Universitat Autònoma de Barcelona

TRABAJO DE FIN DE GRADO

PROTECCIÓN DE DATOS EN LA INFANCIA Y ADOLESCENCIA:

Análisis de riesgos en la era de la inteligencia artificial.

Autora: Kawthar Dayani Aanane

Tutor: Josep Cañabate Pérez

Grado en Derecho

Facultad de Derecho

Fecha de entrega: 11/05/2025

"Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales."

Considerando n.º 38 del Reglamento General de Protección de Datos

Kawthar Dayani Aanane
TFG 2024-2025
4º Derecho UAB

Resumen

El presente Trabajo de Fin de Grado consiste en una investigación jurídica sobre la protección de los datos de personas menores de edad. El análisis parte de la hipótesis de que la aplicación conjunta del RGPD, el Reglamento eIDAS2 y el Reglamento de Inteligencia Artificial puede ofrecer un marco potente y eficaz para proteger los derechos de los niños, niñas y adolescentes frente a los riesgos tecnológicos actuales.

La primera parte del trabajo examina el contenido y los objetivos de los tres reglamentos. La segunda parte desarrolla un análisis de riesgos aplicado a dos casos actuales: el uso de la red social Instagram y el acceso a páginas web de contenido pornográfico. En cada uno se identifican los bienes jurídicos protegidos, riesgos, vulnerabilidades, impacto y probabilidad. Finalmente, se presenta una matriz de riesgos que permite visualizar los riesgos encontrados.

Este enfoque ofrece una visión clara sobre la eficacia y las limitaciones de la regulación europea en la protección de las y los menores en el ámbito digital.

Palabras clave: protección de datos, Instagram, personas menores, eIDAS2, RGPD, pornografía, análisis de riesgos.

Abstract

This bachelor's Thesis is a legal research project focused on the protection of minors' personal data. The analysis is based on the hypothesis that the combined application of the GDPR, the eIDAS2 Regulation, and the Artificial Intelligence Act can provide an effective framework to protect the rights of children and adolescents against today's digital risks.

The first part of the paper examines the content and objectives of the three regulations. The second part presents a risk analysis applied to two real and current cases: the use of the social media platform Instagram and minors' access to pornographic websites. Each one identifies the protected legal interests, risks, vulnerabilities, impact, and probability. Finally, a risk matrix is provided to help illustrate and better understand the risks identified.

This approach provides a clear insight into the strengths and limitations of European regulation when it comes to protecting minors in the digital environment.

Keywords: data protection, Instagram, children, eIDAS2, GDPR, pornography, risk analysis.

Kawthar Dayani Aanane
TFG 2024-2025
4º Derecho UAB

ÍNDICE

INTRODUCCIÓN **2**

1. LA PRIVACIDAD DE LAS PERSONAS MENORES DE EDAD EN EL ENTORNO DIGITAL: REGULACIÓN Y PROTECCIÓN JURÍDICA **4**

1.1. El derecho a la protección de datos como derecho fundamental 4

1.2. El Reglamento General de Protección de Datos 5

1.2.1. Conceptos generales y fundamentos del RGPD *7*

1.3. El eIDAS2: la versión mejorada del Reglamento 910/2014 9

1.4. Relación del RGPD y el eIDAS2 10

1.5. Breve introducción al Reglamento de Inteligencia Artificial y la protección que ofrece a las personas menores 11

2. ANÁLISIS PRÁCTICO DE RIESGOS Y AMENAZAS EN EL ENTORNO DIGITAL **12**

2.1. CASO 1. Protección de cuentas de adolescentes en Instagram 12

2.1.1. Descripción del caso *12*

2.1.2. Identificación del bien jurídico: privacidad y seguridad *13*

2.1.3. Descripción del riesgo o amenaza *14*

2.1.4. Análisis de vulnerabilidades *16*

2.1.5. Evaluación de la probabilidad *17*

2.1.6. Impacto del riesgo *20*

2.1.7. Matriz de riesgos *21*

2.2. CASO 2. Acceso de menores a páginas para adultos 22

2.2.1. Descripción del caso *22*

2.2.2. Identificación del bien jurídico: derecho al desarrollo de la personalidad y libertad sexual *23*

2.2.3. Descripción del riesgo o amenaza *24*

2.2.4. Análisis de vulnerabilidades *25*

2.2.5. Evaluación de la probabilidad *28*

2.2.6. Impacto del riesgo *29*

2.2.7. Matriz de riesgos *30*

3. CONCLUSIONES **32**

4. REFERENCIAS BIBLIOGRÁFICAS **34**

ABREVIATURAS

AEPD o Agencia Española – Agencia Española de Protección de Datos.

Art. – Artículo.

IA – Inteligencia artificial.

INCIBE – Instituto Nacional de Ciberseguridad.

ONG – Organización No Gubernamental.

Reglamento eIDAS o eIDAS – Reglamento (UE) n.º 910/2014.

Reglamento eIDAS2 o eIDAS2 – Reglamento (UE) n.º 2024/1183.

RGPD o Reglamento – Reglamento General de Protección de Datos.

RIA – Reglamento de Inteligencia Artificial.

TFUE o Tratado de Lisboa – Tratado de Funcionamiento de la Unión Europea.

TJUE – Tribunal de Justicia de la Unión Europea.

TUE – Tratado de la Unión Europea.

UE o **La Unión –** Unión Europea.

INTRODUCCIÓN

En la era de la inteligencia artificial, el acceso a internet se ha convertido en una parte fundamental de la vida cotidiana, especialmente para la infancia y la adolescencia[1], quienes a menudo utilizan plataformas digitales sin comprender exactamente los riesgos que esto conlleva.

El constante uso de los dispositivos tecnológicos y las redes sociales, sobre todo desde temprana edad, ha aumentado las preocupaciones sobre la seguridad digital de la infancia, especialmente en el contexto actual fuertemente marcado por la implementación de la inteligencia artificial. Estos avances han abierto nuevas puertas para la interacción y el aprendizaje, pero también han incrementado los riesgos como la exposición a contenido inapropiado, la pornografía, el ciberacoso y la explotación de datos personales.

Esta situación plantea una serie de desafíos en cuanto a la protección de su privacidad que deben ser abordados por un marco normativo adecuado. En este sentido, destacan tres Reglamentos de la Unión Europea relativamente nuevos, diseñados con el objetivo de garantizar la defensa de los derechos fundamentales de todas las personas y, sobre todo, de las menores de edad. Estos cuerpos normativos son el Reglamento General de Protección de Datos (RGPD), el Reglamento eIDAS2 y el Reglamento de Inteligencia Artificial (RIA).

El objetivo principal de este estudio es analizar cómo estas normativas contribuyen a la protección de las personas menores de edad en internet, especialmente en relación a la privacidad y seguridad de sus datos personales. Además, en este trabajo se busca examinar cómo el Reglamento eIDAS2 contribuye a la mejora de la protección de datos de menores y ver como los tres marcos normativos se complementan para ofrecer un ámbito más seguro para los y las menores. Por último, se realizará un análisis de riesgos aplicado a casos actuales, evaluando los riesgos específicos que enfrenta la infancia y juventud en el ámbito digital.

En esta línea, se ha desarrollado la hipótesis de que la implementación de estos tres reglamentos permitirá establecer mecanismos más efectivos para la protección de los niños, niñas y

[1] En coherencia con los valores de igualdad promovidos por la *Universitat Autònoma de Barcelona*, se ha procurado utilizar un lenguaje inclusivo y no sexista a lo largo del presente trabajo, siguiendo las recomendaciones de la *Guia per a l'ús no sexista del llenguatge a la Universitat Autònoma de Barcelona* del *Observatori per a la Igualtat* y el *Servei de Llengües* de la UAB.

adolescentes en entornos digitales, facilitando la verificación de edad y el consentimiento parental sin comprometer su derecho a la privacidad.

Para un desarrollo adecuado, se ha dividido el trabajo en dos capítulos principales, el primero siendo una investigación detallada principalmente del RGPD, puesto que es la norma de referencia en materia de protección de datos, en combinación con el Reglamento eIDAS2 y el RIA. Este marco teórico permitirá comprender las bases jurídicas que sustentan la protección de la infancia y la adolescencia en el ámbito digital.

El segundo capítulo del presente trabajo consiste en realizar un análisis de riesgos de dos casos especialmente relevantes en la actualidad. Para garantizar un buen enfoque, ambos casos se estructuran siguiendo una misma metodología. Cada análisis empieza con la exposición del caso concreto, en la que se contextualiza el supuesto y se explica su relevancia en el entorno digital actual. Seguidamente, se identifican los bienes jurídicos principales que pueden haber sido vulnerados. En tercer lugar, se ofrece una descripción de los riesgos centrada en los posibles daños derivados de la situación planteada. Después se examinan las vulnerabilidades que pueden facilitar la materialización de cada riesgo concreto. Asimismo, se analiza la probabilidad de que dicho riesgo se produzca, así como el impacto que tendría en caso de materializarse, teniendo en cuenta su gravedad y consecuencias sobre el bienestar y los derechos de las personas menores de edad. Por último, se incluye una matriz de riesgos que permite visualizar gráficamente la relación entre la probabilidad y el impacto, clasificando el nivel de riesgo mediante un sistema de colores basado en el *método del semáforo*: verde para riesgos bajos, naranja para riesgos moderados y rojo para riesgos altos.

Este enfoque permite combinar teoría y práctica integrando la interpretación jurídica con el análisis de situaciones concretas y actuales. Así, el trabajo no solo examina la normativa, sino que también propone una forma estructurada de evaluar los riesgos digitales que enfrenta tanto la infancia como la juventud.

Finalmente, este trabajo se presenta como una aportación jurídica y metodológica con el objetivo de ayudar a entender y gestionar los riesgos y amenazas digitales que afectan a niñas, niños y adolescentes en el contexto actual de la transformación tecnológica.

1. LA PRIVACIDAD DE LAS PERSONAS MENORES DE EDAD EN EL ENTORNO DIGITAL: REGULACIÓN Y PROTECCIÓN JURÍDICA

1.1.El derecho a la protección de datos como derecho fundamental

El derecho a la protección de datos ha ido evolucionando a lo largo de la historia, pasando de ser inexistente a un derecho fundamental relevante en una sociedad tan marcada por la tecnología como es la actual.

La necesidad de otorgar una protección especial a los datos personales hizo que el Consejo de Europa marcara el primer paso hacia su protección internacional mediante la adopción de la Convención 108 en el año 1981. Este tratado fue el primer instrumento internacional jurídicamente vinculante que trata la protección de datos (Abril Marti y Maciejewski, 2024) y, desde entonces, su desarrollo ha sido consolidado y reforzado por la Unión Europea (UE).

