recreational Screen Media Use on Physical Activity and Sleep in Families With Children: A Cluster Randomized Clinical Trial. *JAMA Pediatr*. 176:741-9. Disponible en: https://acortar.link/09sfBH

Save the Children (2020). *(Des)información sexual: pornografía y adolescencia. Un análisis sobre el consumo de pornografía en adolescentes y su impacto en el desarrollo y las relaciones con iguales.* Disponible en: https://acortar.link/HffcU7

Sindermann, C., Montag, C. y Elhai, J. D. (2022). The Design of Social Media Platforms—Initial Evidence on Relations Between Personality, Fear of Missing Out, Design Element-Driven Increased Social Media Use, and Problematic Social Media Use.

Sociedad andaluza de oftalmología (SAO) (2024). Comunicado sobre los riesgos del uso de plataformas digitales. Disponible en: https://acortar.link/ZaH4Nt

Song K. *et al.* (2023). Youth Screen Media Activity Patterns and Associations with Behavioral Developmental Measures and Resting-state Brain Functional Connectivity. *J Am Acad Child Adolesc Psychiatry*, 62, pp. 1051-1063. Disponible en: https://acortar.link/P5KVsx

The New York State Senate (2023-2024). Senate Bill S7694A, 2023-2024 Legislative Session, Establishes the Stop Addictive Feeds Exploitation (SAFE) for Kids act prohibiting the provision of addictive feeds to minors. Disponible en: https://acortar.link/PL9ZqR

UNESCO (2024). *Child rights impact assessments in relation to the digital environment: developing global guidance*. Disponible en: https://acortar.link/HiQj51

UNESCO (2023). *Informe de seguimiento de la educación en el mundo, 2023: tecnología en la educación: ¿una herramienta en los términos de quién?* Disponible en: https://doi.org/10.54676/NEDS2300

UNICEF (2021). *Estudio sobre el impacto de la tecnología en la adolescencia. Un estudio comprensivo e inclusivo hacia el uso saludable de las TRIC*. Disponible en: https://acortar.link/feLgSV

Yar, M. (2020). Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK. *Policing: Int. J.* 43(1), pp. 183-197.

Zhao Y. *et al.* (2024). Screen time, sleep, brain structural neurobiology, and sequential associations with child and adolescent psychopathology: Insights from the ABCD study. *J Behav Addict*, 13: 542. Disponible en: https://acortar.link/uVBDYt

ISSN: 2952-6094 | e-ISSN: 2952-6116 | Núm. 13 | Enero de 2025
https://dx.doi.org/10.62269/cavcaa.XX | Consejo Audiovisual de Andalucía