La Unión Europea ha desempeñado un papel destacado en el ámbito de la protección de datos otorgándole, así, un gran valor a la privacidad. Este derecho se ha consagrado como fundamental en la Carta de los Derechos Fundamentales de la Unión Europea (artículo n.º 8) y en la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (principio n.º 17). Aunque esta última Declaración no es legalmente vinculante (Parlamento Europeo, 2022), es esencial para la aplicación de los derechos, ya que proporciona una guía clara para garantizar que la transformación digital, que está sufriendo la sociedad actual, se desarrolle de manera ética y acorde a los valores y derechos de la UE (preámbulo de la Declaración).

En consecuencia, la protección de datos es considerada como un derecho primario de la Unión porque se encuentra explícitamente prevista tanto en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE o Tratado de Lisboa) como en el artículo 39 del Tratado de la Unión Europea (TUE). Según Blasi Casagran y Cañabate Pérez (2024, p. 58), el Tratado de Lisboa ha transformado el marco europeo de protección de datos personales ya que, antes de su adopción solo había derecho derivado pero ninguna regulación primaria. Así pues, el carácter fundamental de este derecho se consolida con la incorporación de estos artículos, que otorgan una base jurídica sólida dentro del derecho primario de la UE.

No obstante, este derecho no es absoluto, sino que se ha de considerar en relación con su función en la sociedad. Esta es la posición que adopta el Tribunal de Justicia de la Unión Europea (TJUE) en su sentencia de 9 de noviembre de 2010, *Caso Volker und Markus Schecke GbR y otros contra Land Hessen*, sección 48. En este contexto, el TJUE tiene un papel relevante en el desarrollo del derecho a la protección de datos, siendo su jurisprudencia uno de los pilares fundamentales en los que descansa este derecho. Aunque la aplicación de dicha jurisprudencia está limitada al territorio de la Unión Europea, es importante destacar que sus repercusiones trascienden las fronteras de esta (Piñar Mañas y Recio Gayo, 2018).

Además, la Carta de los Derechos Fundamentales de la UE mencionada antes establece claramente en su artículo 52 que el derecho a la protección de datos puede estar sujeto a limitaciones, las cuales deberán cumplir con los requisitos establecidos en el primer apartado del mismo artículo:

> ***"Artículo 52 Alcance de los derechos garantizados.***
> *1. Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás."*

Esto pone de manifiesto la necesidad de equilibrar el derecho a la protección de datos con otros derechos fundamentales, como la libertad de expresión. El principio de proporcionalidad permite evaluar si las limitaciones a este derecho son necesarias y están justificadas, garantizando así un adecuado balance entre intereses individuales y colectivos en el marco de los valores de la Unión Europea.

1.2. El Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos (RGPD), adoptado el 27 de abril de 2016 y plenamente aplicable desde el 25 de mayo de 2018, constituye la principal normativa de la Unión Europea en materia de protección de datos.

Su objetivo principal es *"garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea"* (Considerando n.º170 RGPD), cuestión que debe ser abordada a nivel europeo ya que los Estados miembros, por sí solos, no

pueden garantizar una tutela uniforme y eficaz debido a las diferencias en sus legislaciones nacionales (Considerando n.º10 RGPD).

Según Piñar Mañas (2016, p. 17), con la adopción de este Reglamento se busca establecer un marco más sólido y coherente que evite la falta de uniformidad en su aplicación, reduzca la inseguridad jurídica y las discrepancias en la preservación de los derechos y libertades entre los Estados, obteniendo así un nivel de protección alto y homogéneo.

El RGPD establece un ámbito de aplicación material y territorial peculiar. Se aplica al tratamiento de datos personales cuando este se realice por empresas dentro de la Unión Europea, independientemente de que el tratamiento tenga lugar en la UE o fuera de ella. Además, se extiende a organizaciones con sede fuera de la UE que ofrezcan bienes o servicios a personas en la Unión o monitoreen su comportamiento, incluso si el tratamiento de datos se lleva a cabo fuera de la UE (art. 3 RGPD).

En cuanto a sus principios fundamentales, el artículo 5 del Reglamento recoge varios de ellos, esenciales para la debida protección de las y los menores en internet: transparencia, lealtad, licitud y consentimiento.

Al fin de otorgar una salvaguarda más específica, la incorporación del principio de **transparencia** ha sido una de las aportaciones más importantes del Reglamento. En este sentido, la información y comunicación relativa al tratamiento de sus datos debe facilitarse de forma concisa, transparente, inteligible, de fácil acceso y con un lenguaje claro y sencillo (Faggiani, 2018). A pesar de esta exigencia legal, en la práctica, la falta de transparencia sobre cómo las plataformas digitales recopilar y utilizan los datos personales sigue siendo una vulnerabilidad identificada en el análisis práctico de este trabajo (Casos 1 y 2). Garantizar una transparencia real para las personas usuarias más jóvenes es uno de los grandes desafíos para la aplicación efectiva de este principio.

El principio de **lealtad** está estrechamente relacionado con el de transparencia, ya que obliga a informar sobre la existencia del tratamiento de datos y sus objetivos, asegurando la provisión de toda la información adicional necesaria para garantizar que el tratamiento sea leal y transparente (Jiménez Jiménez, 2023). También exige que los datos recogidos sean tratados de manera justa y sin engaños. Un ejemplo de este tratamiento justo, propuesto por Blasi Casagran

y Cañabate Pérez (2024), es que no se debe impedir a las personas el acceso a oportunidades de empleo, créditos o seguros, ni someterlas a penalizaciones mediante productos financieros con riesgos excesivos o costos elevados.

En cuanto al principio de **licitud**, según Piñar Mañas (2017) el tratamiento será licito cuando los datos personales se hayan tratado con el consentimiento del interesado o " *sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud del Derecho de la Unión o de los Estados miembros (...)".* Estas bases legítimas o condiciones se encuentran recogidas en el artículo 6 del RGPD. De las seis que se establecen en este art., podemos destacar cuando el tratamiento de datos es esencial para que el responsable del mismo pueda cumplir con una obligación legal (art. 6.1.c) RGPD) o cuando este tratamiento resulta necesario para velar por los derechos del interesado o de otra persona física (art. 6.1.d) RGPD).

Por último, otro pilar esencial es el **consentimiento**, que debe ser otorgado de manera libre, informada e inequívoca por parte del interesado, garantizando así su control sobre el uso de su información personal. En este contexto, el RGPD establece que las personas menores pueden prestar su consentimiento para el tratamiento de sus datos personales a partir de los 16 años, permitiéndoles ejercer dicho control de manera autónoma (art. 8 RGPD). De esta forma, se entenderá que el tratamiento es lícito. No obstante, en los casos en los que los niños y niñas sean menores de 16 años, sólo será lícito si el consentimiento "*lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó*" (art. 8.1 RGPD). Asimismo, los Estados miembros tienen la posibilidad de fijar por ley una edad inferior para estos fines, siempre y cuando no sea inferior a los 13 años.

1.2.1. Conceptos generales y fundamentos del RGPD

Antes de abordar la problemática que puede plantear el tratamiento de los datos de las personas menores de edad, resulta necesario precisar una serie de conceptos que servirán de base para comprender la normativa y las implicaciones jurídicas relativas a la protección de datos. En este sentido, el RGPD dispone en su artículo 4 un amplio repertorio de definiciones relacionadas con esta materia, sin embargo, para este trabajo se han seleccionado aquellas que se han considerado más importantes: la definición de datos personales, su tratamiento, el responsable de este último y el consentimiento del interesado.

Según el RGPD, los **datos personales** abarcan cualquier información relativa a una persona física identificada o que se pueda identificar ya sea mediante un nombre, datos de localización o con *"uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"* (art. 4.1 RGPD). Este concepto adquiere una relevancia esencial cuando se trata de personas menores, ya que sus datos pueden incluir no solo elementos básicos de identificación, sino también información sensible que refleje su desarrollo personal y social. La protección de estos datos resulta necesaria, puesto que este colectivo está particularmente expuesto a riesgos derivados del uso indebido de su información personal, lo cual podría afectar a su bienestar y desarrollo.

En segundo lugar, para que un dato personal sea susceptible de protección, debe ser objeto de **tratamiento** (STJUE de 13 de mayo de 2014, asunto C-131/12). El reglamento lo define como cualquier operación u operaciones realizadas sobre datos personales que pueden ser la recogida, registro, conservación, utilización, difusión, entre otros. Este tratamiento de datos personales plantea riesgos concretos cuando se refiere a los niños y niñas ya que, estos pueden no ser conscientes de cómo se manejan o recolectan sus datos.

Otra de las definiciones que se debe tener en cuenta es el concepto de **responsable del tratamiento** o, simplemente, responsable. Este puede ser "*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento"* (art. 4.7 RGPD). En relación con las personas menores de edad, el responsable debe tomar medidas adecuadas para asegurar que el tratamiento sea legítimo, adecuado y seguro, teniendo en cuenta las vulnerabilidades de su edad y su capacidad para comprender los riesgos.

Por último, y quizá el concepto más importante a destacar, es el **consentimiento del interesado**. Este se define como cualquier "*manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*" (art. 4.11 RGPD). En este sentido, el consentimiento del interesado es esencial para la legitimidad del tratamiento de datos. El RGPD, concretamente en su artículo 8, exige que el consentimiento debe ser otorgado por los padres o tutores legales de personas menores de 16 años.

1.3. El eIDAS2: la versión mejorada del Reglamento 910/2014

El Reglamento (UE) n.º 910/2014, también conocido como Reglamento **eIDAS**, establece un marco jurídico común para la identificación electrónica y los servicios de confianza en la Unión Europea, con el objetivo de garantizar transacciones electrónicas seguras y mejorar la interoperabilidad entre los Estados miembros (art. 1 Reglamento eIDAS).

Este Reglamento busca eliminar las barreras existentes en el reconocimiento transfronterizo de medios de identificación electrónica y asegurar la autenticación en los servicios públicos y privados en línea, fomentando así la confianza en las interacciones digitales dentro del mercado interior europeo (Considerando n.º 12 Reglamento eIDAS).

Sin embargo, a pesar de los avances logrados con el Reglamento eIDAS, la rápida evolución tecnológica y las nuevas demandas del mercado digital europeo hicieron necesaria una revisión y ampliación de este marco normativo. Como resultado, el 20 de mayo de 2024 entró en vigor el Reglamento (UE) n.º 2024/1183, conocido como **eIDAS2** por el que se modifica el reglamento anterior con el objetivo de "*mejorar su eficacia, extender sus beneficios al sector privado y promover unas identidades digitales de confianza para todos los europeos*" (Ministerio para la Transformación Digital y de la Función Pública, s.f.).

Tal y como explica la Agencia Española de Protección de Datos (2025), el eIDAS2 tiene la finalidad de reforzar la seguridad, facilitar el uso e incrementar la interoperabilidad de los sistemas de identificación electrónica y los servicios de confianza (aquellos servicios que garantizan la seguridad de las transacciones electrónicas, como las firmas y certificados electrónicos) en toda la Unión Europea. Además, se pretende superar las limitaciones del reglamento original mediante la creación de un sistema de identidad digital eficiente y de fácil acceso.

Una de las innovaciones más relevantes del eIDAS2 que recalca la Agencia Española es la obligación de que todos los Estados miembros reconozcan los medios de identificación electrónica emitidos por cualquier otro Estado miembro, promoviendo así una mayor integración y colaboración en el ámbito digital transfronterizo.

Por último, el eIDAS2 introduce la Cartera de Identidad Digital Europea, una herramienta clave que permitirá a la ciudadanía europea gestionar de manera segura su identidad digital y acceder

a servicios públicos y privados. Esta cartera prioriza la privacidad, dándole el control a las personas usuarias sobre sus datos.

1.4. Relación del RGPD y el eIDAS2

El Reglamento eIDAS2 y el RGPD están estrechamente vinculados, ya que ambos persiguen la protección de la privacidad y el refuerzo de los derechos de las personas sobre sus datos personales. Esta relación resulta fundamental para establecer leyes que garanticen un tratamiento seguro de la información "*en el contexto de la identificación electrónica y los servicios de confianza*" (AEPD, 2025).

El eIDAS2 se ha diseñado en consonancia con el RGPD, asegurando que cualquier procesamiento de datos personales en el ámbito de la identificación digital y los servicios asociados cumpla con los principios esenciales establecidos por el RGPD. Entre estos principios se encuentran la transparencia, que exige que las personas estén informadas sobre el uso de sus datos; la minimización de datos, que promueve la recopilación de solo la información estrictamente necesaria; la limitación de la finalidad, que impide el uso de los datos para objetivos distintos a los inicialmente previstos; y el respeto de los derechos de los interesados, como el acceso, rectificación o supresión de sus datos (AEPD, 2025).

Además, el eIDAS2 subraya la necesidad de cumplir con la normativa de protección de datos en el ámbito de los servicios en línea, prestando especial atención al principio de minimización de datos. Esto significa que únicamente se deben utilizar los datos imprescindibles para permitir el acceso a estos servicios, así se evita recopilar información innecesaria. También establece que los sistemas de identificación electrónica deben ser compatibles entre los distintos estados miembros de la Unión Europea, garantizando su interoperabilidad. Asimismo, deben respetar el principio de privacidad desde "el diseño y por defecto", asegurando que la protección de datos esté integrada desde el desarrollo inicial de los sistemas y configurada como estándar (Jiménez Jiménez, 2023).

La estrecha alineación entre ambos reglamentos no solo refuerza la seguridad de las transacciones electrónicas, sino que también asegura un marco legal coherente que protege la privacidad y otorga a la ciudadanía un control efectivo sobre su información personal.

1.5. Breve introducción al Reglamento de Inteligencia Artificial y la protección que ofrece a las personas menores

El Reglamento (UE) 2024/1689 de Inteligencia Artificial (RIA) es el primer reglamento que establece normas sobre el uso de la inteligencia artificial (en adelante, IA). Tiene como objetivo mejorar el funcionamiento del mercado interior mediante la creación de un marco jurídico uniforme para facilitar el desarrollo, la introducción, la comercialización y el uso de sistemas de IA en todos los Estados miembros de la Unión Europea, garantizando la protección de los derechos establecidos en la Carta de los Derechos Fundamentales de la UE (Considerando 1, RIA).

Aprobado por el Parlamento Europeo el 13 de marzo de 2024 y publicado en el Diario Oficial de la Unión Europea el 12 de julio de ese mismo año, el reglamento entra en vigor el 2 de agosto de 2026. Sin embargo, algunos de sus preceptos se aplicarán gradualmente desde 2025 hasta 2027, lo que le otorga una implementación sumamente particular.

Dentro de sus disposiciones, el Reglamento prohíbe una serie de prácticas de IA debido a los riesgos que implican. Estas incluyen el uso de técnicas manipuladoras o *subliminales* con el objetivo de alterar el comportamiento de las personas (art. 5.1.a)), el aprovechamiento de vulnerabilidades derivada de la edad, discapacidad o situación socioeconómica (art. 5.1.b)), la utilización de sistemas de IA para clasificar a individuos en función de su comportamiento (art. 5.1.c)), entre otras.

El artículo 5.1.b) junto con el Considerando n.º 29 del RIA adquieren una especial relevancia para este trabajo ya que, prohíben expresamente el uso de la IA para explotar vulnerabilidades específicas. En concreto, el Considerando n.º 29 señala que estos sistemas pueden agravar la explotación de debilidades relacionadas con la edad, la discapacidad o condiciones socioeconómicas, afectando gravemente a colectivos vulnerables, como minorías o personas en situación de pobreza extrema. Esta prohibición busca prevenir daños acumulativos y garantizar la protección de los derechos fundamentales.

La protección de la infancia y la adolescencia se vuelve aún más relevante en este contexto. Dado que las y los menores están en una etapa crucial de su desarrollo, son especialmente susceptibles a influencias nocivas y abusivas que pueden comprometer su bienestar emocional,

educativo y social. Por ello, las disposiciones del artículo 5.1.b) y el Considerando n.º 29 se presentan como protecciones esenciales para evitar que estos sistemas exploten la inexperiencia y la fragilidad características de este colectivo.

En definitiva, el marco regulador no solo protege a colectivos vulnerables en general, sino que pone especial énfasis en la protección de la juventud, asegurando que la innovación tecnológica se desarrolle de manera ética y alineada con los principios fundamentales de derechos humanos.

2. ANÁLISIS PRÁCTICO DE RIESGOS Y AMENAZAS EN EL ENTORNO DIGITAL

En esta sección del trabajo, se analizarán los riesgos y amenazas a los que están expuestas las personas menores de edad en el entorno digital, con un enfoque particular en los servicios más utilizados por este grupo, como las redes sociales y las páginas web de contenido para adultos. El análisis consistirá en dos casos representativos que permiten identificar con claridad las vulnerabilidades y los riesgos a los que la población adolescente se enfrenta.

Los casos seleccionados son: la protección de las cuentas de adolescentes en Instagram y el acceso de menores a páginas para adultos. Cada uno de ellos aborda bienes jurídicos distintos, lo que permite ofrecer una perspectiva más amplia y complementaria sobre los desafíos actuales.

2.1. CASO 1. Protección de cuentas de adolescentes en Instagram

2.1.1. Descripción del caso

El 17 de septiembre del 2024, Instagram presentó las "*Cuentas de Adolescente*", su nueva iniciativa diseñada para ofrecer una mayor "*protección para los adolescentes*" y proporcionar más "*tranquilidad para los padres*" (Instagram, 2024). Según la plataforma, estas cuentas incluyen "*protecciones integradas*" que restringen quién puede contactar a los y las menores y el tipo de contenido al que pueden acceder. Además, algunas configuraciones, como las restricciones en los mensajes, el control del contenido sensible y la configuración de cuentas privadas, se activan por defecto y solo pueden modificarse con la autorización de la madre, del padre o del tutor cuando los adolescentes son menores de 16 años.

Tal y como señala el diario de El País (2025), la implementación de estas cuentas en Europa comenzó a principios de 2025 y se está llevando a cabo de forma progresiva. Sin embargo, cabe preguntarse: ¿son estas medidas realmente suficientes para proteger a la infancia y adolescencia o hay riesgos que aún requieren una atención adicional?

2.1.2. Identificación del bien jurídico: privacidad y seguridad

En este caso, los bienes jurídicos protegidos son principalmente la privacidad y la seguridad de las y los menores. Ambos bienes están estrechamente vinculados ya que, la vulneración de la privacidad puede desembocar en riesgos que afecten directamente a la seguridad de las personas menores. Por ejemplo, la exposición de datos personales puede dar lugar a situaciones de acoso cibernético, contacto no deseado con desconocidos o incluso el robo de identidad. Estas situaciones comprometen el bienestar emocional y psicológico de los y las menores.

Las medidas de seguridad implementadas por Instagram, como las restricciones en los mensajes o la configuración por defecto de cuentas privadas son esenciales para proteger la privacidad de este colectivo ya que buscan minimizar el riesgo de exposición y controlan quién tiene acceso a la información personal de cada adolescente, garantizando así un entorno más seguro y privado.

En este contexto, es relevante destacar la jurisprudencia del TJUE, concretamente la sentencia de 16 de julio del 2020, asunto C-311/2018 puesto que "*las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión por el referido Reglamento, interpretado a la luz de la Carta*" (párrafo 105). El TJUE recalca la necesidad de garantizar un nivel de protección elevado asegurando que los datos personales sean tratados con estándares de seguridad altos y que no se utilicen sin las garantías mínimas.

Cabe destacar que, aunque la sentencia no hace referencia explícita a las personas menores, sus principios son igualmente aplicables al caso concreto ya que, las garantías de la protección de datos deben aplicarse independientemente del país, región o Estado donde operen las plataformas. En el contexto de Instagram, una red social global, las garantías de protección de

datos deben ajustarse a los estándares europeos para asegurar que las y los menores estén protegidos, tanto dentro como fuera del territorio de la UE. Las medidas de protección deben garantizar que, sin importar el territorio, los datos personales se traten con el mismo nivel de seguridad y privacidad, cumpliendo con las normativas europeas para su protección.

Por otra parte, el artículo 8.1 del RGPD establece de manera específica como debe realizarse la protección de los datos personales de menores de 16 años, exigiendo el consentimiento explícito de los padres o tutores para el tratamiento de sus datos. Este marco legal justifica las medidas adoptadas por Instagram, garantizando que la infancia y la adolescencia no sean sujetos a riesgos innecesarios en cuanto a la exposición de sus datos personales. En este sentido, las medidas establecidas buscan alinearse con las exigencias del Reglamento, protegiendo así tanto la privacidad como la seguridad de los y las menores.

El apartado segundo de este mismo artículo establece que "*el responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible*".

De esta forma, las medidas y correcciones aplicadas por la plataforma social se ajustan tanto a la normativa europea como a las directrices del TJUE, buscando un equilibrio entre el uso seguro y adecuado de Instagram por parte de las y los adolescentes y la protección de sus derechos fundamentales.

2.1.3. Descripción del riesgo o amenaza

Los y las menores que utilizan Instagram se enfrentan diariamente a múltiples riesgos que pueden poner en peligro tanto su privacidad como su seguridad. Por esta razón, la Comisión Europea adoptó el 11 de mayo de 2022 la estrategia "*Better Internet For Kids*" o, de forma más simple, "*BIK+"* para garantizar que sean respetados y protegidos. Sin embargo, como señala la *BIK+* (Comisión Europea, 2022), no todas las interacciones o contenidos a los que están expuestos en línea son positivos. Entre los principales riesgos, se destacan el ciberacoso y el acceso a contenido inapropiado.

Estos son los riesgos que se han elegido para este análisis puesto que la estrategia *BIK+* los identifica como amenazas claves en la protección de la infancia y adolescencia en internet, destacando su relevancia y el impacto que tienen en su seguridad y bienestar.

Además, la mayoría de las aplicaciones utilizadas por este colectivo no están diseñadas teniendo en cuenta su protección, lo que los deja vulnerables a riesgos adicionales (Comisión Europea, 2022), como la exposición no deseada de información personal y la posible explotación de sus datos.

Teniendo en cuenta lo anterior, se identifican varios riesgos relevantes en el contexto de la protección de los y las menores. Uno de los más significativos es el **acceso a contenido inadecuado** puesto que, a pesar de las medidas de restricción y los filtros implementados, las personas menores aún pueden encontrarse con material que no es adecuado para su edad, lo que podría influir negativamente en su desarrollo y bienestar emocional.

Otro riesgo importante es el **ciberacoso**. Este, según el *Cyberbullying Research Center* (como se cita en UNICEF, 2017), se refiere al "*daño intencionado y repetido causado a través del uso de ordenadores, teléfonos móviles y otros dispositivos electrónicos*" (traducción propia del inglés*)*. A diferencia de otras épocas, en las que el acoso cesaba al volver a casa, hoy en día puede continuar a cualquier hora mediante las redes sociales, mensajes o publicaciones. Esta exposición constante hace que el acoso sea más prolongado y puede provocar daños igual de graves que el acoso "ordinario". El uso de redes sociales y plataformas digitales por menores aumenta considerablemente el riesgo de que sean víctimas de ciberacoso. Comentarios hirientes y ofensivos, amenazas o la difusión no consentida de imágenes son algunas de las formas más comunes de este tipo de violencia.

La **falta de conciencia sobre la privacidad** también es uno de los riesgos más destacables porque muchos menores no son plenamente conscientes de los peligros que conlleva compartir información personal en internet, como su ubicación, fotografías o datos sensibles tanto suyos como de personas cercanas. Consecuentemente, esta desinformación los expone al uso indebido de su información. En este sentido, el principio de transparencia del RGPD tiene una importancia especial puesto que, según este principio, la información sobre el tratamiento de datos debe comunicarse de forma clara, comprensible y adecuada para la edad de cada usuario.

Por último, la **explotación de datos personales.** Las plataformas digital pueden recopilar y procesar datos personales de menores sin que estos comprendan el alcance y las consecuencias de dicho tratamiento. Aquí también entra en juego el principio de transparencia mencionado anteriormente.

2.1.4. Análisis de vulnerabilidades

Para evaluar de manera efectiva los riesgos mencionados (acceso a contenido inadecuado, ciberacoso, …), es necesario identificar las vulnerabilidades que podrían incrementar la exposición a estos riesgos. Estas vulnerabilidades aumentan la probabilidad de que los riesgos se conviertan en una realidad.

Según el Instituto Nacional de Ciberseguridad (INCIBE) del estado Español, una vulnerabilidad es "*una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma*" (INCIBE, 2017). Aunque esta definición se centra en los aspectos técnicos, es importante destacar que se ha utilizado para entender el concepto de vulnerabilidad y así, poder adaptarlo al contexto del presente trabajo, en el que se analizan no solo las debilidades técnicas sino que también se consideran los factores sociales y educativos que afectan al colectivo.

Por lo tanto, en este contexto, se han identificado las siguientes vulnerabilidades relacionadas con los y las menores y su interacción con la plataforma de Instagram.

Para el primer riesgo, el **acceso a contenido inadecuado**, las vulnerabilidades a destacar son la **ineficacia de los filtros de contenido** y la **clasificación incorrecta del contenido.** En relación a la primera, según Instagram (2024), se utilizan filtros para restringir el contenido inapropiado, sin embargo, estos pueden no ser fiables y las y los adolescentes podrían seguir teniendo acceso a contenido no adecuado para su edad. Respecto a la segunda vulneración, se pueden dar casos donde se haga una mala clasificación del contenido, lo que podría resultar en la exposición de las personas menores a publicaciones inapropiadas, peligrosas, dañinas, etc.

En relación al segundo riesgo encontrado, es decir, el **ciberacoso**, se han destacado tres vulnerabilidades importantes: la **falta de supervisión parental**, la **dificultad para identificar comportamientos abusivos** y la **deficiencia en la detección automática**. La primera

vulnerabilidad se refiere a que los y las menores a menudo tienen acceso a sus cuentas sin restricciones, lo que aumenta el riesgo de que se encuentren con comentarios hostiles, inapropiados, ... La segunda consiste en que muchos adolescentes no tienen el conocimiento suficiente para reconocer comportamientos de acoso en línea, lo que hace difícil la intervención temprana y adecuada. Y la última se refiere a que las plataformas sociales, como Instagram, no siempre cuentan con medidas suficientemente precisas o rápidas para identificar y parar el acoso de forma efectiva.

Para el riesgo de la **falta de conciencia sobre la privacidad** tenemos que la primera vulnerabilidad es el **desconocimiento sobre los peligros de compartir información.** Esto se debe a que muchos menores no son conscientes de las consecuencias de publicar datos personales, como su ubicación o imágenes. Y, por último, la **falta de educación digital,** es decir, la poca cantidad de programas educativos sobre privacidad que deja a este colectivo aún más vulnerable a prácticas peligrosas en internet.

Finalmente, la **explotación de datos personales** tiene dos vulnerabilidades concretas. La primera es el **desconocimiento sobre el uso de datos** puesto que los y las menores a menudo no conocen concretamente las implicaciones del tratamiento de sus datos personales en las plataformas, lo que los expone a riesgos de explotación. Y la segunda es la **falta de transparencia en la recopilación de datos** la cual está relacionada con el hecho de que las plataformas pueden recopilar información sin una comunicación clara sobre su uso, lo que dificulta que los adolescentes comprendan el alcance del tratamiento de sus datos. En relación con esta última vulnerabilidad, cabe traer a colación el Reglamento eIDAS2 puesto que este ofrece un marco normativo para la implementación de mecanismos seguros de verificación de edad, lo que puede contribuir a mejorar el control sobre el tratamiento de datos.

2.1.5. Evaluación de la probabilidad

En este apartado, se evaluará la probabilidad de que ocurran o se materialicen los riesgos mediante 3 categorías:

- Probabilidad alta: La probabilidad de que el riesgo ocurra es elevada dado que las protecciones actuales no son suficientes para mitigar la amenaza de forma eficaz.

- Probabilidad media: La probabilidad es moderada puesto que el riesgo es relevante pero existen mecanismos de protección que pueden reducir la probabilidad.
- Probabilidad baja: La probabilidad de que el riesgo se materialice es baja ya que las medidas de protección implementadas son efectivas y la exposición del menor a la amenaza es baja.

Para definir y evaluar la probabilidad de materialización del riesgo, se ha tomado como referencia la guía práctica sobre la "*Evaluación de impacto relativa a la protección de datos*" de la Autoridad Catalana de Protección de Datos (2024) y se ha adaptado al contexto del presente trabajo.

En relación a los riesgos o amenazas concretas de este caso, tenemos lo siguiente. Respecto al **acceso a contenido inadecuado**, la probabilidad de que las niñas, niños y adolescentes accedan a contenido inadecuado en internet es **alta**, ya que las medidas de protección actuales no son completamente efectivas para prevenir este riesgo.

El responsable de Educación y Derechos Digitales de la Infancia en UNICEF España, Nacho Guadix García (2025), advierte que es necesario implementar mecanismos de verificación de edad, configurar controles parentales y etiquetar el contenido de manera adecuada para evitar que los y las menores puedan acceder a contenido no apropiado para su edad (ej. trastornos alimenticios, discursos de odio, contenido pornográfico…).

Con la introducción de las nuevas Cuentas de Adolescentes, Instagram busca mitigar o, incluso resolver, este problema mediante las restricciones ya mencionadas (perfiles privados por defecto o interacciones limitadas). Además, se aumenta el control parental para modificar cualquier protección predeterminada. Sin embargo, la eficacia de estas medidas depende, en gran medida, de la implicación de los padres y tutores y, sobre todo, de las personas menores que utilizan la red social. Según un estudio elaborado en colaboración con *Save The Children*, el 60% de los adolescentes españoles sabe cómo saltarse el control parental en el entorno digital, lo que pone en duda la efectividad real de estas restricciones (El País, 2025).

Por otra parte, el **ciberacoso** sigue siendo uno de los principales riesgos a que los niños y niñas están expuestos (Comisión Europea, 2022), por tanto, la probabilidad de sufrir ciberacoso es **alta**. Además, la facilidad para crear cuentas falsas, la falta de supervisión parental y la

dificultad para identificar y denunciar casos de acoso aumentan significativamente su prevalencia.

Entre los factores que favorecen el ciberacoso se encuentran el anonimato en línea, la rápida difusión de contenido y la poca supervisión por parte de los adultos (UNICEF Comité Español, 2024). Estos elementos facilitan la propagación y el impacto del ciberacoso en las plataformas digitales. Aunque Instagram ha implementado restricciones en las Cuentas de Adolescentes, estas no logran impedir que el acoso ocurra, por ejemplo, mediante cuentas anónimas.

Para el riesgo de la **falta de conciencia sobre la privacidad**, nos encontramos ante que muchos menores comparten información personal sin ser plenamente conscientes de los riesgos asociados. La ausencia de una educación digital adecuada refuerza esta vulnerabilidad, ya que dificulta que las y los menores comprendan realmente el alcance del tratamiento de sus datos y las consecuencias de compartir información en línea.

No obstante, la probabilidad se considera **media** ya que, la privacidad es uno de los puntos clave en los perfiles de Instagram de menores. La red social ha implementado medidas concretas para reducir el riesgo como la configuración de perfiles privados por defecto. Sin embargo, estas medidas no sustituyen la necesidad de una educación digital puesto que muchos menores desconocen cómo gestionar correctamente su información en internet.

Finalmente, en relación a la **explotación de datos personales**, la probabilidad de que las plataformas como Instagram exploten los datos personales se puede considerar **media** porque existen, actualmente, relevantes normativas como el RGPD que establece restricciones como la obligación de obtener el consentimiento explícito de los padres o tutores para el tratamiento de datos de personas menores (art. 8.1 RGPD). Su aplicación efectiva, sin embargo, sigue siendo un desafío en el entorno digital en constante evolución. Tal y como señala Educo ONG (2025), "*los menores están expuestos a riesgos debido al uso masivo de dispositivos conectados a internet. Desde redes sociales hasta aplicaciones educativas, muchos servicios recopilan datos sin que los niños y niñas o sus padres sean plenamente conscientes*" (Educo ONG, 2025).

2.1.6. Impacto del riesgo

Para realizar el análisis del impacto también se han utilizado los conceptos y las definiciones de la guía práctica sobre la "*Evaluación de impacto relativa a la protección de datos*" de la Autoridad Catalana de Protección de Datos (2024). A partir de esta guía, se han determinado los tres niveles de impacto. Además, las definiciones de cada impacto, al igual que con la probabilidad, han sido modificadas para su aplicación específica en el contexto de los y las menores en internet.

- Impacto bajo: las personas menores pueden sufrir algunas consecuencias pequeñas, las cuales pueden superar sin problemas (por ejemplo, pérdida de tiempo, enfado, etc.).
- Impacto medio: las personas menores pueden encontrar inconvenientes importantes, que pueden superar con algunas dificultades (por ejemplo, falta de comprensión, estrés, daños físicos, imposibilidad de acceder a algún servicio, etc.).
- Impacto alto: las personas menores pueden sufrir consecuencias graves, que pueden superar con dificultades importantes (por ejemplo, discriminación, robo de identidad, daños psicológicos, daños para la reputación, daños físicos, empeoramiento de la salud, etc.).

El **acceso a contenido inadecuado**, sobre todo material pornográfico o violento, puede tener un impacto **medio** ya que genera efectos negativos en los y las menores como es la exposición a ideas perjudiciales para su desarrollo emocional y cognitivo. Aunque el impacto se puede superar, es necesario mitigar el riesgo con educación digital y control parental.

Por otra parte, el **ciberacoso** representa un riesgo grave para los niños y las niñas, ya que puede provocar ansiedad, aislamiento social, depresión, baja autoestima, entre otros. Además, el acoso en línea puede llegar a extenderse fuera del entorno "*digital*", afectando a la vida del menor. Por tanto, el impacto es **alto**.

Para el riesgo de la **falta de conciencia sobre la privacidad**, se ha considerado que, aunque la probabilidad es media, el impacto de este riesgo en concreto es **bajo** puesto que las consecuencias se pueden superar con la formación digital y herramientas adecuadas. La exposición a publicidad personalizada o contactos no deseados puede generar molestias, pero

no suele tener consecuencias graves. Además, las configuraciones de privacidad en plataformas digitales y la supervisión parental pueden mitigar estos efectos.

Por último, la **explotación de datos personales** tiene un impacto **alto** porque el uso indebido de estos datos puede derivar en consecuencias graves e irreversibles, como la pérdida de control sobre su identidad digital o su uso con fines comerciales sin consentimiento. La recopilación masiva de datos sin una supervisión adecuada aumenta la vulnerabilidad de las personas menores en el entorno digital y la falta de transparencia en el tratamiento de estos datos agrava aún más el problema, dificultando la protección de sus derechos. También es importante mencionar que las consecuencias pueden agravarse aún más si se utiliza la inteligencia artificial que, como señala el art. 5.1.b) del RIA, explote vulnerabilidades derivadas de la edad para manipular la toma de decisiones o incluso fomentar el consumo compulsivo de contenido.

2.1.7. Matriz de riesgos

Para cerrar el análisis de este caso, se ha elaborado una matriz de riesgos para determinar qué riesgos son más graves y cuales tienen mayor probabilidad de ocurrir. Conviene señalar que, tanto en el CASO 1 como en el CASO 2, se han tomado como referencia la guía "*Evaluación de impacto relativa a la protección de datos"* de la *Autoritat Catalana de Protecció de Dades* (2024) y el documento "*Gestión del riesgo y evaluación de impacto en tratamientos de datos personales: Relación de Tablas*" de la AEPD (2021) para realizar la matriz de forma adecuada.

La presente matriz se divide en dos grandes ejes: la probabilidad de que ocurra el riesgo y el impacto que este tendría en caso de materializarse. Además, para facilitar la interpretación, se ha implementado un sistema de colores: el color rojo indica un nivel alto de riesgo, el naranja un riesgo medio y el verde un riesgo bajo.

En esta matriz se evalúan los cuatro riesgos principales asociados a la privacidad y seguridad de los y las menores en las Cuentas de Adolescentes creadas por Instagram. El riesgo menos elevado, en este caso, es la falta de conciencia sobre la privacidad ya que la probabilidad de que se materialice es media y su impacto es bajo, lo que sugiere que las medidas adoptadas por la red social son efectivas.

Por otra parte, los otros riesgos son altos. El ciberacoso se clasifica como un riesgo alto ya que tanto la probabilidad como el impacto son altos, lo que hace que destaque la gravedad del

problema. El acceso a contenido inadecuado representa un riesgo alto, con una probabilidad alta pero con un impacto medio lo que indica que, aunque ocurre con frecuencia, las consecuencias no son tan graves como otros riesgos.

Y, por último, la explotación de datos personales tiene una probabilidad media pero un impacto alto, lo que resalta las consecuencias graves que puede tener el uso indebido de la información personal de los niños, niñas y adolescentes.

		PROBABILIDAD		
		Probabilidad baja	**Probabilidad media**	**Probabilidad alta**
IMPACTO	**Impacto bajo**		Falta de conciencia sobre la privacidad	
	Impacto medio			Acceso a contenido inadecuado
	Impacto alto		Explotación de datos personales	Ciberacoso

Matriz 1 de elaboración propia a partir de las guías de la AEPD y la APDCAT

2.2.CASO 2. Acceso de menores a páginas para adultos

2.2.1. Descripción del caso

El acceso de menores de edad a páginas web con contenido para adultos, como la pornografía, constituye una de las problemáticas más relevantes y crecientes en el entorno digital. Según la Agencia Española de Protección de Datos (2024), en adelante AEPD, y el Instituto Nacional de Ciberseguridad (2021) esta práctica es una de las principales preocupaciones tanto para padres y tutores legales como para educadores ya que, la exposición a contenido inadecuado puede provocar un grave impacto en la salud mental y en el desarrollo adecuado de las y los menores.

A pesar de las restricciones legales que prohíben el acceso de menores a este tipo de contenido, en la práctica existen deficiencias en los métodos de verificación de edad, lo que permite que los y las menores eludan estos controles. La AEPD (2023) ha señalado que los sistemas actuales no son lo suficientemente robustos para prevenir de manera efectiva el acceso de menores a la pornografía.

Asimismo, la ya mencionada estrategia BIK+ reconoce que la exposición de menores a este tipo de contenido es un riesgo actual (Federation of Catholic Family Associations in Europe, 2022). La facilidad con la que las personas menores pueden eludir las advertencias de edad y acceder a contenido inadecuado puede tener consecuencias perjudiciales para su desarrollo psicológico, emocional, personal y sexual.

Este fenómeno pone de relieve una problemática más amplia: la falta de mecanismos adecuados de control y la necesidad de una regulación efectiva que permita garantizar la protección de este colectivo vulnerable.

2.2.2. Identificación del bien jurídico: derecho al desarrollo de la personalidad y libertad sexual

El acceso de menores a contenido inapropiado en internet vulnera varios derechos fundamentales. En primer lugar, el derecho al desarrollo de la personalidad de cada menor. La Convención sobre los Derechos del Niño aprobada en 1989 por la Asamblea General de las Naciones Unidas deja claro, tanto en su preámbulo como en su artículo 29.1, que el desarrollo de la personalidad constituye un objetivo esencial en la protección de la infancia. Este desarrollo requiere un entorno adecuado para el crecimiento de un niño o niña. Por ello, la exposición a contenido pornográfico puede afectar gravemente este bien jurídico.

La pornografía puede influir negativamente en la forma en que los y las adolescentes comprenden las relaciones interpersonales e íntimas. Además también puede provocar confusión, ansiedad, desensibilización emocional e incluso generar un impacto negativo en su propia imagen y autoestima (Escuela Internacional de Mediación, 2024).

Además del derecho al desarrollo de la personalidad, la libertad sexual de las y los menores también se ve afectada. Se trata de un derecho fundamental que permite a cada persona tomar decisiones autónomas sobre su vida sexual y reproductiva, sin sufrir discriminación ni

coerciones. Este derecho garantiza que las personas sean libres de autodeterminarse en el ámbito de su sexualidad, es decir, pudiendo decidir sobre su vida sexual, su identidad de género y orientación sexual con total libertad (Conceptos Jurídicos, s.f.).

Ambos derechos están intrínsecamente relacionados, ya que un entorno adecuado para el desarrollo personal y la autodeterminación sexual es esencial para el bienestar y la salud del colectivo de personas menores de edad. La falta de protección frente a estos contenidos vulnera estos derechos fundamentales, lo que resalta la necesidad de medidas más eficaces y de la implementación de mecanismos de control más eficaces y eficientes para garantizar la protección de las y los menores en el entorno digital.

2.2.3. Descripción del riesgo o amenaza

Como se ha señalado previamente, el acceso a contenido inapropiado, concretamente de pornografía, representa una preocupación creciente en el ámbito de la protección de la infancia en entornos digitales. Para llevar a cabo un análisis de riesgos eficaz, es sumamente importante identificar aquellos riesgos que suponen una amenaza real y significativa para el bienestar de los y las adolescentes.

En el presente caso, se han considerado los siguientes cuatro riesgos teniendo en cuenta fuentes relevantes para la protección de menores como los informes de la ONG *Save The Children* y la AEPD.

Uno de los riesgos más destacados es la **distorsión de la percepción de la sexualidad y de las relaciones interpersonales.** Este riesgo se puede dar al consumir pornografía, lo que deriva, consecuentemente, en una visión irreal del sexo. Según el informe "*(Des)información sexual: pornografía y adolescencia"* de *Save The Children* (2020), muchos adolescentes consideran la pornografía como su principal fuente de información sexual, lo que afecta negativamente a su forma de relacionarse, fomentando la cosificación, la violencia y las relaciones desiguales. Esta percepción equivocada puede dificultar el desarrollo de vínculos afectivos basados en la empatía, el respeto y la comunicación. En este mismo informe se pone en relieve la gran preocupación por "*la falta de capacidad de la adolescencia para ser crítica con la pornografía y para comprender que lo que ve es ficción*" y también se destaca que muchos adolescentes acceden a contenidos pornográficos sin haber desarrollado todavía una madurez afectivo-

sexual adecuada, lo que contribuye a reforzar estereotipos de género y esta distorsión de su percepción de la sexualidad.

Relacionado con este punto, otro riesgo es la **normalización de la violencia** en las relaciones sexuales. Al consumir contenido violento, los adolescentes pueden llegar a aceptar prácticas violentas, vejatorias o abusivas como algo común o incluso deseable. El informe anterior de *Save The Children*, señala que "*la normalización de ciertas prácticas «atenúa la moral o ética» y hace más fácil que comportamientos violentos y vejatorios formen parte del deseo sexual en la adolescencia*". Además, un punto clave que el informe también destaca es que "*la autopercepción de la violencia es una construcción compleja en todas las edades, y en la adolescencia se ve atravesada, además, por mayores presiones del entorno y por falta de experiencia y educación*".

La **adicción sexual** es otro de los riesgos que, a largo plazo, puede tener graves repercusiones. Según la ONG *Dale Una Vuelta*, en colaboración con la AEPD y la Fundación del Colegio Oficial de Psicología de Madrid, el acceso esporádico a contenido para adultos puede convertirse fácilmente en una adicción caracterizada por "*tolerancia, dependencia, falta de control, abstinencia, regulación disfuncional de las emociones con la pornografía, conflictos en diferentes áreas de la vida y necesidad de consumo frecuente*" (Infografía publicada por las tres entidades, s.f.).

Finalmente, otro riesgo igualmente grave es la **explotación de datos personales.** En la misma infografía de *Dale Una Vuelta,* se considera la explotación de datos personales como uno de los riesgos más destacados al enunciar que "*Internet se adueña de tu privacidad*" y que "*La pornografía se paga con tus datos. Los datos personales tienen valor para quien quiere localizar menores, acceder a ellos, conocer sus debilidades, volverlos adictos y manipularlos".*

2.2.4. Análisis de vulnerabilidades

Las siguientes vulnerabilidades relacionadas con los riesgos anteriormente descritos pueden facilitar la exposición de menores a situaciones perjudiciales y aumentar su gravedad.

Una de las vulnerabilidades más críticas en relación con la **distorsión de la percepción de la sexualidad y de las relaciones interpersonales** es la **falta o poca educación afectivo-sexual.** Se trata de una de las principales vulnerabilidades que hay que tener en cuenta. Así lo considera

el informe de *Save The Children* (2020) mencionado anteriormente, al valorar que los adolescentes no reciben una formación adecuada en educación afectivo-sexual.

Según UNESCO (2023), este tipo de educación tiene como objetivo "*dotar a los niños y jóvenes de conocimientos, capacidades, actitudes y valores que les permitan vivir con buena salud, bienestar y dignidad; desarrollar relaciones sociales y sexuales respetuosas*".

Finalmente, el informe de *Save The Children* también destaca que "*se debe incorporar un enfoque más amplio, que aborde la afectividad y las emociones, que revise las masculinidades dominantes y la desigualdad de género y, por último, que no deje atrás la diversidad en todas sus vertientes".*

Otra vulnerabilidad importante de este primer riesgo es la **ausencia de sistemas robustos de verificación de edad** que bloqueen el acceso a contenido nocivo por parte de personas menores de edad. La exposición prematura y sin filtro a la pornografía afecta gravemente al desarrollo cognitivo y emocional de los adolescentes (Escuela Internacional de Mediación, 2024). Un ejemplo claro de esta deficiencia es la plataforma *PornHub*, una de las páginas web de contenido pornográfico más visitadas a nivel mundial. La web solo solicita una confirmación de edad sin verificarla efectivamente, con sólo un *clic* se puede acceder. Aunque ofrece un enlace para que las madres, padres y tutores legales bloqueen el acceso, esta medida no garantiza una protección real. Para solventar esta deficiencia, el Reglamento eIDAS2 promueve la creación de mecanismos de autentificación seguros que la plataforma podría implementar para garantizar un ámbito más seguro para la infancia.

En cuanto a la **normalización de la violencia,** las vulnerabilidades abarcan la exposición frecuente a contenido pornográfico violento y la exposición a contenido violento pero en otras plataformas digitales. En relación a la primera vulnerabilidad, la **exposición frecuente a contenido pornográfico violento o con prácticas vejatorias** puede alterar la percepción de los y las menores sobre lo que es aceptable en las relaciones sexuales e interpersonales. Este material promueve dinámicas de dominación, humillación o ausencia de consentimiento, lo que puede influir negativamente en la construcción de su identidad afectivo-sexual. *Save The Children* (2020) afirma que en este contenido se enseña a los chicos a "*menospreciar a las mujeres; a sexualizar el dolor femenino* […] *"y a no cuestionar el deseo y convertir el sexo en una obligación que implica la dominación de la mujer".* Por otro lado, *"a las chicas se les*

ofrece una única opción en la que su placer pasa a un segundo plano y su disposición es incondicional y en muchas ocasiones sumisa." Asimismo, la **exposición a contenido violento en otras plataformas digitales** se refiere a que la visualización de material nocivo no se limita a páginas para adultos sino que los niños, niñas y adolescentes también pueden acceder a este tipo de contenido a través de redes sociales, videojuegos, plataformas de *streaming*, anuncios, etc.

En relación al riesgo de la **adicción sexual.** Sus principales vulnerabilidades son las siguientes. La **falta de control y supervisión** adecuada por parte de los progenitores o tutores legales puede facilitar el acceso descontrolado a contenidos inapropiados. *Save the Children* (2020) destaca la necesidad de que las familias, junto con los docentes y educadores, asuman un rol activo en la educación afectivo-sexual de los niños y adolescentes. De este modo, se favorece el desarrollo de una actitud crítica y consciente frente a los contenidos que consumen y comparten en el entorno digital.

Por otra parte, el **acceso constante y sin restricciones** supone un aumento del riesgo puesto que el fácil acceso a dispositivos electrónicos conectados a Internet ha llevado a que los y las menores, incluso los niños de edades tempranas, puedan acceder sin dificultad a páginas webs de contenido inadecuado (Escuela Internacional de Mediación, 2024). Esta disponibilidad inmediata, unida a la falta de mecanismos eficaces de verificación de edad, contribuye al desarrollo de consumo compulsivo.

Por último, la **explotación de datos personales** también conlleva vulnerabilidades concretas. La primera de ellas es la **falta de comprensión sobre la gestión de datos personales.** Esta vulnerabilidad se refiere a que muchos menores no comprenden exactamente cómo se utilizan y comparten sus datos personales, especialmente en sitios web de contenido para adultos.

Tal y como señalan Dale Una Vuelta, la AEPD y el Colegio Oficial de la Psicología de Madrid (s.f.) en su infografía "*El impacto de la pornografía en menores*", estos datos tienen un gran valor para quienes buscan "*localizar menores, acceder a ellos, conocer sus debilidades, volverlos adictos y manipularlos"* lo que demuestra el riesgo que supone una baja educación digital.

La segunda vulnerabilidad de la explotación de datos personales es la **falta de conciencia sobre los riesgos de compartir información.** A diferencia de la falta de comprensión, las y los menores pueden no ser completamente conscientes de los riesgos o consecuencias de compartir su información en internet ya sea su propia información o la de terceros (p. ej. familiares, amigos, conocidos, …). Este desconocimiento aumenta el riesgo de la explotación de sus datos personales. Otro punto a destacar es el concepto de privacidad entendido por los y las menores, según INCIBE (s.f.) la perciben como una necesidad de evitar que los adultos (padres o profesores) tengan acceso a su información en internet pero "*no dan tanta importancia a las consecuencias de sus actos en Internet y les cuesta pensar en términos de futuro*".

2.2.5. Evaluación de la probabilidad

Siguiendo el mismo sistema que se ha utilizado para determinar la probabilidad en el primer caso, en este supuesto tenemos que, para la **distorsión de la percepción de la sexualidad y de las relaciones interpersonales,** la probabilidad de que se materialice es **alta** dado que el acceso de menores a contenido inapropiado, como la pornografía, es relativamente sencillo. Aunque la mayoría de las páginas webs para adultos indiquen que solo pueden entrar personas mayores de 18 años, en la práctica no se implementan sistemas complejos de verificación de edad que garanticen el cumplimiento debido de esta limitación. Esta deficiencia facilita que los adolescentes puedan eludir los controles y acceder sin grandes complicaciones, lo que incrementa notablemente el riesgo de que desarrollen una percepción distorsionada de la sexualidad y las relaciones interpersonales.

Además, tal y como se ha mencionado en el presente trabajo, el informe de *Save The Children* (2020) sostiene que la pornografía es la principal fuente de información y educación sexual que tienen los adolescentes.

En relación a la **normalización de la violencia,** según lo expuesto en el análisis de sus vulnerabilidades, la probabilidad también es **alta** debido a la frecuencia con la que los menores están expuestos a contenidos pornográficos que representan prácticas violentas o vejatorias como algo normal o deseable. Muchos adolescentes consumen pornografía de manera habitual (*Save The Children* 2020), lo que conlleva una exposición reiterada a representaciones distorsionadas de las relaciones sexuales. Asimismo, en la adolescencia, la capacidad crítica

para identificar y cuestionar estos comportamientos no está completamente desarrollada, por lo que existe un mayor riesgo de que se interioricen como conductas aceptables en la vida real.

Para la **adicción sexual,** la probabilidad es **media.** Esto es así puesto que, aunque el fácil acceso y la falta de supervisión aumentan el riesgo, la adicción sexual no es un riesgo que afecte a todos los adolescentes que consumen o pueden consumir contenido pornográfico. Además, también depende de factores individuales como la frecuencia del consumo, la educación digital del menor, el control parental y la edad en la que se accede por primera vez (Intastur Instituto terapéutico, s.f.).

Finalmente, respecto a la **explotación de datos personales,** teniendo en cuenta sus vulnerabilidades, la probabilidad de materialización del riesgo de la explotación de datos es relativamente **alta** porque como se ha expuesto a lo largo de este análisis, los y las menores no poseen una comprensión adecuada sobre cómo se gestionan sus datos ni son plenamente conscientes de los riesgos asociados a compartir información en línea (Setién, 2017).

2.2.6. Impacto del riesgo

De acuerdo con el procedimiento aplicado en el primer supuesto, en esta ocasión se observa que ninguno de los riesgos planteados encaja en la categoría de *impacto bajo*, ya que la adicción sexual, la explotación de datos personales y demás riesgos no suelen provocar simples pérdidas de tiempo o consecuencias fácilmente superables, sino que acarrean repercusiones que afectan al desarrollo integral de las y los menores.

Esta conclusión también es respaldada por el Gobierno de España, que reconoce en una noticia publicada por la Secretaría de Estado de Justicia que "*el acceso temprano a este tipo de contenido tiene graves consecuencias entre los y las menores*" (2024).

Por consiguiente, el impacto de cada uno de los riesgos es el siguiente. En relación a la **distorsión de la percepción de la sexualidad y de las relaciones interpersonales** es importante destacar que el acceso a contenido pornográfico en una franja de edad tan crucial para el desarrollo de los y las menores lleva consigo el riesgo de alterar la forma en que este colectivo entiende la sexualidad, llevándolo a interiorizar modelos irreales basados en la pornografía. Esto puede afectar directamente a su desarrollo afectivo y sus expectativas sobre

las relaciones interpersonales. Por tanto, el impacto de este riesgo debe considerarse como **alto**, dada su influencia en el desarrollo psicológico y emocional de cada menor.

Normalización de la violencia: este riesgo también tiene un impacto **alto** ya que la exposición a contenido inadecuado puede promover actitudes machistas, tolerancia hacia la agresividad en las relaciones sexuales y la cosificación de las personas lo que en algunos casos puede derivar en situaciones de abuso. Así lo considera una investigación de SEDRA - Federación de Planificación Familiar (2022) con la que se pretende desvelar el impacto de la pornografía en personas jóvenes de Castilla-La Mancha destacando que *"[…] los/as jóvenes perciben que la pornografía presenta la violencia y el control como algo atractivo y que despierta el deseo de todas las personas […]"*. Esta percepción contribuye a normalizar conductas que refuerzan estereotipos y roles de poder desequilibrados entre mujeres y hombres, afectando al desarrollo de relaciones basadas en el respeto y el consentimiento.

Por otra parte, la **adicción sexual** tiene un impacto **medio** ya que, si bien no todos los menores desarrollan una conducta adictiva, existe una creciente evidencia de que la exposición frecuente y sin control puede promover un consumo compulsivo y excesivo, tal y como advierten Dale Una Vuelta, la AEPD y la Fundación Colegio Oficial de la Psicología de Madrid (s.f.). Esta conducta puede interferir en su vida cotidiana, en su rendimiento escolar, sus relaciones interpersonales, etc. creando dependencia emocional. No obstante, a diferencia de los otros riesgos analizados, el impacto de esta adicción varía significativamente entre individuos ya que deben tenerse en cuenta las circunstancias personales de cada menor.

Por último y como en el anterior caso, la **explotación de datos personales** presenta un impacto **alto**. Esto se debe a que se trata de un grupo especialmente vulnerable que requiere una mayor protección a la hora de recopilar o utilizar sus datos (Considerando n.º 38 RGPD). La exposición de su privacidad implica riesgos graves que pueden vulnerar sus derechos fundamentales, a su seguridad y a su dignidad, al posibilitar su identificación, seguimiento o manipulación en entornos digitales sin el debido control ni consentimiento (AEPD, 2023).

2.2.7. Matriz de riesgos

De igual modo que en el CASO 1, se ha elaborado una matriz de riesgos para valorar el impacto y la probabilidad de los riesgos identificados.

La adicción sexual es el riesgo menos elevado en comparación con los demás riesgos puesto que presenta una probabilidad e impacto medios. Como bien se ha dicho, no todos los menores pueden desarrollar esta adicción pero un acceso frecuente y sin control a contenidos inapropiados puede aumentar la probabilidad de padecerla. Por otra parte, la normalización de la violencia tiene una probabilidad alta pero un impacto medio. Esto es así porque la exposición constante a contenido violento puede naturalizar conductas agresivas en las relaciones interpersonales, aunque su impacto puede variar dependiendo del entorno familiar y educativo del menor.

Finalmente, y en relación a los dos últimos riesgos, se observa en la matriz que ambos se clasifican con un impacto y probabilidad altos. Tanto la explotación de datos personales como la distorsión de la percepción de la sexualidad y de las relaciones interpersonales representan amenazas especialmente graves. Por un lado, tenemos que la falta de comprensión de las y los menores sobre las implicaciones de compartir información en internet los expone a un uso indebido de sus datos. Por otra parte, el consumo de contenido pornográfico como principal fuente de educación sexual puede consolidar una visión distorsionada de las relaciones afectivas y sexuales.

		PROBABILIDAD		
		Probabilidad baja	**Probabilidad media**	**Probabilidad alta**
IMPACTO	**Impacto bajo**			
	Impacto medio		Adicción sexual	Normalización de la violencia
	Impacto alto			Explotación de datos personales Distorsión de la percepción sexualidad y relaciones

Matriz 2 de elaboración propia a partir de las guías de la AEPD y la APDCAT

3. CONCLUSIONES

A partir de la investigación jurídica y del análisis práctico desarrollado en el presente trabajo, se da respuesta a la hipótesis inicial, que planteaba si la implementación de los tres reglamentos europeos —el Reglamento General de Protección de Datos, el Reglamento eIDAS2 y el Reglamento de Inteligencia Artificial— permite establecer mecanismos más eficaces para la protección de personas menores de edad en entornos digitales, logrando un equilibrio entre la verificación de edad y el consentimiento, todo ello sin comprometer su derecho a la privacidad.

Del estudio realizado, se concluye que la hipótesis se cumple parcialmente. Si bien el desarrollo legislativo europeo se orienta hacia una mejora significativa de esta situación, persisten limitaciones relevantes en la aplicación efectiva de estos instrumentos que impiden garantizar una protección completa de los derechos de la infancia en el ámbito digital.

En primer lugar, el RGPD constituye la base del sistema europeo de protección de datos y establece principios fundamentales como la transparencia, el consentimiento y la lealtad para el tratamiento de datos de personas menores de edad. No obstante, la norma no proporciona herramientas técnicas específicas para garantizar, de forma práctica, la verificación de la edad ni del consentimiento de quienes ejercen la patria potestad. Esta ausencia responde a una decisión del legislador europeo de mantener una neutralidad tecnológica, tal y como se recoge en el Considerando n.º15, al indicar que "*la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas*". Esta neutralidad permite adaptar el reglamento a los avances tecnológicos, pero también deja un vacío en cuanto a herramientas prácticas, especialmente si se relaciona al tratamiento de datos personales de menores.

En este contexto, el Reglamento eIDAS2 representa un avance sustancial al prever mecanismos de identificación digital seguros y respetuosos con la privacidad, como la futura Cartera Europea de Identidad Digital. Esta herramienta podría facilitar de manera fiable la identificación de personas menores de edad y de sus representantes legales, permitiendo así cumplir con las exigencias del RGPD relativas al consentimiento informado. No obstante, su impacto efectivo dependerá de su implementación práctica, la cooperación entre Estados miembros y la adopción por las plataformas digitales.

Por su parte, el RIA introduce un enfoque preventivo fundamental, al prohibir el desarrollo y uso de sistemas que exploten vulnerabilidades derivadas de la edad, entre otras circunstancias. Esta disposición refuerza la protección de los derechos de la infancia frente a prácticas discriminatorias o manipuladoras por parte de sistemas automatizados. Sin embargo, la norma se encuentra aún en fase de aplicación progresiva, lo que limita su efectividad inmediata.

Desde una perspectiva práctica, los casos analizados muestran que los riesgos a los que se enfrentan las personas menores en entornos digitales siguen siendo un problema significativo a pesar del marco normativo europeo.

En el primer caso sobre las cuentas de adolescentes en Instagram, se observa que, a pesar de las medidas adoptadas por la plataforma y de las exigencias normativas, persisten riesgos como el ciberacoso y la explotación de sus datos personales. La verificación del consentimiento parental sigue siendo débil, y existen lagunas técnicas que dificultan una supervisión adecuada y efectiva.

En el segundo caso, vinculado al acceso a contenidos pornográficos, las deficiencias son aún más evidentes. A pesar de la protección adicional que ofrece el RGPD (p. ej. su art. 8) y la prohibición de explotación de vulnerabilidades vinculadas a la edad establecida en el RIA, los sistemas de control de acceso son ineficaces y fácilmente eludibles. La falta de mecanismos complejos para verificar la edad, junto con la ausencia de una educación digital y afectivo-sexual adecuada, incrementan el impacto de riesgos graves como la distorsión de la percepción de la sexualidad, la normalización de la violencia o la exposición a contenidos que pueden afectar negativamente al desarrollo personal de cada persona menor.

En vista de lo anteriormente expuesto, puede concluirse que los reglamentos estudiados proporcionan un marco normativo sólido con un enfoque adecuado para reforzar la protección de la infancia en el entorno digital. Sin embargo, su efectividad depende en gran medida de la implementación práctica coherente, de la existencia de herramientas técnicas adecuadas y, esencialmente, del compromiso por parte de las plataformas digitales, las autoridades públicas y los entornos educativos. Por tanto, para garantizar una protección real, resulta esencial una aplicación coordinada, una supervisión continua y la promoción de una cultura digital basada en el uso ético y responsable de la tecnología.

4. REFERENCIAS BIBLIOGRÁFICAS

Legislación

Carta de los Derechos Fundamentales de la Unión Europea, Diario Oficial de la Unión Europea (2012).

Convención sobre los Derechos del Niño (1989). Asamblea General de las Naciones Unidas.

Convenio n.º 108 del Consejo de Europa (1981).

Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, Diario Oficial de la Unión Europea (2022).

Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (…), Diario Oficial de la Unión Europea (2014).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (…), Diario Oficial de la Unión Europea (2016).

Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 (…), Diario Oficial de la Unión Europea (2024).

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (…), Diario Oficial de la Unión Europea (2024).

Tratado de Funcionamiento de la Unión Europea, Diario Oficial de la Unión Europea (2012).

Tratado de la Unión Europea, Diario Oficial de la Unión Europea (2012).

Jurisprudencia

Sentencia de 9 de noviembre de 2010 del Tribunal de Justicia de la Unión Europea, *Caso Volker und Markus Schecke GbR y otros contra Land Hessen*, sección 48. ECLI:EU:C:2010:662

Sentencia de 13 de mayo de 2014 del Tribunal de Justicia de la Unión Europea, *Caso Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*. Asunto C-131/12. ECLI:EU:C:2014:317

Sentencia de 16 de julio de 2020 del Tribunal de Justicia de la Unión Europea*, Caso Data Protection Commissioner contra Maximillian Schrems y Facebook Ireland.* Asunto C-311/2018.

Artículos, obras y textos jurídicos

Blasi Casagran, C., & Cañabate Pérez, J. (2024). *Legislación y derecho digital para no juristas*. Universitat Autònoma de Barcelona, Servei de Publicacions.

Faggiani, V. (2018). Derechos del menor e internet. Una aproximación desde el derecho constitucional europeo. F. J. Durán Ruiz (Dir.), *Desafíos de la protección de menores en la sociedad digital,* (pp. 21-53). Tirant Lo Blanch.

Hernández López, J. M. (2018). *Reglamento General de Protección de Datos*. Tirant Lo Blanch.

Jiménez Jiménez, N. (2023). Privacidad y datos personales. E. Velasco Núñez (Dir.), *Marco normativo de la UE para la transformación digital* (pp. 481-510). La Ley.

López Calvo, J. (2017). *Comentarios al Reglamento Europeo de Protección de Datos.* Sepín.

Observatori per a la Igualtat de la UAB & Servei de Llengües de la UAB. (2011). *Guia per a l'ús no sexista del llenguatge a la Universitat Autònoma de Barcelona*. Universitat Autònoma de Barcelona.

Piñar Mañas, J. L. (2016). Introducción. Hacia un nuevo modelo europeo de protección de datos. *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad,* (pp. 15-20). Editorial Reus.

Piñar Mañas, J. L. (2017). *Reglamento general de protección de datos*. Editorial Reus.

Piñar Mañas, J. L., & Recio Gayo, M. (2018). *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*. Wolters Kluwer.

Páginas web

Abril Marti, P. & Maciejewski, M. (2024, Mayo). *La protección de los datos personales*. Fichas temáticas sobre la Unión Europea. https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

Agencia Española de Protección de Datos. (2023, Diciembre 14). *La AEPD presenta un sistema de verificación de edad para proteger a los menores de edad ante el acceso a contenidos de adultos en Internet.* Agencia Española de Protección de Datos. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-presenta-sistema-verificacion-edad-para-proteger-a-menores-de-edad

Agencia Española de Protección de Datos. (2025, Enero 24). *eIDAS2, la cartera europea de identidad digital y el RGPD (I).* Agencia Española de Protección de Datos. https://www.aepd.es/prensa-y-comunicacion/blog/eldas2-la-cartera-europea-de-identidad-digital-y-el-rgpd-i

Canal Sur Media. (2023, Noviembre 23). *La pornografía se convierte en la principal fuente de información sexual para los adolescentes*. Canal Sur, Radio y Televisión. https://www.canalsur.es/noticias/andalucia/la-pornografia-se-convierte-en-la-principal-fuente-de-informacion-sexual-para-los-adolescentes/1987191.html

Castro, S. (2025, Febrero 24). *El 60% de los adolescentes sabe sortear el control parental en el entorno digital.* El País. https://elpais.com/sociedad/2025-02-24/el-60-de-los-adolescentes-sabe-sortear-el-control-parental-en-el-entorno-digital.html

Conceptos Jurídicos. (s.f.). *Libertad sexual.* Conceptos Jurídicos. https://www.conceptosjuridicos.com/libertad-sexual/

Dharma Consulting. (2023, Julio 26). *Entendiendo los riesgos del proyecto: La matriz de probabilidad e impacto*. Dharmacon. https://dharmacon.net/2023/07/26/entendiendo-los-riesgos-del-proyecto-la-matriz-de-probabilidad-e-impacto/

Educo. (2025, Enero 27). *Las 8 cosas que debes saber sobre la protección de datos de menores de edad.* Educo. https://www.educo.org/blog/8-cosas-debes-saber-sobre-proteccion-menores

Escuela Internacional de Mediación. (2023, Enero 17). *El consumo de pornografía en adolescentes.* Escuela Internacional de Mediación. https://eimediacion.edu.es/noticias-eim-menores/el-consumo-de-pornografia-en-adolescentes/

Escuela Internacional de Mediación. (2024, Febrero 5). *Consecuencias del acceso de menores a contenidos pornográficos.* Escuela Internacional de Mediación. https://eimediacion.edu.es/noticias-eim-menores/cuidado-menores-educacion/

European Comission. (s.f.). *Better Internet for Kids.* European Union. https://better-internet-for-kids.europa.eu/en/bik

European Commission. (2022, Junio 21). *Child-friendly version of the European strategy for a better internet for kids (BIK+).* European Commission. https://digital-strategy.ec.europa.eu/en/library/child-friendly-version-european-strategy-better-internet-kids-bik

European Commission. (s.f.). *Legal framework of EU data protection.* European Commission. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en?prefLang=es

Federation of Catholic Family Associations in Europe, FAFCE. (2022, Mayo 24). *The EU strategy for a Better Internet for Children recognises online pornography as a risk for children.* https://www.fafce.org/the-eu-strategy-for-a-better-internet-for-children-finally-recognises-online-pornography-as-a-risk-for-children/

Guadix García, N. (2023, Febrero 11). *Día de Internet Segura*. UNICEF. https://www.unicef.es/blog/educacion/dia-internet-segura-consejos-para-padres

Instagram. (2022, Junio 6). *Actualización del control de contenido delicado.* Instagram. https://about.instagram.com/es-la/blog/announcements/updates-to-the-sensitive-content-control

Instagram. (2024, Septiembre 17). *Instagram presenta las cuentas para adolescentes: protecciones integradas para los adolescentes y tranquilidad para los padres*. Instagram. https://about.instagram.com/es-la/blog/announcements/instagram-teen-accounts

Instituto Nacional de Ciberseguridad de España. (2017, Marzo 20). *Amenaza vs. vulnerabilidad: ¿Sabes en qué se diferencian?* INCIBE https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Instituto Nacional de Ciberseguridad de España. (2021, Julio 19). *Los menores y el acceso a contenido sexual en línea.* INCIBE https://www.incibe.es/menores/blog/los-menores-y-el-acceso-contenido-sexual-en-linea

Instituto Nacional de Ciberseguridad de España. (s. f.). *Privacidad*. INCIBE. https://www.incibe.es/menores/tematicas/privacidad

Intastur Instituto terapéutico. (s. f.). *Adicción al contenido adulto en adolescentes.* Intastur. https://www.intastur.es/adiccion-al-contenido-adulto-en-adolescentes

Meta. (2024, Septiembre 17). *Presentamos las cuentas de Instagram para adolescentes: protecciones integradas para los adolescentes y tranquilidad para los padres*. Meta. https://about.fb.com/ltam/news/2024/09/presentamos-las-cuentas-de-instagram-para-adolescentes-protecciones-integradas-para-los-adolescentes-y-tranquilidad-para-los-padres/

Ministerio de la Presidencia, Justicia y Relaciones con las Cortes. (2024, Enero 16). *El Gobierno impulsa la protección de menores frente al acceso a pornografía en internet.* https://www.mjusticia.gob.es/es/institucional/gabinete-comunicacion/noticias-ministerio/Gobierno-impulsa-proteccion-menores-pornografiaografía-en-internet

Ministerio para la Transformación Digital y de la Función Pública. (s.f.). *Preguntas frecuentes sobre el Reglamento (UE) Nº 910/2014 sobre identificación electrónica y servicios de confianza (eIDAS)*. Avance Digital. https://avance.digital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/preguntas-frecuentes.aspx

Palenzuela Paniagua, S. M., Leal Helmling, J., & Jiménez Pulido, I. (2024, Diciembre 30). *Hablemos de pornografía en los adolescentes.* Revista de la Sociedad Andaluza de Medicina Familiar y Comunitaria (SAMFyC). https://www.samfyc.es/revista/hablemos-de-pornografia-en-los-adolescentes/

Parlamento Europeo Think Tank. (2022, Junio 7). *European declaration on digital rights and principles.* Parlamento Europeo. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282022%29733518

PornHub. (s.f.). *PornHub*. https://es.pornhub.com

Safety Culture. (2025, Febrero 4). *Matriz de riesgo*. SafetyCulture. https://safetyculture.com/es/temas/evaluacion-de-riesgos/matriz-de-riesgo/

Setién, M. (2017, Mayo 11). *La mayoría de los menores no son conscientes de los riesgos de Internet.* ABC. https://www.abc.es/familia/educacion/abci-mayoria-menores-no-conscientes-riesgos-internet-201705111609_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Ffamilia%2Feducacion%2Fabci-mayoria-menores-no-conscientes-riesgos-internet-201705111609_noticia.html

Stanford Medicine Children's Health. (s. f.). *Desarrollo cognitivo en la adolescencia*. Stanford Medicine Children's Health. https://www.stanfordchildrens.org/es/topic/default?id=cognitive-development-in-adolescence-90-P04694

Team Asana. (2025, Febrero 3). *Riesgos del proyecto*. Asana. https://asana.com/es/resources/project-risks

UNESCO. (2023, Septiembre 27). *Educación integral en sexualidad: Para educandos sanos, informados y empoderados.* UNESCO. https://www.unesco.org/es/health-education/cse

UNICEF Comité Español. (2024, Abril 17). *Ciberacoso: Qué es, impacto y cómo detenerlo.* UNICEF.https://www.unicef.es/blog/educacion/ciberacoso-que-es-impacto-y-como-detenerlo

Documentos en PDF

Agencia Española de Protección de Datos. (2021, Junio). *Guía sobre la gestión del riesgo y la evaluación de impacto en tratamientos de datos personales.* Agencia Española de Protección de Datos. [Documento en PDF]. https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Agencia Española de Protección de Datos. (2021, Junio). *Relación de tablas de apoyo para la gestión del riesgo y la evaluación de impacto en protección de datos (EIPD).* Agencia Española de Protección de Datos. [Documento en PDF]. https://www.aepd.es/documento/relacion-tablas-guia-riesgo-eipd-tablas.odt

Agencia Española de Protección de Datos. (2023, Diciembre). *Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos inadecuados.* [Documento en PDF]. https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf

Agencia Española de Protección de Datos. (2024, Octubre). *Nota técnica. Internet seguro por defecto para la infancia y el papel de la de verificación de edad.* Agencia Española de Protección de Datos. [Documento en PDF]. https://www.aepd.es/guias/nota-tecnica-internet-seguro-por-defecto-para-la-infancia.pdf

Autoritat Catalana de Protecció de Dades. (2024, Junio). *Evaluación de impacto relativa a la protección de datos.* Autoritat Catalana de Protecció de Dades. [Documento en PDF]. https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-EIPD.pdf

Dale Una Vuelta, Fundación Colegio Oficial de la Psicología de Madrid y Agencia Española de Protección de Datos. (s.f.). *El impacto de la pornografía en menores.* [Infografía en PDF]. https://www.daleunavuelta.org/wp-content/uploads/2024/10/impacto_pornografia_menores.pdf

European Commission. (2022, Junio 21). *Child-friendly leaflet BIK+* Publications Office of the European Union. [Folleto en PDF]. https://digital-strategy.ec.europa.eu/en/library/child-friendly-version-european-strategy-better-internet-kids-bik

Save The Children. (2020, Septiembre 22). *(Des)información sexual: pornografía y adolescencia.* Save The Children. [Documento en PDF]. https://www.savethechildren.es/informe-desinformacion-sexual-pornografia-y-adolescencia

SEDRA - Federación de Planificación Familiar. (2022, Febrero). *Impacto de la pornografía en la sexualidad de las personas jóvenes de Castilla-La Mancha.* [Documento en PDF]. https://institutomujer.castillalamancha.es/sites/institutomujer.castillalamancha.es/files/documentos/paginas/archivos/1_impacto_de_la_pornografria_en_personas_jovnes.pdf

UNICEF. (2017, Diciembre). *THE STATE OF THE WORLD'S CHILDREN 2017 - Children in a Digital World.* [Documento en PDF]. https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf