Informe 1

Análisis del marco normativo y marco político sobre la protección de la infancia en la sociedad digital

Pablo Rivera-Vargas, Ainara Moreno-González y Judith Jacovkis (coord.)

Enero 2025

DigiProtEd

Listado completo de autores/as de cada apartado por orden alfabético (apartados)

Mercedes Blanco-Navarro (1.1, 1.3 y 2.1)
Gustavo Herrera-Urízar (1.4 y 2.3)
Carmen Lloret (1.4 y 2.4)
Carles Lindín (1.4 y 2.1)
Pedro Mellado (2.2)
Ainara Moreno-González (Introducción, metodología, 1.1, 1.3, 2.2 y conclusiones)
Carlos Navia Canales (1.5 y 2.3)
Lluís Parcerisa (1.5)
Francisco Ramos Pardo (1.5 y 2.3)
Pablo Rivera-Vargas (Introducción, metodología, 1.1, 1.2, 2.4 y conclusiones)
Norma Rodríguez de Segovia (1.1, 1.2 y 2.4)
Pablo Sánchez Antolín (1.3 y 2.1)
Cristóbal Suárez Guerrero (1.3 y 2.2)

Cómo citar este documento: Rivera-Vargas, P., Moreno-González, A., y Jacovkis, J. (2025). *Análisis del marco normativo y marco político sobre la protección de la infancia en la sociedad digital*. *DIGIPROTED.* Esbrina. Recuperado de: https://esbrina.eu/es/2024/02/06/plataformas-digitales-y-datificacion-en-la-educacion-primaria-en-espana-la-proteccion-de-la-infancia-en-un-contexto-de-digitalizacion-educativa-digiproted-2/

Este documento es parte del proyecto Plataformas digitales y datificación en la educación primaria en España: la protección de la infancia en un contexto de digitalización educativa (DigiProtEd), en el que participan las siguientes universidades:

Proyecto PID2022-137033NA-I00 financiado por MCIN/AEI /10.13039/501100011033/ y por FEDER Una manera de hacer Europa

Índice

Introducción

En los últimos años, el ámbito educativo ha experimentado cambios significativos debido a la aceleración forzada de la digitalización en las escuelas a raíz de la pandemia mundial de COVID-19, planteando nuevos retos para la comunidad educativa e impactando en la forma en la que vemos y entendemos la tecnología (Castañeda et al., 2020). En este contexto, y con el propósito de asegurar la continuidad de la educación y fomentar el desarrollo de la enseñanza digital, se decidió incorporar a grandes empresas tecnológicas, en el ámbito educativo, como proveedoras de servicios, herramientas y recursos.

La inclusión de tecnologías digitales, especialmente las plataformas utilizadas en los procesos de enseñanza y aprendizaje, representa un reto para los sistemas educativos a nivel global, especialmente en lo que respecta a la protección de la infancia en estos nuevos entornos sociodigitales. En los últimos años, algunas investigaciones han empezado a indagar en los efectos de la digitalización de la infancia sobre su protección en estos espacios, abordando temas como la privacidad o la protección de los datos (Pangrazio & Selwyn, 2020; Perrotta et al., 2021; Parcerisa et al., 2022); o la capacidad de las grandes Corporaciones Tecnológicas para monitorear el comportamiento en línea de las personas usuarias y, posteriormente, modelar las propias plataformas en función de esto (Yeung, 2018).

Asimismo, estas evidencias se complementan con informes de otros organismos de carácter internacional que señalan la necesidad de salvaguardar la protección de la infancia en la sociedad digital. En este sentido, la Relatora Especial sobre el derecho a la educación de la ONU, Boly Barry (2022) establece el derecho a la privacidad y la protección de los datos personales de la infancia como una condición indispensable a la hora de garantizar su desarrollo, autonomía y dignidad.

En este escenario, surge el proyecto *"Plataformas digitales y datificación en la educación primaria en España: la protección de la infancia en un contexto de digitalización educativa (DigiProtEd)*" (MICIN, PID2022-137033NA-I00) que pretende explorar y analizar los efectos socioeducativos de la utilización de las plataformas digitales, y del almacenamiento y gestión de datos, sobre la protección de la infancia en la educación primaria en España. El proyecto se divide en 4 fases; este informe recoge los resultados de la revisión de normativas y políticas correspondiente a la primera de las fases.

El objetivo de esta fase ha sido **identificar y analizar las políticas y normativas europeas, españolas y autonómicas sobre la protección de la infancia en contextos digitales**, abordando algunas preguntas como las que se plantean a continuación:

- ¿Cuáles son la principales normativas y políticas establecidas en el contexto internacional, europeo, estatal y autonómico sobre la protección de la infancia en la sociedad digital?

- ¿Cuáles son los principales actores involucrados, según las normativas y políticas, en la protección de la infancia en la sociedad digital?
- ¿Cuáles son los roles de cada uno de estos actores?
- ¿Los marcos normativos y políticos siguen una misma línea?

A partir de esta introducción, el informe se ha organizado de la siguiente manera. En primera instancia, se exponen las principales características del diseño metodológico que se ha llevado a cabo. Posteriormente se presentan los resultados en dos bloques. En el primero se describe el rol de los actores relevantes en la protección de la infancia en la sociedad digital. En el segundo se plantean algunos interrogantes orientados a favorecer la comprensión de la articulación de los documentos normativos y políticos en relación con la protección de la infancia en la sociedad digital. Por último, se exponen las principales conclusiones del trabajo.

Metodología

A partir de lo anterior, se ha llevado a cabo un estudio de corte cualitativo basado en un análisis documental de un total de 30 documentos normativos y políticos. Esta estrategia posibilita la obtención de información retrospectiva y referencial sobre la situación o fenómeno de estudio, mediante el análisis de documentos de diferentes índoles, entre ellos los normativos y políticos (Massot et al., 2009). En especial, este tipo de análisis sirve como punto de partida y herramienta de contraste para complementar y/o validar la información recopilada a través de otras técnicas (Latorre et al., 1996).

Los documentos han sido seleccionados de forma intencional en función de su capacidad para responder al objetivo señalado anteriormente. Para ello, inicialmente se incluyeron los documentos que ya analizamos en una experiencia investigativa previa, el proyecto *edDIT*[1] (Rivera-Vargas et al., 2023). Seguidamente, se complementó el listado con las recomendaciones del equipo investigativo del proyecto *DigiProtEd* y de personas expertas vinculadas al ámbito de derechos digitales y derecho a la educación.

El listado final de documentos que abordan la protección de la infancia en la sociedad digital incluye un total de 15 textos relacionados con el marco político y 15 con el marco normativo. Al mismo tiempo, este listado considera distintos niveles de representación o incidencia: internacional, europeo, estatal y autonómico (Catalunya, Comunitat Valenciana y Castilla-La Mancha). Cabe destacar que este listado no es en ningún caso una agrupación exhaustiva y definitiva de textos sobre el ámbito digital y los derechos de la infancia. Más bien, estos documentos se han considerado apropiados para la ejecución de esta fase de DigiProtEd, sin que esto conlleve o niegue la existencia de otros textos normativos y políticos relevantes que podrían ser también incluidos en un trabajo como el que aquí se ha desarrollado.

A continuación, en las tablas 1 y 2 se muestra el listado y la caracterización de los documentos de ambos tipos. Aquí se incluyen 5 descriptores generales: identificador, nombre, año, contexto y enlace.

Tabla 1

Listado y caracterización de los documentos políticos

Identificador	Nombre del documento	Año	Contexto	Enlace
MP1	Observación General nº25 (Naciones Unidas)	2021	Global	Enlace
MP2	Observación General nº13 relativa al Derecho a la Educación (Naciones Unidas)	1999	Global	Enlace
MP3	Repercusiones de la digitalización de la educación en el derecho a la educación. Informe de la relatora Especial sobre el derecho a la	2022	Global	Enlace

[1] Ver aquí informe del proyecto edDIT: Informe-edDIT_CASTELLA_web.pdf (affac.cat)

	educación, Koumbou Boly Barry (Naciones Unidas)			
MP4	Convenio para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Council of Europe)	1981	Europa	Enlace
MP5	Declaración Europea sobre los derechos y Principios Digitales para la Década Digital	2022	Europa	Enlace
MP6	Plan de acción de educación digital 2021-2027 (Comisión Europea)	2020	Europa	Enlace
MP7	Propuesta de resolución del Parlamento Europeo, Informe sobre la formulación de la política de educación digital (Parlamento Europeo)	2021	Europa	Enlace
MP8	Plan de Recuperación, Transformación y Resiliencia. Componente 21: Modernización y digitalización del sistema educativo, incluida la educación temprana de 0-3 años (Gobierno de España)	2021	España	Enlace
MP9	Pacto de Estado. Protegiendo a la infancia y la adolescencia en el entorno digital (Gobierno de España)	2023	España	Enlace
MP10	España Digital 2026 (Gobierno de España)	-	España	Enlace
MP11	Menores, salud digital y privacidad (AEPD). Estrategia y líneas de acción (Gobierno de España)	2024	España	Enlace
MP12	Plan de Recuperación, Transformación y Resiliencia. Componente 19. Plan Nacional de Capacidades Digitales (Gobierno de España)	2023	España	Enlace
MP13	Carta catalana por los derechos y las responsabilidades digitales (Generalitat de Catalunya)	2019	Catalunya	Enlace
MP14	Pla d'educació digital de Catalunya 2020-2023 (Generalitat de Catalunya)	2020	Catalunya	Enlace
MP15	Decreto 55/2023, de 6 de junio, por el que se establece la política de protección de datos en la Administración de la Junta de Comunidades de Castilla-La Mancha. [2023/5190] (Gobierno de Castilla y la Mancha)	2023	Castilla-La Mancha	Enlace

Fuente: Elaboración propia

Tabla 2

Listado y caracterización de los documentos normativos

Identificador	Nombre del documento	Año	Contexto	Enlace
MN1	Directiva 2002/58/CE del Parlamento europeo y del consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directivas sobre la privacidad y las comunicaciones electrónicas) (Unión Europea)	2002	Europa	Enlace
MN2	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 y por el que se	2016	Europa	Enlace

	deroga la Directiva 95/46/CE (Reglamento general de protección de datos)			
MN3	Resolución de 7 de julio de 2020, para la ejecución del programa "educa en Digital"	2020	España	Enlace
MN4	Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia	2021	España	Enlace
MN5	Informe sobre el uso seguro y respetuoso de los medios digitales en el currículo básico	2019	España	Enlace
MN6	Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos Personales y garantía de los derechos digitales	2018	España	Enlace
MN7	Carta derechos digitales (Gobierno de España)	2021	España	Enlace
MN8	Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos	2010	Cataluña	Enlace
MN9	Ley 7/2023, de 10 de marzo, de Atención y Protección a la Infancia y la Adolescencia de Castilla-La Mancha	2023	Castilla-La Mancha	Enlace
MN10	Orden 178/2022, de 14 de septiembre, de la Consejería de Educación, Cultura y Deportes, por la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios. (2022/8545)	2022	Castilla-La Mancha	Enlace
MN11	Resolución de 28 de junio de 2018, de la Subsecretaría de la Conselleria de Educación, Investigación, Cultura y Deporte, por la que se dictan instrucciones para el cumplimiento de la normativa de protección de datos en los centros educativos públicos de titularidad de la Generalitat. [2018/11040]	2018	Valencia	Enlace
MN12	Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación	2020	España	Enlace
MN13	Ley 7/2010, de 20 de julio, de Educación de Castilla-La Mancha	2010	Castilla-La Mancha	Enlace
MN14	LLEI 12/2009, del 10 de juliol, d'educació	2009	Cataluña	Enlace
MN15	LEY 26/2018, de 21 de diciembre, de la Generalitat, de derechos y garantías de la Infancia y la adolescencia [2018/12057]	2018	Valencia	Enlace

Fuente: Elaboración propia

Tras el establecimiento del listado definitivo de textos, se inició el proceso de vaciado y análisis de los mismos.

En primer lugar, se procedió al vaciado y clasificación de toda la información extraída de los documentos consultados en base a dimensiones y categorías específicas (según corresponda). Para ello, se elaboró una planilla en Excel separando los documentos normativos de los textos de carácter político[2]. Respecto al marco político, toda la información se organizó y analizó en base a las dimensiones y categorías que se muestran en la tabla 3. En relación con los textos del marco normativo, se llevó a cabo el mismo procedimiento en base a las dimensiones que

[2] Ver aquí planilla para el vaciado y análisis de los documentos: Instrumento Análisis MN_MP.xlsx (sharepoint.com) Esta planilla es la base de las tablas 1 y 2.

se presentan en la tabla 4. En ambos casos, tanto las dimensiones como las categorías de análisis se establecieron en función de los objetivos del proyecto y de manera consensuada con el equipo investigativo.

Tabla 3

Dimensiones y categorías de análisis del marco político

Dimensiones	Categorías
1. Proceso de plataformización	Definición Otras tecnologías digitales Actores involucrados Acciones de la Administración Pública Rol de la escuela Financiamiento Códigos emergentes
2. Datificación	Definición Actores involucrados Acciones de la Administración Pública Rol de la escuela Financiamiento Códigos emergentes
3. Derecho a la educación digital y protección de la infancia	Garantías del derecho a la educación Equidad digital Estrategias de regulación de uso de las TD en la escuela Protección de la identidad digital y la privacidad de la infancia Responsabilidad digital de las figuras de referencia y la Administración Pública Competencia digital de las figuras de referencia y la Administración Pública Códigos emergentes
4. Docencia	Prácticas docentes mediadas por PD o TD Formación docente Libertad docente Códigos emergentes
5. Corporaciones Tecnológicas	Responsabilidad de la empresa en la garantía del derecho a la educación y la protección de la infancia Vínculo de las empresas tecnológicas con el sistema educativo Códigos emergentes

Fuente: Elaboración propia

Tabla 4

Dimensiones de análisis del marco normativo

Dimensiones
1. Plataformas digitales
2. Otras tecnologías digitales
3. Datificación
4. Derecho a la educación digital
5. Protección de la infancia

6.	Administración Pública
7.	Corporaciones Tecnológicas
8.	Escuela
9.	Docentes
10.	Familias
11.	Otros actores
12.	Otros aspectos emergentes

Fuente: Elaboración propia

En segundo lugar, y tras realizar el primer vaciado de todos los textos en las plantillas de análisis, se diseñaron dos tablas dinámicas Excel con toda la información recogida en esta fase[3]. Posteriormente, con la finalidad de identificar el mapa de actores y al mismo tiempo, diseñar un esquema de presentación de los resultados, se incorporaron los datos al software de análisis cualitativo Atlas.ti.

A partir de aquí, a continuación, se presentan en dos bloques los principales resultados obtenidos tras el desarrollo de esta fase de trabajo investigativo:

1. Identificación y descripción de roles y responsabilidades de los diferentes actores sociales en relación con la protección de la infancia en la sociedad digital.
2. Preguntas orientativas del equipo de investigación a los documentos analizados: relación entre los diferentes marcos y territorios consultados y coherencia entre las responsabilidades de los diferentes actores.

Referencias

Castañeda, L., Salinas, J., & Adell-Segura, J. (2020). Hacia una visión contemporánea de la Tecnología Educativa. *Digital Education Review*, 37, 240-268. https://doi.org/10.1344/der.2020.37.240-268

Latorre, A., Del Rincón, D., & Arnal, J. (1996). *Bases Metodológicas de la Investigación Educativ*a. Hurtado Ediciones.

Massot, I., Dorio, I., & Sabariego, M. (2009). Estrategias de análisis y recogida de información. En R. Bisquerra, (Ed.), *Metodología de la investigación educativa* (pp. 330-366). La muralla.

Pangrazio, L., & Selwyn, N. (2020) Towards a school-based critical data education. *Pedagogy, Culture & Society,* 1–18. https://doi.org/10.1080/14681366.2020.1747527

Parcerisa, L., Jacovkis, J., Rivera-Vargas, P., & Herrera-Urízar, G. (2022). Corporaciones tecnológicas, plataformas digitales y privacidad: comparando los discursos sobre la

[3] Ver aquí tabla dinámica marco político: Marco Político-Tablas.xlsx (sharepoint.com)
Ver aquí tabla dinámica marco normativo: Marco_Normativo_tablas.xlsx (sharepoint.com)

entrada de las BigTech en la educación pública. *Revista Española de Educación Comparada,* 42, 221-239. https://doi.org/10.5944/reec.42.2023.34417

Perrotta, C., Gulson, K. N., Williamson, B., & Witzenberger, K. (2021). Automation, APIs and the distributed labour of platform pedagogies in Google Classroom. *Critical Studies in Education, 62*(1), 97-113. https://doi.org/10.1080/17508487.2020.1855597

Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/3XVI7GV

Rivera-Vargas, P., Jacovkis, J., Herrera-Urízar, G., Calderón-Garrido, D., Miño-Puigcercós, R., Parcerisa, L., Folguera, S., Moreno, A., Massot, B., Passerón, E., Alonso, C., Gasull-Figueras, L., & Rilo-Borredà, C. (2023). *Plataformas digitales BigTech del sistema educativo catalán y derechos de la infancia: amenazas y retos*. Informe final proyecto edDIT *"Corporacions tecnològiques, plataformes educatives digitals i garantia dels drets de la infància amb enfocament de gènere"*, aFFaC y Esbrina Recerca Universitat de Barcelona. http://hdl.handle.net/2445/192941

Yeung, K. (2018). Five Fears about Mass Predictive Personalisation in an Age of Surveillance Capitalism. *International Data Privacy Law,* 8, 258-269. https://doi.org/10.1093/idpl/ipy020

1. Primera parte. Actores, responsabilidades y acciones para la protección de la infancia en la sociedad digital

A lo largo de este apartado, y atendiendo al contenido de los documentos analizados, se presentan los principales actores implicados en la protección de la infancia en la sociedad digital, así como su rol y responsabilidades asociados a esta tarea. El primer apartado presenta la identificación de los actores presentes en el conjunto de documentos analizados, así como de las relaciones existentes entre ellos. Los siguientes apartados, exponen los roles y responsabilidades de cada uno de los actores identificados en los textos analizados.

1.1. Mapa de actores en torno a la protección de la infancia en la sociedad digital

El presente apartado ofrece un mapa de actores relevantes vinculados a la protección de la infancia en la sociedad digital. No se trata, por tanto, de un mapeo exhaustivo, sino más bien de una aproximación que ha sido generada a partir de la información que aparece en el listado de los 30 textos normativos y políticos seleccionados y analizados en esta fase del proyecto.

En el análisis de estos documentos se han identificado organismos gubernamentales, organizaciones no gubernamentales, instituciones educativas, Corporaciones Tecnológicas y otros agentes relevantes. La pluralidad de estos actores resalta la naturaleza multidimensional de la protección infantil en el entorno digital, subrayando la necesidad de un enfoque coordinado y colaborativo.

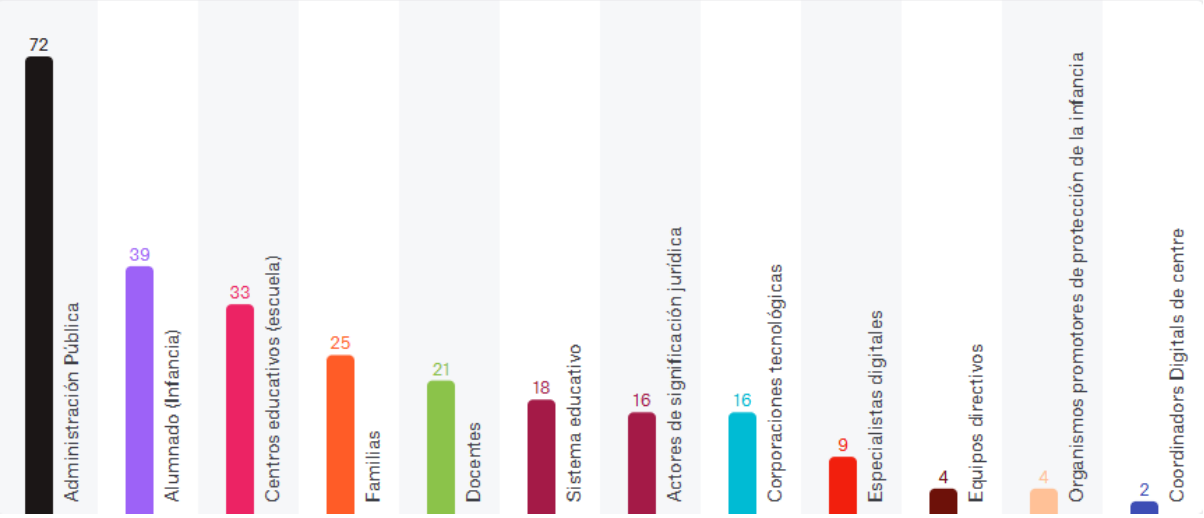

Figura 1. Actores identificados y frecuencia de aparición extraído del análisis en Atlas.ti

En la figura 1 se presenta un gráfico de barras en el que se muestran los 12 actores identificados, además del número total de menciones a cada uno de estos en los 30 documentos analizados. Para el desarrollo de los siguientes apartados de esta primera parte del informe agrupamos a este número total de actores en 4 grandes bloques:

- Administración Pública: Administración Pública con 72 menciones y Sistema educativo con 18 menciones.
- Escuela: Centros educativos con 33 menciones, alumnado con 39 menciones, familias con 25 menciones, docentes con 21 menciones, equipos directivos con 4 menciones, y coordinación digital del centro con 2 menciones.
- Corporaciones Tecnológicas: 16 menciones.
- Otros actores con significación jurídica: 16 menciones.

En cuanto a las relaciones entre los actores, la figura 2 es un Mapa-Red que profundiza en las interacciones entre ellos, mostrando de manera visual cómo se conectan en la práctica. Esta representación permite identificar nodos clave, donde algunos actores, como la Administración Pública, el Sistema Educativo, las Familias y los Centros Educativos, desempeñan un papel central y poseen múltiples conexiones, lo que refleja su importancia en la protección de la infancia en el ámbito digital.

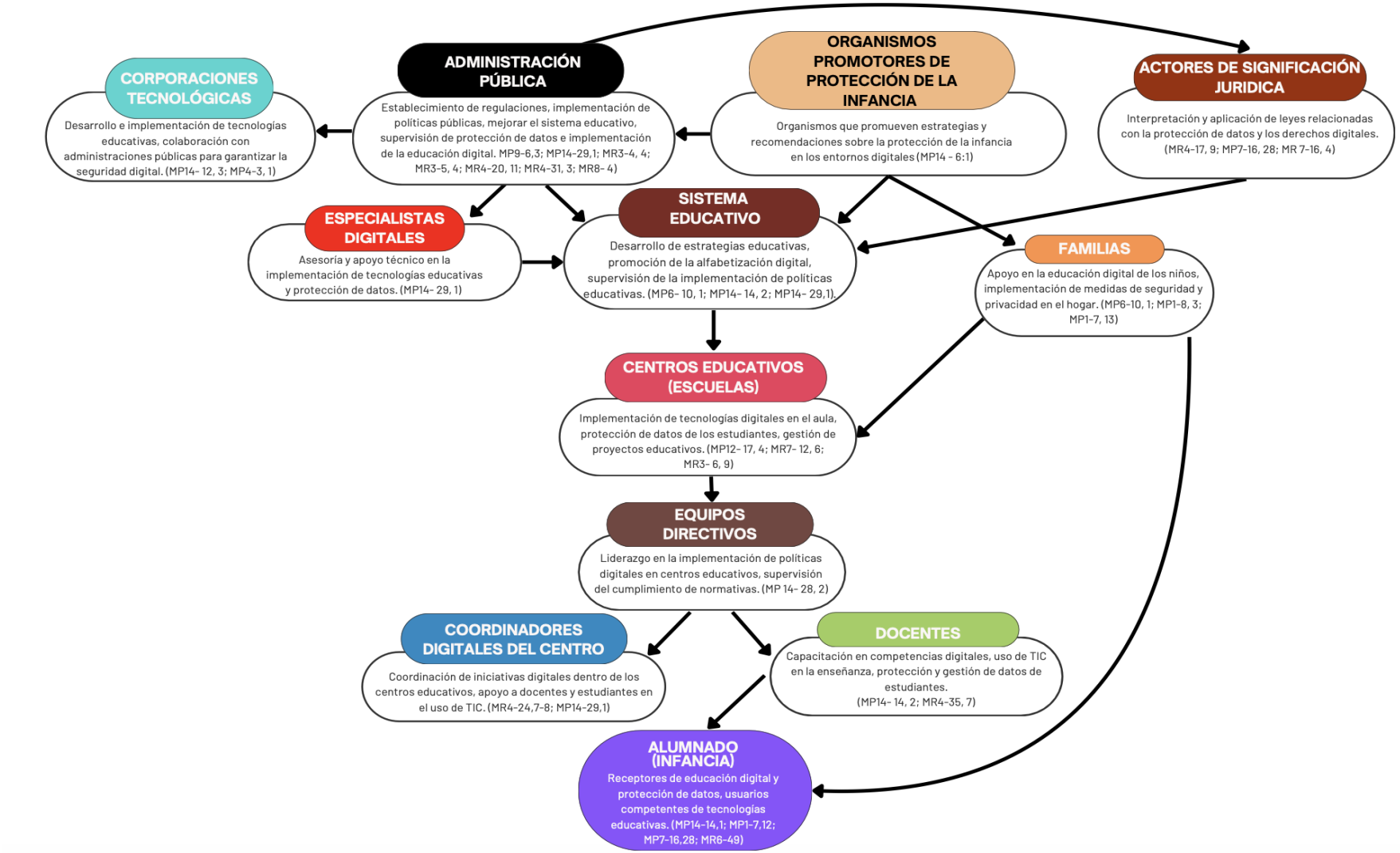

Figura 2. Mapa-Red de actores creado a través del análisis con Atlas.ti

El Mapa-Red de actores, por tanto, proporciona una aproximación a los principales roles y relaciones funcionales de los actores identificados a partir del análisis de los textos. Este mapa no pretende establecer jerarquías definitivas, sino ofrecer al lector de este documento una herramienta que facilite la comprensión de la distribución de responsabilidades y conexiones entre los actores.

En síntesis, más allá de simplemente listar actores y sus roles, es esencial considerar cómo se relacionan y analizar hasta qué punto forman una red de colaboración e influencia mutua. Los actores como la Administración Pública, el Sistema Educativo, las Familias y las Corporaciones Tecnológicas no actúan de manera aislada; sus interacciones configuran un ecosistema dinámico en el que la coordinación y el intercambio de responsabilidades resultan fundamentales para garantizar la protección infantil efectiva en el entorno digital.

1.2. La Administración Pública en relación con la protección de la infancia en entornos digitales

De acuerdo con la Ley 40/2015[4] (España, 2015) en su artículo 3, "las Administraciones Públicas tienen la responsabilidad de servir con objetividad los intereses generales, actuando bajo los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, siempre en pleno sometimiento a la Constitución, la ley y el derecho" (España, 2015; 7). Además, el artículo 2 de la misma Ley establece que el sector público en España incluye "la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las entidades que integran la Administración Local y el sector público institucional" (España, 2015: p. 6). Por lo tanto, entendemos por Administración Pública al conjunto de organismos del sector público encargados de servir con objetividad los intereses generales, bajo los principios de eficacia, jerarquía, descentralización y coordinación, siempre en cumplimiento del marco jurídico.

Situados en este régimen jurídico, se desprende que la Administración Pública juega un rol determinante en el diseño e implementación de políticas públicas, sociales y educativas para toda la población, incluyendo aquellas destinadas a fortalecer la protección de la infancia en la sociedad digital.

Según la información recopilada y analizada de los documentos seleccionados (MP1; MP3; MP8; MP10; MP12; MP13; MP14; MP15; MN3; MN4; MN5; MN6; MN7; MN8; MN9; MN10; MN11; MN12), la principal responsabilidad de la Administración Pública es garantizar un entorno digital seguro y adecuado para el desarrollo integral de niños y niñas. Esto implicaría el diseño y la implementación efectiva de legislaciones y políticas que regulen el acceso y uso de tecnologías digitales, protegiendo a la infancia de contenidos nocivos y de riesgos como el ciberacoso y la exposición a la violencia. Paralelamente, implicaría el fomento de la alfabetización digital entre niños, niñas y jóvenes, empoderándoles para que utilicen las tecnologías de manera consciente y crítica, y facilitando su crecimiento en tanto parte de una ciudadanía digital plena y activa (MN3; MN5).

A continuación, y a partir del análisis de los documentos seleccionados, presentamos seis de las principales líneas de acción (responsabilidades) de la Administración Pública en cuanto a la protección de la infancia en la sociedad digital. Cada línea de acción responde a las necesidades prioritarias detectadas en el análisis y aborda distintos aspectos clave en estos ámbitos[5]:

- Garantía del Derecho a la Educación Digital
- Dotación de recursos para la digitalización de la educación

[4] De 1 de octubre, de Régimen Jurídico del Sector Público.

[5] Estas seis líneas de acción han sido identificadas en el análisis de los documentos seleccionados. En ningún caso pretendemos cerrar el foco analítico al respecto, ni establecer estas 6 acciones como únicas.

- Implementación de tecnologías digitales en el currículo educativo
- Promoción de la formación del profesorado en el uso de tecnologías digitales
- Información y formación para la ciudadanía
- Protección de los datos personales y Ciberseguridad

1.2.1. Principales líneas de acción de la Administración Pública en la protección de la infancia

1.2.1.1 Garantía del Derecho a la Educación Digital[6]

Cuando hablamos de derecho a la educación en la sociedad digital aludimos a una expansión del contenido del derecho a la educación para hacer frente los desafíos de la sociedad digital. En específico, nos referimos al acceso equitativo a tecnologías y recursos digitales que facilitan el aprendizaje y el desarrollo personal y profesional. Este derecho implica no solo la disponibilidad de herramientas tecnológicas adecuadas, como dispositivos digitales e internet, sino también la garantía de que todo el alumnado, y la infancia en su conjunto, tenga las mismas oportunidades para aprender y beneficiarse de estos recursos, sin distinciones por situación socioeconómica, género, ubicación geográfica o capacidades (Helsper, 2021).

El derecho a la educación digital, según lo expuesto en la Observación N.º 25 (MP1), abarca la alfabetización digital, que no solo incluye el manejo seguro y efectivo de las tecnologías digitales, sino también del pensamiento crítico sobre la información en línea y habilidades para el manejo de datos. Además, implica la capacitación de educadores y educadoras en el uso pedagógico de las tecnologías, la integración de competencias digitales en los currículos y la creación de políticas que promuevan un uso ético y efectivo de las tecnologías en la educación.

Junto a lo anterior, la educación digital debe fomentar habilidades, competencias y el desarrollo personal, asegurando la no discriminación y la igualdad (MN12). Además, es esencial que toda persona tenga acceso a la tecnología y a la conectividad a Internet, y, por tanto, se garantice su derecho a una educación digital inclusiva y equitativa (MP3, 5; MN12, 52).

> Según la Comisión Internacional sobre los Futuros de la Educación, convocada por la Directora General de la UNESCO, la alfabetización digital y el acceso digital deberían considerarse derechos básicos en el siglo XXI. La Comisión ha destacado la necesidad de ampliar el concepto del derecho a la educación para que incluya las competencias

[6] En esta sección se analizan los documentos que contienen datos encontrados que se relacionan con la garantía del derecho a la educación digital: MP1 y MP3 a nivel internacional, MN6 y MN7 a nivel estatal y, por último, MP13 (Catalunya) y MN9 (Castilla-La Mancha). Para este apartado no se encontraron menciones en el documento de la Comunitat Valenciana.

> digitales y el acceso digital como forma de apoyar el derecho a la educación, el derecho a la información y los derechos culturales. Como se recoge en la Declaración Mundial sobre la Conectividad para la Educación de Rewired de 2021, las iniciativas en materia de conectividad deberían regirse por una ética de la inclusión y tener su punto de partida en las personas desfavorecidas (MP3, 5-6).
>
> Las administraciones públicas velarán por el acceso de todos los estudiantes a los recursos digitales necesarios, para garantizar el ejercicio del derecho a la educación de todos los niños y niñas en igualdad de condiciones. En todo caso, las tecnologías de la información y la comunicación (TIC) y los recursos didácticos que se empleen, se ajustarán a la normativa reguladora de los servicios y sociedad de la información y de los derechos de propiedad intelectual, concienciando en el respeto de los derechos de terceros (MN12, 52, 4).

En concordancia con este derecho a la educación, la Administración Pública debe garantizar que el sistema educativo prepare al alumnado para la sociedad digital, promoviendo un uso seguro y respetuoso con a dignidad humana y asegurando la formación adecuada del profesorado y alumnado en competencias digitales y derechos fundamentales (MN6 50, 02). Según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales en su artículo 83, el derecho a la educación digital implica:

> (…) la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales (MN6 49, 11).

Según la Carta de Derechos Digitales del Gobierno de España de 2021 (MN7), el derecho a la educación digital debe integrar a la comunidad educativa en la sociedad digital, promoviendo el respeto a la dignidad y los derechos fundamentales. Esto incluye impulsar la formación del profesorado en competencias digitales y promover planes de formación para trabajadores y adultos, especialmente para colectivos vulnerables. Según este documento, la Administración Pública debería garantizar que en el sistema educativo exista un uso seguro y equitativo de los medios digitales, reducir las brechas de género y fomentar el pensamiento crítico. Además, debería asegurar la accesibilidad universal y el acceso a recursos digitales en todos los niveles educativos, atendiendo a la diversidad y necesidades específicas de los estudiantes (MN7, 18-19).

En relación con las brechas de acceso al entorno digital, la Carta de Derechos Digitales de 2021 (MN7), menciona que se fomentará y facilitará el acceso de todos los colectivos a los

entornos digitales, incluyendo la capacitación necesaria para su uso. Además, menciona que se promoverán políticas públicas específicas para abordar las brechas de acceso, atendiendo a posibles sesgos discriminatorios basados en la edad, nivel de autonomía, grado de capacitación digital o cualquier otra circunstancia personal o social. Estas políticas buscan garantizar la plena ciudadanía digital y la participación en los asuntos públicos de todos los colectivos en mayor riesgo de exclusión social (MN7, 14, 3-4).

Poniendo el foco en las CCAA, en el análisis de los documentos observamos algunas referencias interesantes. Por ejemplo, la Ley Orgánica 3/2020 de Educación de España (MN12) plantea lo siguiente en relación con la responsabilidad de las administraciones educativas sobre potenciar la competencia digital en el desarrollo del currículo:

> Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red (MN12, 82).

Conectado con lo anterior, la Carta Catalana por los derechos y las responsabilidades digitales de 2019 (MP13) establece que "Toda persona tiene el derecho y la responsabilidad de educarse y educar sobre y a través de las tecnologías digitales y de los nuevos derechos y las nuevas estructuras sociales, económicas y culturales de la era digital" (MP13, 18, 9).

Este principio subraya la importancia de la alfabetización digital no solo como una habilidad técnica, sino también como un componente necesario para participar plenamente en la sociedad.

En relación con la Ley 7/2023, de 10 de marzo, de Atención y Protección a la Infancia y la Adolescencia de Castilla-La Mancha (MN9), en su artículo 33, menciona que la Administración Pública, a través de la Consejería de Educación, debe garantizar:

> El acceso a los medios telemáticos y al desarrollo de los conocimientos y competencias digitales, evitando la brecha digital de las personas más vulnerables y promoviendo un uso razonable de las tecnologías de la información y la comunicación, de acuerdo a la edad y la maduración de cada persona menor de edad (MN9, 23, 15).

En conclusión, las administraciones públicas tienen la responsabilidad de garantizar a la infancia y adolescencia el acceso a un uso seguro, equitativo y ético de las tecnologías digitales, poniendo énfasis en reducir las brechas existentes, en el desarrollo de competencias digitales adecuadas y en garantizar una participación plena y efectiva en la sociedad del siglo XXI.

1.2.1.2 Dotación de recursos para la digitalización de la educación[7]

A partir del análisis de los documentos, se observa que los Estados, como garantes del derecho a la educación, no solo deben asegurar una educación pública de calidad, sino también regular de manera adecuada la participación del sector privado en el ámbito educativo. Esto incluye garantizar que la educación privada no debilite el rol del Estado ni contribuya a aumentar las desigualdades (MP3, 6, 6). En este sentido, el Informe Especial de la ONU sobre el derecho a la educación, titulado "Repercusiones de la digitalización de la educación en el derecho a la educación" (Boly Barry, 2022), subraya varias consideraciones clave al respecto:

> El derecho a la educación obliga a los Estados a proporcionar una educación pública, gratuita y de calidad. Los Estados siguen teniendo la obligación de respetar, proteger y hacer efectivo el derecho a la educación cuando los actores privados participan en la educación, y deben regular la participación del sector privado en la educación. Los Estados deben velar porque la educación privada se adecúe a las normas educativas; que su existencia no ponga en peligro el papel del Estado como garante de la educación; que no sea utilizada para acrecentar la desigualdad o la injusticia, y que los alumnos de la educación privada sean sus principales beneficiarios. Estas obligaciones se aplican no solo a las instituciones educativas privadas, sino también cuando se crean alianzas entre los sistemas educativos públicos y los actores privados, en particular a la hora de diseñar y ejecutar programas de educación digital (MP3, 6, 6).

En relación con la inversión pública para la educación digital, se menciona lo siguiente en el documento España Digital 2026 (MP10):

> En el ámbito de las competencias digitales, durante 2021 se ha acelerado la inversión pública para la digitalización de la educación y la formación profesional. Además de culminar la inversión en equipos portátiles para los estudiantes del Programa Educa en Digital, lanzado poco después de la irrupción de la pandemia, se ha modernizado el catálogo de especialidades de la FP y se han transferido más de 100 millones a las Comunidades Autónomas para la digitalización de las infraestructuras de las escuelas y centros de formación (MP10, 15, 3).

Para la ejecución del Programa Educa en Digital de 2020 (MN3), el Ministerio de Educación y Formación Profesional de España trazó los siguientes objetivos:

[7] Los documentos analizados en esta sección que contienen datos sobre la dotación de recursos fueron, a nivel internacional, el MP3; a nivel estatal, el MP10, MN3 y MN6; y a nivel autonómico, Catalunya (MP14), Castilla-La Mancha (MN10) y Comunitat Valenciana (MN11).

> 1. Mejorar la Competencia Digital Educativa, que incluye la del alumnado, la del profesorado y la de los centros educativos. 2. Implantar el Plan Digital de Centro Educativo aportando equipamiento, transformando espacios, aportando formación y aplicando métodos de Inteligencia Artificial para facilitar el proceso de enseñanza-aprendizaje. 3. Crear Recursos Educativos Abiertos (REA) en formato digital. 4. Fomentar el uso de metodologías y competencias digitales avanzadas. (MN3, 4, 4).

En el documento de España Digital 2025, se contemplaron estrategias para atender las necesidades digitales, a través de la elaboración del Plan Nacional de Competencias Digitales, donde se define la estrategia global a corto y mediano plazo, además del inicio del Plan Educa en Digital, que contempla la dotación de equipamientos y conectividad para el alumnado de los centros de primaria y secundaria (MP10, 122, 5).

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en su artículo 97 sobre "Políticas de impulso de los derechos digitales", menciona que el Gobierno, junto con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los objetivos de superar las brechas digitales y garantizar el acceso a Internet a colectivos vulnerables y económicamente desfavorecidos mediante medidas como un bono social de acceso a Internet (MN6, 54, 5-6).

En relación con el punto anterior, según el Informe de Cobertura de Banda Ancha en España (Ministerio de Asuntos Económicos y Transformación Digital, 2022), desde 2018, a través de las ayudas públicas, se han beneficiado 4,7 millones de viviendas con redes de banda ancha ultrarrápida. Estas ayudas se han realizado mediante el Programa de Universalización de Infraestructuras Digitales para la Cohesión Banda Ancha (UNICO), que forma parte de las inversiones previstas por el Gobierno en el marco del Plan de Recuperación y la Agenda España Digital 2026, y está financiado con los fondos de Next Generation EU (Ministerio de Asuntos Económicos y Transformación Digital, 2022).

Poniendo el foco en las CCAA, el Pla d'educació digital de Catalunya 2020-2023 menciona que el Departament d'Educació debe proporcionar a los centros educativos los servicios digitales necesarios para mejorar la actividad educativa, incluyendo aplicaciones didácticas, contenidos educativos de calidad y servicios de registro académico (MP14, 10, 1).

En la Orden 178/2022, de 14 de septiembre, de la Consejería de Educación, Cultura y Deportes de Castilla-La Mancha, se menciona que, en el ámbito de la brecha digital y la gestión de dispositivos, se deberá: "organizar un procedimiento de cesión de dispositivos tecnológicos y acceso a Internet para el alumnado del centro, prestando especial atención al alumnado en situación de vulnerabilidad para facilitar la accesibilidad al aprendizaje" (MN10, 32783, 11).

En el plan de tratamiento de datos en los centros educativos de la Comunitat Valenciana (MN11) se indica que, según la Ley orgánica de educación 2/2006, "los responsables de la

educación deben proporcionar a los centros los recursos y los medios que necesitan para desarrollar su actividad y alcanzar tal objetivo" (MN11, 46425, 2).

Con lo expuesto anteriormente, se podría concluir que la Administración Pública debería proveer de financiamiento para que todo el alumnado tenga acceso a tecnologías y recursos digitales de calidad. Este compromiso incluye la dotación de equipos, conectividad, y la regulación de alianzas público-privadas para evitar desigualdades.

1.2.1.3 Implementación de tecnologías digitales en el currículo educativo[8]

Tal como se menciona en el Informe Especial de la ONU sobre el derecho a la educación (2022), ya desde antes de la pandemia, el desarrollo y distribución de la tecnología digital estaba aumentando rápidamente en la educación a través de diversos dispositivos y herramientas como teléfonos inteligentes, computadoras, tabletas, proyectores, pizarras interactivas, sistemas inteligentes, robots, plataformas, aplicaciones, juegos y realidad virtual. La utilización de la tecnología se ha vuelto inherente y omnipresente en la educación. Las principales tendencias actuales incluyen enfoques mixtos que combinan métodos presenciales con actividades informáticas, educación a distancia para estudiantes de diversas características, sistemas de inteligencia artificial para personalizar el aprendizaje, gamificación para mejorar la educación y el análisis del aprendizaje mediante minería de datos y aprendizaje automático (MP3, 3, 3).

En España se ha subrayado la importancia de integrar competencias digitales en todos los niveles educativos, tal como se menciona en los documentos MN5, MN6 y MP12.

El Informe sobre el uso seguro y respetuoso de los medios digitales en el Currículo Básico del Ministerio de Educación y Formación Profesional (2019) menciona que: "el uso seguro y responsable de las Tecnologías de la Información y Comunicación constituye un elemento transversal que debe abordarse desde todas las materias y en todas las etapas educativas, desde la Educación Primaria a Bachillerato" (MN5, 1, 1).

A nivel estatal, a lo largo de los últimos años, se han adoptado diversas iniciativas para promover la protección de la infancia mediante el desarrollo y promoción de la competencia digital en educación. Entre estas, destacan iniciativas vinculadas a la formación de docentes y a la integración de competencias digitales en los currículos escolares, tal como lo menciona el Plan Nacional de Capacidades Digitales 2023:

[8] Los documentos analizados en esta sección que contienen datos sobre la implementación de tecnologías digitales en el currículo educativo fueron, a nivel internacional, el MP3; a nivel estatal, el MP12, MN5 y MN6; y a nivel autonómico, Catalunya (MP14) y Castilla-La Mancha (MN10). Para este apartado no se encontró menciones en el documento de la Comunitat Valenciana.

> Es necesario introducir la digitalización en el entorno educativo y formativo, tanto en el acceso a los medios digitales adecuados como en los métodos de enseñanza y el desarrollo curricular en todos los niveles educativos (Primaria, Secundaria, Formación Profesional y Universitaria), de tal modo que la alfabetización digital sea una constante desde las edades más tempranas, dado que solo así se inculca el principio de "formación durante toda la vida" (MP12, 4-5).

Asimismo, la Ley Orgánica 3/2018 de protección de Datos Personales y garantía de los derechos digitales establece que las Administraciones educativas deben incorporar en el currículo de asignaturas de libre configuración la competencia digital y los elementos relacionados con los riesgos del uso inadecuado de las TIC, prestando especial atención a la violencia en línea (MN6 49, 12).

El Pla d'educació digital de Catalunya 2020-2023 (MP14) menciona que la competencia digital será transversal y estará establecida en el currículo de todas las etapas educativas, con el fin de contribuir a mejorar los aprendizajes y la reflexión sobre el uso seguro de las tecnologías digitales y la identidad digital del alumnado (MP14, 17, 5).

Por otra parte, la Consejería de Educación de Castilla-La Mancha, en la Orden 178/2022, menciona que está implementando acciones para la puesta en marcha del programa de cooperación territorial para la mejora de la competencia digital educativa, donde las Administraciones educativas deben "promover el uso de las tecnologías de la información y la comunicación (TIC) en el aula como medio didáctico apropiado y valioso para llevar a cabo las tareas de enseñanza y aprendizaje" (MN10, 32780, 7).

En resumen, según la documentación analizada, la integración de competencias digitales en el currículo educativo es inherente a la era digital (MP3, 3). En España se ha subrayado la importancia de estas competencias en todos los niveles educativos (MN5, 1). El Ministerio de Educación destaca la necesidad de un uso seguro y responsable de las TIC en todas las etapas educativas (MN6, 49). Iniciativas como el Plan Nacional de Capacidades Digitales 2023 promueven la alfabetización digital desde edades tempranas (MP12, 4-5). Y, a nivel autonómico, el Pla d'educació digital de Catalunya 2020-2023 establece la competencia digital como transversal en todas las etapas educativas (MP14, 17) y la Consejería de Educación de Castilla-La Mancha impulsa el uso de tecnologías en el aula para mejorar el proceso de enseñanza-aprendizaje (MN10, 32780).

1.2.1.4 Promoción de la formación del profesorado en el uso de tecnologías digitales[9]

[9] En esta sección, fueron analizados los documentos que contienen datos sobre la promoción de la formación del profesorado en el uso de tecnologías digitales a nivel estatal (MP10, MP8 y MN6), y a nivel autonómico, Catalunya (MP14) y Castilla-La Mancha (MN10). No se encontraron menciones a esta cuestión en el documento de la Comunitat Valenciana.

Del análisis de los documentos revisados se desprende que un aspecto clave de la acción de la Administración Pública para garantizar la educación digital es asegurar que el profesorado alcance un nivel elevado de competencia digital. En este contexto, el Artículo 83 de la Ley Orgánica 3/2018 (MN6) establece las directrices necesarias para que el profesorado reciba la formación adecuada en el uso de tecnologías digitales. Esta formación es fundamental para que el profesorado pueda integrar de manera efectiva las herramientas digitales en los procesos de enseñanza, respondiendo a las demandas tecnológicas actuales.

> El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza (…). Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

Además, el Plan de Recuperación ha proporcionado un impulso adicional con el componente 19 "Plan Nacional de Capacidades Digitales". Este plan abarca acciones destinadas a desarrollar competencias digitales de manera transversal en otros componentes que están vinculados con la modernización del sistema educativo, la formación profesional y el mercado laboral (MP10, 121, 2).

El Plan Nacional de Competencias Digitales menciona, entre sus medidas destacadas, la formación y capacitación digital del conjunto de la población en todo el estado. Además, en el documento se habla sobre iniciativas como la digitalización de las escuelas, el Plan de Formación Profesional Digital y la lucha contra la brecha digital de género mediante programas que promuevan las vocaciones científico-tecnológicas y la capacitación digital para mujeres y niñas (MP8, 12, 3). En este contexto, la capacitación del profesorado en el uso de las tecnologías digitales es importante, porque al estar adecuadamente formados, los docentes pueden integrar de manera efectiva las herramientas digitales en el proceso educativo, asegurando que el alumnado adquiera las competencias digitales necesarias para su desarrollo personal y profesional en una sociedad cada vez más digitalizada.

En 2013, la Unión Europea publicó el marco DigCompEdu para definir las competencias digitales de la ciudadanía. Este marco, revisado en 2016 y establecido como una referencia común para todos los estados miembros, ofrece definiciones específicas de competencias digitales para diversos campos profesionales, asegurando que se incluyan las características necesarias para desempeñar tareas laborales concretas. En el ámbito educativo se desarrolló el *DigCompEdu*, enfocado a las competencias digitales docentes (MP14, 8, 3-4).

La competencia digital docente (CDD) es un factor importante para la calidad educativa. El Departament d'Educació de Catalunya ha desarrollado el Pla d'educació digital de Catalunya 2020-2023 (MP14) basado en el Proyecto Interdepartamental de Competencia Digital Docente y en las recomendaciones de *DigCompEdu* de la Comisión Europea (MP14, 23, 1).

> En aquest document es defineix la CDD com la capacitat que el professorat té de mobilitzar i transferir tots els seus coneixements, estratègies, habilitats i actituds sobre les tecnologies per a l'aprenentatge i el coneixement en situacions reals i concretes de la seva praxi professional per tal de: i) facilitar l'aprenentatge de l'alumnat i l'adquisició de la seva competència digital; ii) dur a terme processos de millora i innovació a l'ensenyament d'acord amb les necessitats de l'era digital; i iii) contribuir al seu desenvolupament professional d'acord amb els processos de canvi que tenen lloc a la societat i als centres educatius. Tanmateix, la competència digital docent fa referència a les habilitats de caràcter didàctic i metodològic, però també és necessària una competència TIC referida a l'ús instrumental de les tecnologies (MP14, 23, 2).

El Marco de Referencia de la Competencia Digital Docente (MRCDD) mantiene la estructura del DigCompEdu en seis áreas, que son cada una de las categorías en las que se organizan las competencias digitales de los docentes dentro del marco y se centran en diferentes aspectos de las actividades profesionales de los docentes: compromiso profesional, contenidos digitales, enseñanza y aprendizaje, evaluación y retroalimentación, empoderamiento del alumnado y desarrollo de la competencia digital del alumnado. Para garantizar estas competencias, el Departament d'Educació de Catalunya se propone realizar formación continua a los docentes, y coordinar con universidades para la acreditación de nuevos profesores y el reconocimiento y evaluación de las competencias digitales como requisito para la profesión docente. Además, se espera fomentar la creación de redes docentes para compartir experiencias y materiales didácticos y de esta forma integrar la tecnología digital en la educación (MP14, 23, 3-6).

En el documento Normativo (MN10) de Castilla-La Mancha, se señala que el Ministerio de Educación y Formación Profesional ha puesto en marcha programas de cooperación territorial, dos de los cuales están relacionados con la transformación digital de la enseñanza: Digitalización del Ecosistema Educativo (EcoDigEdu) y Competencia Digital Educativa (CompDigEdu). Este último tiene como objetivo final "mejorar el desarrollo de la competencia digital del alumnado y el uso de las tecnologías digitales en el aprendizaje a través del desarrollo de la competencia digital del profesorado (tanto individual como colegiada)" (MN10, 32780, 5).

En resumen, y tal como afirma la Ley Orgánica 3/2020 de Educación de España (MN12), la Administración Pública tiene la responsabilidad de garantizar que los docentes estén adecuadamente formados en el uso de tecnologías digitales, asegurando así una educación de calidad en la era digital. De esta manera, estos profesionales podrán guiar al alumnado en el uso seguro y eficaz de las tecnologías, fomentando la innovación y la mejora educativa necesarias en una sociedad cada vez más digitalizada.

1.2.1.5 Informar y formar a la ciudadanía[10]

A partir del análisis de los documentos revisados, se reconoce que la Administración Pública desempeña un papel esencial en la tarea de informar y formar a la ciudadanía sobre la protección de la infancia en el entorno digital. Por ejemplo, la Observación General N.º 25 de las Naciones Unidas (2021) (MP1) resalta la importancia de llevar a cabo formaciones para profesionales y empresas sobre los efectos del entorno digital en los derechos de los niños y niñas, así como la aplicación adecuada de las normas internacionales en este ámbito. Estas formaciones deben realizarse tanto antes de la contratación como durante el empleo, para garantizar que quienes trabajan con la infancia cuenten con preparación para cumplir con estas normativas:

> Los profesionales que trabajan para y con los niños, así como el sector empresarial, incluida la industria de la tecnología, deben recibir formación sobre los efectos del entorno digital en los derechos del niño en múltiples contextos, las diversas formas en que los niños ejercen sus derechos en el entorno digital y la manera en que acceden a las tecnologías y las utilizan. También deben recibir formación sobre la aplicación de las normas internacionales de derechos humanos en el entorno digital. Los Estados parte deben lograr que, antes de la contratación y durante el empleo, se imparta formación relacionada con el entorno digital a los profesionales de la enseñanza en todos los niveles a fin de apoyar el perfeccionamiento de sus conocimientos, aptitudes y prácticas (MP1, 4, 7).

Junto a esto, "deben impartir formación especializada a los agentes del orden, a los fiscales y a los jueces en relación con las vulneraciones de los derechos del niño específicamente relacionadas con el entorno digital, entre otras formas mediante la cooperación internacional" (MP1, 5, 11).

Esta formación especializada es importante para que estos profesionales puedan identificar, investigar y procesar adecuadamente los casos que involucren abusos o vulneraciones de derechos en el ámbito digital.

También, para proteger a la infancia en entornos digitales de situaciones de violencia y proporcionar información sobre estrategias de protección, la Administración Pública debería desarrollar campañas educativas de sensibilización y difusión. Tal como se menciona en la Ley Orgánica 8/2021:

[10] Los documentos analizados en esta sección que contienen datos sobre la protección de la infancia en la sociedad digital fueron, a nivel internacional, el MP1; a nivel estatal, el MN4; y a nivel autonómico, Catalunya (MP14 y MN8), Castilla-La Mancha (MP15) y la Comunitat Valenciana (MN11).

> Las administraciones públicas desarrollarán campañas de educación, sensibilización y difusión dirigidas a los niños, niñas y adolescentes, familias, educadores y otros profesionales que trabajen habitualmente con personas menores de edad sobre el uso seguro y responsable de Internet y las tecnologías de la información y la comunicación, así como sobre los riesgos derivados de un uso inadecuado que puedan generar fenómenos de violencia sexual contra los niños, niñas y adolescentes como el ciberbullying, el grooming, la ciberviolencia de género o el sexting, así como el acceso y consumo de pornografía entre la población menor de edad (MN4, 35, 7).

En la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, se menciona que deben diseñarse y ejecutarse planes para la divulgación de los derechos de las personas con relación a la protección de datos y el acceso a la información, y la evaluación del impacto sobre la privacidad (MN8, 5, 4). También, en el Pla d'educació digital de Catalunya 2020-2023 (MP14), se destaca la necesidad de realizar capacitaciones digitales a toda la ciudadanía, para asegurar la participación de todas las personas en la sociedad del siglo XXI (MP14, 17, 2).

En esta misma línea, el Decreto 55/2023, de 6 de junio, por el que se establece la política de protección de datos en la Administración de la Junta de Comunidades de Castilla-La Mancha, menciona en el artículo 20 que:

> Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación en materia de protección de datos para el personal empleado público que presta sus servicios en la Administración de la Junta de Comunidades de Castilla-La Mancha y sus organismos públicos (MP15, 20841, 16).

En conclusión, la protección a la infancia en la sociedad digital requiere el compromiso continuo de la Administración Pública para desarrollar campañas de sensibilización y educación a la ciudadanía en general, en especial a las personas que trabajan con la infancia. Estas iniciativas se deben realizar con la finalidad de disminuir las vulneraciones de derechos de la infancia en el entorno digital de manera efectiva, garantizando que los mismas sean respetados y protegidos.

1.2.1.6 Protección de los datos personales y Ciberseguridad[11]

En esta línea de acción, varios documentos destacan la importancia de que la Administración Pública monitoree y proteja el tratamiento de los datos personales, especialmente en relación con la infancia. La Observación General N.º 25 (2021) de las Naciones Unidas (MP1), que aborda los derechos de la niñez en el entorno digital, establece directrices específicas sobre la protección y manejo de dichos datos. Estas directrices subrayan la necesidad de garantizar

[11] Los documentos analizados en esta sección que contienen datos sobre la protección de datos personales y ciberseguridad fueron, a nivel internacional, el MP1; a nivel estatal, el MP10, MN4 y MN7; y a nivel autonómico, Catalunya (MP13), Castilla-La Mancha (MP15) y la Comunitat Valenciana (MN11).

que los menores y sus cuidadores puedan acceder, rectificar y eliminar su información personal cuando sea necesario. Además, se enfatiza la importancia de salvaguardar la privacidad en todos los entornos digitales, asegurando que cualquier manejo de sus datos cumpla con los más altos estándares de seguridad y respeto a sus derechos.

> Los Estados partes deben garantizar que los niños y sus padres o cuidadores puedan acceder fácilmente a los datos almacenados, rectificar los que sean inexactos u obsoletos y eliminar los datos almacenados de forma ilegal o innecesaria por autoridades públicas, particulares u otras entidades, con sujeción a limitaciones razonables y legales. Deben garantizar asimismo el derecho de los niños a retirar su consentimiento y a oponerse al procesamiento de datos personales cuando la persona encargada de procesarlos no demuestre que existen motivos legítimos e imperiosos para ello. Además, deben proporcionar información a los niños, padres y cuidadores sobre estas cuestiones, en un lenguaje adaptado a los niños y en formatos accesibles (MP1, 8, 4).

Además, el Estado debe lograr que se recopilen periódicamente datos de investigaciones sobre el impacto del entorno digital en la vida de la infancia. La recogida de estos datos se debe realizar de manera exhaustiva y desglosada por edad, sexo, discapacidad, ubicación geográfica, origen étnico y situación socioeconómica, y debe servir de base para diseñar y evaluar la legislación, las políticas y las prácticas de protección de la infancia (MP1, 6, 1).

En esta misma línea, la Administración Pública, tiene la responsabilidad y compromiso de llevar a cabo diagnósticos periódicos que consideren criterios de edad y género sobre el uso seguro de Internet entre niños, niñas y adolescentes (MN4, 36, 5). Además, debe promover el intercambio de información, conocimientos, experiencias y buenas prácticas con la sociedad civil en lo referente a la protección de los datos de menores en Internet, adoptando un enfoque multidisciplinar e inclusivo (MN4, 20, 11).

En la Carta de Derechos Digitales del Gobierno de España del 2021 (MN7), se dice sobre la protección de las personas menores de edad en entorno digital lo siguiente:

> Los centros educativos, las Administraciones y cualesquiera personas físicas o jurídicas que desarrollen actividades en entornos digitales en las que participen personas menores de edad están obligados, por la legislación aplicable, a la protección del interés superior de la persona menor y sus derechos fundamentales, especialmente los derechos a la intimidad, al honor y a la propia imagen, al secreto de las comunicaciones y el derecho a la protección de datos personales. Deberá recabarse su consentimiento, si es mayor de 14 años, o el de sus representantes legales, para la publicación o difusión de sus datos personales o su imagen a través de servicios de redes sociales (MN7, 12, 6).

Las Comunidades Autónomas se rigen por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que establece que “los datos de carácter personal deben ser protegidos de forma efectiva y auditable por defecto, y se debe velar por la soberanía personal con el fin de ejercer derechos como los de almacenaje, modificación, recuperación, tratamiento y cancelación” (MP13, 17, 8; MP15, 20836, 5).

Además, la Comunitat Valenciana, según la resolución de 28 de junio de 2018, dispone que la Subsecretaria de la Conselleria de Educación, Investigación, Cultura y Deporte es responsable de velar por el cumplimiento de la legislación en materia de protección de datos, conforme al artículo 9 del Decreto 130/2012. Esto implica la implementación de medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales tratados en los centros educativos (MN11, 46425, 5).

Por otro lado, la Administración General del Estado, a través del Centro de Operaciones de Ciberseguridad, debe coordinar respuestas a ciberincidentes, facilitar servicios e inteligencia avanzada, y gestionar eventos de seguridad centralizados, desplegando sensores y realizando búsquedas proactivas de amenazas (MP10, 52, 2-3).

Por lo expuesto anteriormente, podemos concluir que la Administración Pública debería garantizar la protección de los datos personales y la ciberseguridad, especialmente en lo que respecta a la infancia. Esto implica no solo el monitoreo y regulación del tratamiento de datos, sino también la realización de investigaciones periódicas para comprender el impacto del entorno digital en la infancia. Además, se debe fomentar la educación y la capacitación sobre el uso seguro de Internet y promover la colaboración con proveedores de servicios digitales y la sociedad civil. La implementación de políticas claras y la creación de infraestructuras como el Centro de Operaciones de Ciberseguridad son esenciales para asegurar que el alumnado pueda navegar en línea de manera segura.

1.2.2 Síntesis

La revisión del rol de la Administración Pública en la protección de la infancia en la sociedad digital ha abarcado dimensiones como el derecho a la educación, la dotación de recursos para la digitalización de la educación, la inclusión de tecnologías digitales en el currículo educativo, la formación del profesorado en el uso de tecnologías digitales, las campañas de sensibilización sobre la sociedad digital y también, la protección de datos personales y ciberseguridad.

A partir del análisis de los documentos del marco normativo y del marco político se podría concluir que las principales líneas de trabajo de la Administración Pública para garantizar el derecho a la educación y la protección de la infancia en la sociedad digital son:

1.2.2.1 En relación con el derecho a la educación digital:

El análisis nos ha permitido observar que ya se han establecido una serie de medidas integrales relacionadas con el derecho a la educación digital. Estas medidas abarcan diversos aspectos clave, desde la alfabetización digital hasta la reducción de brechas en el acceso a la tecnología.

En primer lugar, los documentos destacan la promoción de la alfabetización digital y la capacitación de los educadores, integrando competencias digitales en los currículos. Subrayan la importancia de asegurar una formación adecuada tanto del profesorado como del alumnado en dichas competencias (MP1, MN6 50, 2), evidenciando el compromiso hacia una educación adaptada al entorno digital.

En segundo lugar, se pone de relieve la creación de políticas que promuevan un uso ético y efectivo de las tecnologías digitales en la educación. Estas políticas están orientadas a garantizar la no discriminación y la igualdad en el acceso a la tecnología y la conectividad a Internet (MP1, MP3, 5, 1-4), como un elemento fundamental para asegurar la equidad en el entorno educativo digital.

En tercer lugar, los documentos analizados destacan la importancia de fomentar el acceso universal a entornos digitales. Señalan la necesidad de abordar las brechas de acceso y reducir las disparidades de género, asegurando que todas las personas puedan participar plenamente en la sociedad digital (MN7, 14, 3-4; MN7, 18-19).

1.2.2.2 En relación con la dotación de recursos para la digitalización de la educación:

Se han identificado varias líneas de acción relacionadas con la dotación de recursos para la digitalización de la educación. Estas acciones están orientadas a asegurar una educación pública de calidad, con la adecuada infraestructura y conectividad para todos los colectivos, especialmente aquellos más vulnerables.

En primer lugar, los documentos subrayan la necesidad de proveer una educación pública, gratuita y de calidad, regulando la participación de actores privados para evitar desigualdades en el acceso a la digitalización (MP3, 6, 6). En este sentido, se enfatiza el rol del Estado en garantizar la equidad.

En segundo lugar, se destaca la inversión en la digitalización de la educación y la formación profesional, lo cual incluye infraestructuras, equipos y conectividad. Esta inversión es presentada como esencial para asegurar una educación adaptada a los desafíos tecnológicos actuales (MP10, 15, 3; MN3, 4, 4; MP10, 122, 5).

En tercer lugar, los documentos analizados mencionan un Plan de Acceso a Internet como una medida fundamental para superar las brechas digitales, garantizando el acceso a Internet para colectivos vulnerables y económicamente desfavorecidos (MN6, 54, 5-6). Esta medida es clave para asegurar una inclusión plena en el entorno educativo digital.

En cuarto lugar, se aborda la provisión de servicios digitales y recursos a los centros educativos, incluyendo aplicaciones didácticas, contenidos educativos de calidad y servicios de registro académico. Estas acciones están diseñadas para mejorar la actividad educativa y garantizar una gestión eficiente de los recursos educativos (MP14, 10, 1; MN11, 46425, 2).

1.2.2.3 En relación con la implementación de tecnologías digitales en el currículo educativo:

En un conjunto de documentos, se destaca la relevancia de implementar tecnologías digitales en el currículo educativo como un aspecto esencial para asegurar una educación adaptada al contexto tecnológico actual. Las acciones señaladas en los documentos abordan tanto la formación técnica como la protección de los estudiantes en el uso de las tecnologías.

En primer lugar, varios textos resaltan la inclusión de competencias digitales en el currículo educativo para garantizar una formación técnica adecuada, al tiempo que se promueve el uso seguro y responsable de las tecnologías por parte del alumnado (MN5, MN6, MP12, MP14). Esta medida busca que los estudiantes adquieran las habilidades necesarias para enfrentar los desafíos del entorno digital.

En segundo lugar, se subraya que el uso seguro y responsable de las tecnologías digitales debe ser un elemento transversal, abordado en todas las materias y etapas educativas, desde la Educación Primaria hasta el Bachillerato (MN5; MN12). Esta perspectiva integradora busca preparar a los estudiantes en cada nivel educativo para un uso ético de las tecnologías.

En tercer lugar, algunos documentos señalan la necesidad de promover la protección de la infancia mediante el desarrollo de competencias digitales, destacando iniciativas específicas para la formación de docentes y la integración de estas competencias en los currículos escolares (MP1; MP12). Este enfoque apunta a fortalecer la seguridad digital en el entorno educativo.

En cuarto lugar, se menciona la incorporación de competencias digitales en las asignaturas de libre configuración, con especial atención a los riesgos asociados al uso inadecuado de las tecnologías digitales, como la violencia en línea (MN6; MP1). Esta acción busca concienciar a los estudiantes sobre los peligros del entorno digital y formar una ciudadanía digital responsable.

1.2.2.4 En relación con la promoción de la formación del profesorado en el uso de tecnologías digitales

En el análisis de estos documentos hemos identificado también múltiples elementos comunes en relación con la promoción de la formación del profesorado en el uso de tecnologías digitales. Las acciones propuestas se centran en garantizar que los docentes cuenten con las competencias digitales necesarias para integrarlas de manera efectiva en el proceso educativo.

En primer lugar, algunos documentos subrayan la necesidad de garantizar que el profesorado adquiera las competencias digitales y reciba la formación necesaria para la enseñanza. Esto incluye tanto el uso de los medios digitales como la seguridad en su manejo, además de la garantía de los derechos fundamentales en Internet (MN6, MN12).

En segundo lugar, se destaca el desarrollo y adopción de marcos de competencia digital docente, como el *DigCompEdu*, que busca asegurar que los docentes puedan integrar efectivamente las tecnologías digitales en el proceso educativo (MP6; MP14). Este marco proporciona una guía clara sobre cómo mejorar las habilidades digitales en la enseñanza.

En tercer lugar, los documentos analizados señalan la importancia de facilitar la formación continua del profesorado, coordinando con universidades para la acreditación y reconocimiento de las competencias digitales. Además, se fomenta la creación de redes docentes que permitan compartir experiencias y materiales didácticos, promoviendo un aprendizaje colaborativo (MP1; MP8; MP14).

1.2.2.5 En relación con la formación y la información de la ciudadanía

El análisis de los documentos nos ha permitido reconocer un conjunto de medidas dirigidas a la protección de la infancia en la sociedad digital. Estas acciones abordan desde campañas de sensibilización hasta la formación especializada de profesionales, con el objetivo de garantizar la seguridad y los derechos de los niños en el entorno digital.

En primer lugar, los documentos destacan la importancia de desarrollar campañas educativas de sensibilización y difusión dirigidas a niños, adolescentes, familias, educadores y profesionales. Estas campañas están enfocadas en el uso seguro y responsable de Internet y las TIC, así como en la prevención de riesgos como la violencia sexual en línea (MP1; MP9; MN4; MN9).

En segundo lugar, se subraya la necesidad de realizar formaciones para profesionales y empresas que trabajan con la infancia, abordando los efectos del entorno digital en los derechos de los niños y la aplicación de normas internacionales. Estas formaciones deben ser impartidas tanto antes de la contratación como durante el empleo (MP1; MP8; MP10).

En tercer lugar, los documentos mencionan la importancia de impartir formación especializada a agentes del orden, fiscales y jueces sobre las vulneraciones de los derechos de los niños y niñas en el entorno digital, con el fin de asegurar una respuesta adecuada en estos casos (MP1; MN4).

En cuarto lugar, se destaca la divulgación de los derechos de las personas en relación con la protección de datos, el acceso a la información y la evaluación del impacto sobre la privacidad. Esta medida busca garantizar que los derechos de la infancia sean respetados en el entorno digital (MN6; MN8).

Por último, los documentos también mencionan la implementación de los Certificados de Registro de Delincuentes Sexuales, como una herramienta para proteger a los menores en el ámbito digital (MN11, 46437, 4).

1.2.2.6 En relación con la protección de los datos personales y ciberseguridad:

A partir del análisis de los documentos, se puede identificar un conjunto de medidas clave en relación con la protección de los datos personales y la ciberseguridad, especialmente en lo que respecta a la infancia. Estas medidas abordan tanto la gestión de los datos personales como la seguridad en el entorno digital.

En primer lugar, los documentos subrayan la importancia de monitorear y proteger el tratamiento de los datos personales, garantizando que los niños, niñas y sus cuidadores puedan acceder, rectificar y eliminar datos cuando sea necesario (MP1, MN6; MN8).

En segundo lugar, se destaca la necesidad de recopilar periódicamente datos de investigaciones sobre el impacto del entorno digital en la vida de la infancia, desglosados por factores como género, edad y situación socioeconómica, para fundamentar la legislación, políticas y prácticas (MP1, MN6; MN8).

En tercer lugar, los documentos resaltan la promoción del intercambio de información, conocimientos y buenas prácticas con la sociedad civil en materia de protección de los datos de menores en Internet (MN4; MN6; MN8; MP9).

En cuarto lugar, se enfatiza la necesidad de garantizar la protección de los derechos fundamentales de los menores en entornos digitales, asegurando que el consentimiento para la publicación o difusión de sus datos personales o imágenes sea adecuado y conforme a la ley (MN7; MN8; MP9).

En quinto lugar, se menciona la importancia de adherirse a los principios de protección de datos establecidos en el Reglamento General de Protección de Datos (RGPD) y en la Ley Orgánica 3/2018, en todas las actividades relacionadas con el tratamiento de datos personales (MN6; MN8; MP15).

En sexto lugar, los documentos destacan la coordinación de respuestas a ciberincidentes y la gestión de eventos de seguridad centralizados mediante el Centro de Operaciones de Ciberseguridad, como una medida clave para reforzar la ciberseguridad en el entorno digital (MN6; MN8; MP10; MP15).

Podemos concluir que la responsabilidad de la Administración Pública en la protección de la infancia en entornos digitales es asegurar que todos los niños, niñas y jóvenes puedan desarrollarse en un ambiente seguro y favorable. Esto implica garantizar el acceso equitativo a tecnologías y recursos digitales, promoviendo la alfabetización digital y la formación de educadores en competencias digitales. Asimismo, es necesaria la provisión de financiamiento

para la digitalización de la educación, la implementación de tecnologías digitales en el currículo educativo, y la formación continua del profesorado. Además, la Administración Pública debe desarrollar campañas de sensibilización para educar sobre el uso seguro de Internet y proteger los datos personales de los menores, estableciendo políticas claras de ciberseguridad.

Las directrices establecidas por organismos internacionales como la ONU, junto con la legislación estatal y la autonómica enfatizan la necesidad de una formación especializada y una aplicación estricta de las normas de derechos humanos en el ámbito digital. Esto no solo protege a la infancia de riesgos en el internet, sino que también promueve un uso ético de las tecnologías digitales.

1.2.3 Listado de documentos incluidos

MP1: Organización de las Naciones Unidas. (2021). *Observación General Nº 25, relativa a los derechos de los niños en relación con el entorno digital, Convención sobre los Derechos del Niño.* https://bit.ly/4gWWnXx

MP3: Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/4elJBzM

MP8: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 21: Modernización y digitalización del sistema educativo, incluida la educación temprana de 0-3 años*. https://bit.ly/3XIqtoH

MP10: Gobierno de España. (n.d.). *España Digital 2026.*

MP12: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 19. Plan Nacional de Capacidades Digitales.* https://bit.ly/3ZKocvM

MP13: Generalitat de Catalunya. (2019). *Carta catalana por los derechos y las responsabilidades digitales.* Departament de Polítiques Digitals i Administració Pública. https://bit.ly/3zprudm

MP14: Generalitat de Catalunya. Departament d'Educació. (2020). *Pla d'educació digital de Catalunya 2020-2023*. https://bit.ly/3z33nyv

MP15: Decreto Nº 55, *por el que se establece la política de protección de datos en la Administración de la Junta de Comunidades de Castilla-La Mancha* (6 de junio de 2023). https://bit.ly/3Y0k4X7

MN3: Resolución, *de la Subsecretaría, por la que se publica el Convenio entre el Ministerio de Educación y Formación Profesional, el Ministerio de Asuntos Económicos y*

Transformación Digital y la Entidad Pública Empresarial Red.es, M.P., para la ejecución del programa "Educa en Digital" (7 de julio de 2020). https://bit.ly/3XMmtDP

MN4: Ley Ogánica N° 8, *Ley de protección integral a la infancia y la adolescencia frente a la violencia* (4 de junio de 2021). https://bit.ly/4doiVx1

MN5: Ministerio de Educación y Formación Profesional. (2019). *Informe sobre el uso seguro y respetuoso de los medios digitales en el currículo básico*. https://bit.ly/4eGngNd

MN6: Ley Orgánica N° 3, *Ley de Protección de Datos Personales y garantía de los derechos digitales* (5 de diciembre de 2018). https://bit.ly/4ds3NPc

MN7: Gobierno de España. (2021). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia*. https://bit.ly/4eiIxgn

MN9: Ley N° 7, *Ley de Atención y Protección a la Infancia y la Adolescencia de Castilla-La Mancha* (10 de marzo de 2023). https://bit.ly/3BgdqmL

MN10: Orden N° 178, *de la Consejería de Educación, Cultura y Deportes, por la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios* (14 de septiembre de 2022). https://bit.ly/3MZMhr0

MN11: Resolución, *de la Subsecretaría de la Conselleria de Educación, Investigación, Cultura y Deporte, por la que se dictan instrucciones para el cumplimiento de la normativa de protección de datos en los centros educativos públicos de titularidad de la Generalitat* (28 de junio de 2018). https://bit.ly/3Y0kfBL

Otras referencias

Boly Barry, K. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación: Informe de la Relatora Especial sobre el derecho a la educación* (Consejo de Derechos Humanos, 50º período de sesiones, Tema 3 de la agenda, A/HRC/50/32). Naciones Unidas. https://bit.ly/3TL770W

España. (2015). *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*. Boletín Oficial del Estado, núm. 236, de 2 de octubre de 2015, páginas 89411 a 89484. https://bit.ly/3TL7fxs

Helsper, E. J. (2021). *The Digital Disconnect: The Social Causes and Consequences of Digital Inequalities*. Sage Publications Ltd.

Jacovkis, J., Rivera-Vargas, P., Parcerisa, L., & Calderón, D. (2022). Resistir, alinear o adherir. Los centros educativos y las familias ante las BigTech y sus plataformas educativas digitales. *Edutec. Revista Electrónica de Tecnología Educativa*, 82, 104-118. https://doi.org/10.21556/edutec.2022.82.2615

Ministerio de Asuntos Económicos y Transformación Digital. (2022). *Informe de cobertura de banda ancha en España de 2022*. Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. https://bit.ly/3Y2uYfk

1.3. La escuela en relación con la protección de la infancia en la sociedad digital

En este apartado se presentan los roles de cinco actores de la comunidad educativa en relación con la protección de la infancia en la sociedad digital, a saber:

- Los centros educativos.
- Los equipos directivos de los centros educativos.
- El profesorado.
- El alumnado.
- Las familias.

Una vez recogidas sus principales funciones de acuerdo con los documentos analizados, el apartado aborda también la coherencia entre lo que los marcos político y normativo demandan de cada uno de los actores.

1.3.1. Centros educativos

En relación con los centros educativos, en parte importante de la documentación analizada (MP1; MP3; MP14; MN4; MN10) encontramos varias menciones a su rol en vinculado a la protección de la infancia en la sociedad digital. Esto se manifiesta en diferentes aspectos que se explican a continuación.

En lo referido a la provisión de recursos, en la Observación General nº25 de las Naciones Unidas (2021) (MP1) se plantea la colaboración entre los centros educativos y otros actores, como el sector de la tecnología digital, la ciudadanía, universidades, Administración Pública, entre otros, para garantizar el acceso universal al estudiantado:

> Colaborar con las escuelas y el sector de la tecnología de la información y la comunicación y cooperar con las empresas, la sociedad civil, el mundo académico y las organizaciones a fin de hacer efectivos los derechos de los niños en relación con el entorno digital en los planos intersectorial, nacional, regional y local (MP1, 3, 12).

Respecto a la autonomía de los centros educativos, en el documento Repercusiones de la digitalización de la educación en el derecho a la educación (Boly Barry, 2021) se plantea lo siguiente:

> Mientras quienes formulan las políticas establecen el marco general de los resultados de aprendizaje que deben alcanzarse al final de la enseñanza obligatoria, los centros educativos necesitan autonomía para decidir cuándo y cómo introducir contenidos específicos y la tecnología en las aulas. Deberían ser alentados a concebir su propio enfoque de las tecnologías digitales y la educación mediática, con la participación de

> los directores de los centros, los docentes, los padres, los alumnos y los expertos (MP3, 17, 3).

En distintos documentos se ha manifestado que los centros deben adoptar medidas para proteger al alumnado de situaciones de violencia: “Los centros educativos [...] adoptarán todas las medidas necesarias para garantizar la protección y seguridad de los niños, niñas y adolescentes que comuniquen una situación de violencia” (MN4, 25, 3). Además, deben informar a su alumnado sobre las estrategias o normativas del centro ante este tipo de situaciones:

> Todos los centros educativos al inicio de cada curso escolar [...] facilitarán a los niños, niñas y adolescentes toda la información, que, en todo caso, deberá estar disponible en formatos accesibles, referente a los procedimientos de comunicación de situaciones de violencia regulados por las administraciones públicas y aplicados en el centro o establecimiento, así como de las personas responsables en este ámbito. Igualmente, facilitarán desde el primer momento información sobre los medios electrónicos de comunicación, tales como las líneas telefónicas de ayuda a los niños, niñas y adolescentes (MN4, 24, 7-8).

También deben mantener actualizada la información respecto a este tipo de problemáticas relacionadas con la violencia y facilitar el acceso a aquellos procedimientos vinculados a la búsqueda de ayuda:

> Los citados centros [...] mantendrán permanentemente actualizada esta información en un lugar visible y accesible, adoptarán las medidas necesarias para asegurar que los niños, niñas y adolescentes puedan consultarla libremente en cualquier momento, permitiendo y facilitando el acceso a esos procedimientos de comunicación y a las líneas de ayuda existentes (MN4, 24, 7-8).

En relación con la ciberseguridad y la protección de los datos personales en entornos digitales, los centros educativos deben “ofrecer estrategias concretas de protección y establecer buenas prácticas de ciberseguridad” (MP14, 29, 2). Para ello, según lo establecido en la Ley Orgánica 3/2020 de Educación de España (MN12), es necesario que colaboren con otros actores, como la Agencia de Protección de Datos, o que reciban el apoyo de la Administración Pública (MP14).

Un aspecto adicional identificado en los documentos es la dificultad para atribuir responsabilidades claras a los centros educativos en este ámbito. Por ejemplo, el documento MP3 señala que “la asunción de responsabilidades para la toma de decisiones basadas en datos a menudo no está clara” (MP3, 14, 4). Así, aunque se exigen ciertas responsabilidades a los centros educativos en cuanto al uso de tecnologías digitales y la protección de la infancia, persisten áreas vinculadas al tratamiento de datos en las que no queda claro quién debe

asumir la responsabilidad principal ni cuál es el papel específico del centro educativo en este sentido.

Finalmente, poniendo el foco en las CCAA, podemos apreciar en el caso de Castilla y la Mancha la Orden 178/2022, de 14 de septiembre, de la Consejería de Educación, Cultura y Deportes (MN10), en la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios (2022/8545), que se otorga a la escuela el papel de fomentar el uso de tecnologías digitales en los procesos de enseñanza y aprendizaje con la finalidad de desarrollar la competencia digital tanto del alumnado como del profesorado, para convertirse en espacios digitalmente competentes:

> Mejorar el desarrollo de la competencia digital del alumnado y el uso de las tecnologías digitales en el aprendizaje a través del desarrollo de la competencia digital del profesorado (tanto individual como colegiada) y de la transformación de los centros en organizaciones educativas digitalmente competentes (MN10, 32780, 5).

1.3.2 Equipos directivos

En relación con el papel fundamental que desempeñan los equipos directivos en la protección de la infancia en la sociedad digital, se destacan varios aspectos clave agrupados por niveles estatal y autonómicos.

A nivel estatal, los equipos directivos juegan un rol fundamental en la dinamización del plan digital de los centros educativos, como parte del proceso de integración tecnológica en la enseñanza. Según los documentos, esta tarea se realiza mediante los *Planes Digitales de Centro*, en los que "las escuelas definirán la adecuada integración de la tecnología en el proceso de enseñanza y aprendizaje" (MP12, 17, 4).

En cuanto a la protección de los datos del alumnado, se revela que existe cierto desconocimiento por parte de los equipos directivos en relación con el uso de los datos, ya que "los directores de los centros y los educadores suelen desconocer el uso de los datos por parte de terceros" (MP3, 14, 4). A pesar de ello, se les asigna la responsabilidad de garantizar la confidencialidad: "Todas las personas que tengan acceso a datos de carácter personal están obligadas a guardar secreto sobre estos" (MN11, 13, 1-3), y deben "promover la comunicación inmediata a las Agencias de Protección de Datos en casos de posible tratamiento ilícito de datos de menores" (MN4, 32, 2).

Finalmente, la *Ley Orgánica 2/2006, de 3 de mayo, de Educación*, modificada por la *Ley Orgánica 3/2020*, establece que los equipos directivos deben promover el uso de las TIC en el aula, asegurando su utilización adecuada y eliminando riesgos como la violencia en la red y los estereotipos de género que dificultan la adquisición de competencias digitales en igualdad de condiciones (MN10, MN12).

En lo concerniente a las CCAA, EL *Pla d'educació digital de Catalunya 2020-2023* resalta el papel de los equipos directivos en la transformación digital de los centros educativos. Este proceso requiere que los equipos, junto con el profesorado, realicen un análisis de las necesidades del centro y establezcan una estrategia digital que gestione adecuadamente los espacios, recursos y agrupaciones para optimizar el uso de las tecnologías (MP14, 32, 1).

Este plan también subraya el rol de liderazgo pedagógico que desempeñan los equipos directivos, descrito en el artículo 142 de la LEC, donde se delinean sus funciones dentro del marco de este liderazgo (MP14, 28, 3). Asimismo, los equipos directivos son responsables de "determinar la gobernanza en los centros educativos" y de implementar de manera coordinada la competencia digital, siguiendo los principios del *Pla d'educació digital de Catalunya* en los documentos de gestión del centro (MP14, 28, 2).

En Castilla-La Mancha, la *Orden 178/2022* (MN10) regula la elaboración del Plan Digital de los centros educativos sostenidos con fondos públicos no universitarios. Según esta normativa, los equipos directivos deben "promover el uso de las tecnologías de la información y la comunicación (TIC) en el aula como un medio didáctico apropiado" y, al mismo tiempo, "tratar de eliminar las situaciones de riesgo derivadas de la inadecuada utilización de las TIC"(MN10, 32780, 7), prestando especial atención a la violencia en la red y a la desaparición de estereotipos de género que dificultan la adquisición de competencias digitales en condiciones de igualdad.

En la Comunitat Valenciana, los equipos directivos son responsables de garantizar la confidencialidad de los datos personales del alumnado. Según la normativa local, "todas las personas que tengan acceso a datos de carácter personal están obligadas a guardar secreto sobre estos". Esta responsabilidad incluye la "comunicación inmediata a las Agencias de Protección de Datos en caso de tratamiento ilícito de los datos personales de menores" (MN11, 13, 1-3).

1.3.3. El profesorado

En primer lugar, en los documentos analizados, el rol de del profesorado en la protección de la infancia en la sociedad digital se encuentra más vinculado a las acciones que debe llevar a adelante en el marco de las prácticas de enseñanza y de aprendizaje, que a una descripción de las características del rol que lo vinculen de manera directa a la protección de la infancia.

Por tanto, atisbos de esta caracterización la encontramos tan solo en dos marcos políticos: el Plan de acción de educación digital 2021-2027 de la Comisión Europea (MP6) y la Propuesta de resolución del Parlamento Europeo, Informe sobre la formulación de la política de educación digital (MP7).

En ellos se reconoce el carácter del profesorado como profesionales vinculados a la Administración Pública y su función como garante del cuidado, la asistencia, la enseñanza y la protección de la infancia y adolescencia.

> Los educadores son profesionales con amplios conocimientos y capacitación que necesitan la confianza y las capacidades que les permitan utilizar la tecnología de forma eficaz y creativa para interesar y motivar a sus alumnos (...) (MP 6 - 10,6).
>
> Se ha demostrado que los escolares necesitan un profesorado que posea un nivel suficiente de competencia en el ámbito digital como para facilitar un aprendizaje eficaz en línea y ofrecer un conjunto de recursos ya preparados para el entorno en línea (...) (MP 7-22, 1).

Ahora bien, los marcos normativos y políticos analizados también consideran que estas capacidades no son inherentes al rol docente, sino que, como se menciona en la mayoría de ellos, el profesorado requiere de capacitación para mejorar su Competencia Digital Docente (CDD) y la infraestructura y equipamiento (hardware, software y conectividad) para llevar adelante las acciones que se le encomiendan.

Por ejemplo, en la Carta de Derechos Digitales del Gobierno de España (2021) se señala que en las políticas de educación digital de la UE "se potenciará que el profesorado reciba formación para adquirir competencias digitales y para la enseñanza y transmisión de los valores y derechos referidos en el número anterior" (MN 7 – 18, 14).

La Competencia Digital Docente es definida en el Plan de Educación Digital de Catalunya como "les habilitats de caire didàctic i metodològic compaginades amb l'ús instrumental de les tecnologies, posades al servei de l'èxit educatiu de tot l'alumnat" (MP14 – 10, 3). Esto vincula de manera directa la caracterización del profesorado presente en los documentos (especialmente el MP6 y el MP7) con las acciones y responsabilidades que se le asignan en el marco de la protección de la infancia en el contexto digital.

En esta línea, algunos de los documentos analizados (MP 3, MP 4, MP 9, MP 12, MP 14) sitúan al profesorado como responsable de llevar adelante las siguientes acciones:

i.- Aplicar metodologías de enseñanza y aprendizaje diseñadas para el entorno digital.

> Empleo de las TIC en su labor diaria, así como el desarrollo y aplicación de metodologías para la enseñanza en un contexto digital y, eventualmente, deslocalizado (MN3, 6, 8).
>
> En la seva pràctica diària, el docent ha de desenvolupar la CDD de manera integral, exercitant simultàniament les 5 dimensions que la conformen: disseny, planificació i implementació didàctica; organització d'espais i recursos educatius; comunicació i col·laboració; ètica i civisme digital; i desenvolupament professional (MP14, 23, 3).

ii.- Garantizar la salud digital y la prevención del uso indebido y/o adictivo de las TIC.

> La formación específica en seguridad y uso seguro y responsable de Internet, incluyendo cuestiones relativas al uso intensivo y generación de trastornos conductuales (MN4, 19, 5).

iii.- Favorecer el uso seguro y responsable de Internet por parte del alumnado (MP9, 4, 5).

iv.- Facilitar el desarrollo de competencias y espacios seguros en Internet para promover la participación social y cívica de niños, niñas y adolescentes (MP9, 4, 5).

v.- Innovar en los procesos de enseñanza y aprendizaje utilizando TIC, creando contenidos y compartiendo prácticas

> Dur a terme processos de millora i innovació a l'ensenyament d'acord amb les necessitats de l'era digital (MP14, 23, 2).
>
> Contribuir al seu desenvolupament professional d'acord amb els processos de canvi que tenen lloc a la societat i als centres educatius (MP14, 23, 2).

En síntesis, una parte significativa de los documentos normativos y políticos analizados indican que el rol del profesorado en la sociedad digital sigue siendo fundamental para el desarrollo y aprendizaje del alumnado, manteniendo su responsabilidad como garante del derecho al libre desarrollo de la infancia y adolescencia (MP1). No obstante, el contexto digital plantea nuevas exigencias, siendo prioritario que los docentes adquieran competencias específicas, conocidas como Competencia Digital Docente (MN 3, 4, 7; MP 3, 5, 6, 7, 8, 9, 10, 11, 14).

En la misma línea según el "Plan de Recuperación, Transformación y Resiliencia. Componente 19. Plan Nacional de Capacidades Digitales" (MP12):

> Para que el destinatario final, el alumno, adquiera esa competencia, es esencial que se produzca la mejora de la Competencia Digital Docente que, además, permitirá el máximo aprovechamiento de los medios digitales (MP12, 17, 4).

El compromiso con el desarrollo de esta nueva capacidad es asumido tanto por los gobiernos autonómicos como por los Estados y la Unión Europea.

1.3.4. Protección hacia el alumnado

Es importante mencionar que los documentos analizados no asignan un rol activo al alumnado en materia de protección de sus propios derechos. Se los presenta como titulares de derechos que deben ser protegidos, pero no como actores con agencia en materia de su propia protección

Dicho esto, la documentación analizada presenta una variedad de medidas dirigidas a la protección de la infancia por parte de diversos actores sociales y políticos. Estas medidas incluyen indicaciones para garantizar la privacidad de los menores en el entorno digital (MP1; MP3, 11, 3), así como el etiquetado de contenidos inapropiados para su edad (MP1) y la prevención de la mercantilización de sus datos (MP9; MP7). También se abordan acciones para evitar la creación de perfiles destinados a "transmitir contenidos potencialmente nocivos con fines comerciales" (MP1, 5, 3) y la prohibición de prácticas que "manipulen o inhiban el derecho de los niños a la libertad de pensamiento y de creencias en el entorno digital" (MP1, 7, 5). Se establece además que no se debe limitar su libertad de expresión (MP1; MP3) ni obligarlos a pagar indirectamente con sus datos por servicios aparentemente gratuitos (MP1). Además de estas medidas, se mencionan los problemas asociados con el uso abusivo o

inadecuado de las tecnologías en la infancia (MP9; MP11) y los posibles efectos negativos de una sociedad cada vez más digitalizada (MP1).

Entre las propuestas que se presentan para lograr esta protección estarían, por ejemplo, la creación de un "observatorio de la Infancia que incluya a los actores y agentes con responsabilidad en el interés del menor" (MP1, 9, 3), alusiones al Reglamento General de Protección de Datos (RGPD), "que señala que los niños merecen una protección específica de sus datos personales" (MP11, 2, 3), a velar para que no se les exponga a "la violencia, la discriminación, el uso indebido de sus datos personales, la explotación comercial u otras conculcaciones de sus derechos" (MP1, 11, 9).

En el ámbito educativo se indica que cuando se usan plataformas educativas y herramientas digitales se debe analizar "su adecuación a la regulación del derecho a la protección de datos" (MP11, 5, 8) y asegurarse de que "los datos personales de los niños deben ser accesibles únicamente para las autoridades, organizaciones y personas encargadas por ley de procesarlos de conformidad con las debidas garantías (MP1, 8, 7). También se le solicita a la "comisión que aborde, en colaboración con el Comité Europeo de Protección de Datos (CEPD), la naturaleza específica de los datos sobre educación y los datos relativos a alumnos y estudiantes" (MP7, 16, 28).

Una propuesta para la protección de la infancia en el ámbito digital, que incluye a la familia, hace referencia, por ejemplo, a que el padre/madre o el/la cuidadora, deben de dar "su consentimiento informado, libre y previo al procesamiento de esos datos" (MP1, 8, 3). Para esto, las familias necesitan recibir una formación adecuada sobre el uso e impacto de los dispositivos digitales (MP1; MP7) que implica que niños y niñas puedan "retirar su consentimiento y a oponerse al procesamiento de datos personales cuando la persona encargada de procesarlos no demuestre que existen motivos legítimos e imperiosos para ello" (MP1, 8, 4).

También se encuentran referencias que, indirectamente, están dirigidas a la protección y participación digital de los menores. Por ejemplo, se asegura su alfabetización digital y mediática (MP3; MP5; MP6; MP7; MP10; MP12; MP14) para protegerles de contenidos inapropiados, contactos peligrosos, contratos abusivos y explotación. Además, se les dota de "estrategias destinadas a proteger sus datos personales y los de los demás" (MP1, 11, 10). Asimismo, se reconoce su derecho a participar en una educación digital de calidad (MP6; MP14) y en la sociedad digital (MP9).

Estas medidas no solo se refieren a las competencias digitales del alumnado, sino que también aluden a la mejora de las infraestructuras digitales para reducir las brechas tecnológicas (MP1; MP10; MP14; MP8; MP12), a la optimización de la interacción entre estudiantes y docentes (MP8), y a la atención especial que requiere el alumnado con necesidades educativas especiales, para quienes el aprendizaje en línea presenta mayores desafíos (MP7).

Entre los problemas identificados, destacan los siguientes:

> El alumnado no puede impugnar de manera efectiva los acuerdos de privacidad en los entornos educativos, ni puede negarse a proporcionar datos, aun cuando sus

> preocupaciones sean legítimas. Esta situación es especialmente preocupante en el caso de los niños que no pueden renunciar a la escolaridad obligatoria (MP7, 15, 6).
>
> Los contenidos personalizados y los anuncios que siguen a los niños en Internet distorsionan sus experiencias en línea, interfiriendo con sus derechos a la educación, a la información, a la privacidad y a la libertad de opinión y expresión (MP3, 15, 4).

Además, se señala que la mayoría de los países aún no cuentan con leyes de protección de datos específicas para la infancia (MP3). Por lo tanto, se sigue exigiendo a los proveedores de servicios digitales que implementen "marcos normativos, códigos industriales y condiciones de servicio acordes con las normas más estrictas de ética, privacidad y seguridad" (MP1, 5, 2). También se les insta a "respetar las directrices, normas y códigos pertinentes y aplicar normas de moderación de contenidos lícitas, necesarias y proporcionadas" (MP1, 6, 9). Es fundamental que el control de contenidos se equilibre con otros derechos de la infancia, en particular, los derechos a la libertad de expresión y privacidad (MP1, 6, 9)."

1.3.5. Las familias

Por lo que se refiere a las familias, encontramos algunos documentos que hacen referencia a su papel respecto a la protección de la infancia en la sociedad digital (MP1; MP6; MP7; MP14; MN3; MN4). Este rol se manifiesta en varios elementos claves, que se exponen a continuación.

En primer lugar, y en relación con un aspecto fundamental, es imprescindible que las familias puedan contar con los recursos tecnológicos necesarios en el hogar para la completa inclusión de sus hijos e hijas en el espacio digital. Aun así, este es un aspecto que no se puede delegar en las familias, ya que generaría desigualdades. Por ello, en la Resolución de 7 de julio de 2020, para la ejecución del programa "educa en Digital" (2020) se propone el plan "Puesto educativo en el hogar" que "consta de un dispositivo tipo ordenador portátil o equivalente con software de base necesario incorporando, junto con elementos de seguridad, configurado para uso educativo; y de una conexión a Internet" (MN3, 6, 5). La responsabilidad de este programa recae, entonces, en la Administración Pública.

En segundo lugar, para que las familias puedan desempeñar un papel de soporte y acompañamiento con sus hijos e hijas en su desarrollo educativo digital en los espacios digitales, es necesario que estas también reciban formación y acompañamiento. En las siguientes citas ello se pone de manifiesto (MN4):

> Asimismo, fomentarán medidas de acompañamiento a las familias, reforzando y apoyando el rol de los progenitores a través del desarrollo de competencias y habilidades que favorezcan el cumplimiento de sus obligaciones legales, y, en particular, las establecidas en el artículo 84.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales (MN4, 35, 8).

> Subraya el papel cada vez más importante que desempeñan los padres, las familias [...] y la necesidad de que cuenten con buenas capacidades técnicas, digitales y en relación con internet, así como con equipos adecuados, y pide que se les faciliten mecanismos especiales de formación y apoyo; hace hincapié en la necesidad de prestar asistencia a las familias en lo que respecta a las herramientas digitales, a fin de aumentar el acceso a la educación a distancia (MP7, 15).

Además, también se insta a las familias a hacer uso de mecanismos de control parental, así como de herramientas de denuncia y bloqueo con la finalidad de proteger a los y las menores (MN4, 36, 7). Al mismo tiempo se sugiere a las familias ser conscientes de que muchas de las amenazas a la privacidad de la infancia "pueden surgir como resultado [...] de las actividades de los miembros de la familia [...] por ejemplo cuando los padres publican fotografías en línea" (MP1, 7, 12-13).

En tercer lugar, se considera vital que las familias se involucren activamente en la educación digital de sus hijos e hijas. En este sentido, "[La] participación de los padres para tener una educación y formación digitales de calidad, accesibles e inclusivas debería ser más activa y estrecha" (MP6, 10, 1). Además, en el documento MP14 se habla sobre el papel de la familia en la escuela a través de la comunicación con esta institución (14,3).

En cuarto lugar, uno de los ejercicios clave de las familias es el de otorgar o no consentimiento para el procesamiento de los datos, producidos en espacios digitales, de sus hijos e hijas. Para ello, es imprescindible que "el padre o el cuidador, den su consentimiento informado, libre y previo al procesamiento de esos datos" (MP1, 8, 3). Además, las familias, a nivel global, poseen la capacidad de retirar su consentimiento en cualquier momento, así como de tener acceso a los datos de sus hijos e hijas (MP1, 8, 4).

A modo de resumen, en los documentos consultados se muestra el rol de las familias como acompañantes en el proceso de educación digital de sus hijos e hijas. No obstante, recaen sobre ellas algunas acciones concretas como la de otorgar o no consentimiento para el tratamiento de los datos de los y las menores generados en espacios digitales, así como la de colaborar con las escuelas. En definitiva, tal y como expone el documento MP7, "Los padres son también esenciales para orientar a los niños en el entorno en línea" (22, 1).

1.3.6. Análisis sobre la coherencia entre actores dentro de la escuela

A lo largo de las secciones de las que se compone el apartado fue posible identificar el rol que los marcos políticos y normativos analizados brindan a los distintos actores escolares en materia de protección de la infancia.

Ello nos permite presentar, a modo de resumen, tanto la caracterización de los roles como de las acciones asociadas a ellos en el contexto de la sociedad digital.

Así, los centros educativos son presentados en los documentos analizados como entornos facilitadores de la educación digital y, por tanto, como entornos básicos de la protección de los derechos de la infancia. Las acciones que se les asignan, entonces, están signadas por la provisión de tecnología, formación e información. También aparecen a cargo de la definición de protocolos específicos de prevención y de su divulgación con la comunidad escolar.

Ello nos lleva al segundo actor, el equipo directivo, el cual es representado como líder de la transformación digital del centro, y, por tanto, responsable de gran parte de las acciones que aparecen adosadas a la escuela como entorno. Por ello, la principal tarea asignada al rol directivo en los documentos analizados es la de dirigir el Plan Digital del Centro, que tiene la completa y efectiva integración de tecnología con sentido pedagógico como función inherente. Ello contempla tanto la provisión de hardware, software y formación, como la definición de políticas escolares de protección de datos.

Hasta aquí, el rol de los actores en materia de protección de la infancia gira en dos intensidades. Por un lado, los actores macroeducativos (instituciones, por ejemplo) operan a nivel normativo, mientas que, por otro lado, actores de nivel microeducativo trabajan el tema de la protección a nivel individual y contextual.

Los documentos analizados presentan al profesorado como el miembro de la comunidad educativa garante del cuidado, la asistencia, la enseñanza y la protección de la infancia y adolescencia en los entornos digitales. Por tanto, las acciones asociadas a este rol se vinculan con la incorporación con sentido de la tecnología digital en las prácticas de enseñanza y de aprendizaje; estas deben ser innovadoras para favorecer la adquisición de habilidades digitales por parte de los estudiantes; deben, además, promover un uso responsable y saludable de las tecnologías para proteger a los estudiantes de un uso intensivo y de la generación de trastornos conductuales; y, finalmente, deben promover la conciencia crítica y la protección de los datos personales para fomentar que el estudiantado ejerza una ciudadanía responsable.

Ahora bien, si el profesorado aparece como garante último de los derechos de la niñez, ¿qué rol juegan las familias? De la misma forma que se puede hablar de coordinación entre los organismos educativos y el equipo directivo de la escuela, a nivel microeducativo, observamos una conexión entre el profesorado y las familias, en tanto estas últimas aparecen en los textos analizados como las responsables de brindar el entorno individual de soporte y acompañamiento a sus hijos e hijas. Por ello, las acciones asignadas a las familias están vinculadas al control parental en el uso de los dispositivos, para proteger a los estudiantes de situaciones de abuso o violencia, así como a su responsabilidad en la autorización de la cesión de datos del alumnado que se requieren para el uso de muchos de los entornos digitales.

Finalmente, tal como ya hemos mencionado, los documentos analizados no asignan un rol activo al alumnado en materia de protección de sus propios derechos. Se los presenta como titulares de derechos que deben ser protegidos, pero no como actores con agencia en materia de su propia protección. Está última en el ámbito digital se presenta vinculada a cuestiones como la privacidad, la protección de datos, el cuidado de la exposición a contenidos dañinos, la prevención del consumo problemático de tecnología y, finalmente, a cuestiones vinculadas con la equidad en el acceso tanto a infraestructuras como a servicios digitales.

De este modo podemos concluir que, en los marcos políticos y normativos consultados, la protección de la infancia en el entorno digital es una responsabilidad institucional y de las personas adultas. Ahora bien, directivos, docentes y familias comparten la necesidad de acciones de formación específica que les brinden las herramientas necesarias para llevar adelante las tareas asignadas a su rol, siendo clave también la garantía del acceso a un mínimo de infraestructura en hardware y software para llevarlas adelante.

Asimismo, el análisis realizado sugiere la necesidad de un cambio en el rol del alumnado, para que pueda convertirse en un actor más activo en la protección de sus propios derechos.

1.3.7. Síntesis

A modo de síntesis, los marcos normativos y políticos analizados otorgan las siguientes responsabilidades respecto a la protección de la infancia digital a cada uno de los actores:

Centros educativos:

- Provisión de recursos para garantizar el acceso a la tecnología digital al alumnado.
- Fomento del uso de tecnologías digitales en los procesos de enseñanza y aprendizaje.
- Adopción de medidas para proteger al alumnado de situaciones de violencia, exposición de la privacidad y acceso a contenidos perjudiciales.

Equipos directivos:

- Liderazgo pedagógico del proceso de transformación digital en las escuelas.
- Prevención de situaciones de violencia, exposición de la privacidad y acceso a contenidos perjudiciales.
- Protección de los datos del alumnado.

Profesorado:

- Aplicación de metodologías de enseñanza y de aprendizaje diseñadas para el entorno digital.
- Garantía de la salud digital y la prevención del uso indebido y/o adictivo de las TIC.
- Innovación en los procesos de enseñanza y aprendizaje con utilización de TIC, creando contenidos y compartiendo prácticas.

Familias:

- Acompañamiento de sus hijos e hijas en espacios digitales.
- Uso de mecanismos de control parental, así como de herramientas de denuncia y bloqueo con la finalidad de proteger a los y las menores.
- Decisión sobre el consentimiento informado para el procesamiento de los datos de sus hijos e hijas que se generan en el uso de entornos digitales.

Alumnado:

En el apartado referido a este colectivo no se presenta su responsabilidad respecto a la protección de la infancia en la sociedad digital, ya que se lo considera objeto de la acción. Es decir, según los documentos consultados, el resto de los colectivos debe garantizar la protección del alumnado en entornos digitales.

1.3.8 Listado de documentos incluidos

MP1: Organización de las Naciones Unidas. (2021). *Observación General Nº 25, relativa a los derechos de los niños en relación con el entorno digital, Convención sobre los Derechos del Niño.* https://bit.ly/4gWWnXx

MP3: Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/4elJBzM

MP5: Parlamento Europeo. (2023). *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital. https://bit.ly/4ekjpWx*

MP6: Comisión Europea, Dirección General de Educación, Juventud, Deporte y Cultura, (2023). *Plan de acción de educación digital 2021-2027: mejorar la provisión de capacidades digitales en la educación y la formación*, Oficina de Publicaciones de la Unión Europea. https://bit.ly/47HzzXr

MP7: Parlamento Europeo. (2021). *Propuesta de resolución del Parlamento Europeo: Informe sobre la formulación de la política de educación digital*. https://bit.ly/47Ma8E6

MP8: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 21: Modernización y digitalización del sistema educativo, incluida la educación temprana de 0-3 años*. https://bit.ly/3XIqtoH

MP9: Pacto de Estado. (2023). Protegiendo a la infancia y la adolescencia en el entorno digital, medidas de consenso para un Pacto de Estado ante la nueva legislatura y la presidencia de España en la Unión Europea. https://bit.ly/3BhnMTq

MP10: Gobierno de España. (n.d.). *España Digital 2026.*

MP11: Agencia Española de Protección de Datos. (2024). *Menores, salud digital y privacidad: Estrategia y líneas de acción*. https://bit.ly/3ZHFGcd

MP12: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 19. Plan Nacional de Capacidades Digitales.* https://bit.ly/3ZKocvM

MP14: Generalitat de Catalunya. Departament d'Educació. (2020). *Pla d'educació digital de Catalunya 2020-2023*. https://bit.ly/3z33nyv

MN3: Resolución, *de la Subsecretaría, por la que se publica el Convenio entre el Ministerio de Educación y Formación Profesional, el Ministerio de Asuntos Económicos y Transformación Digital y la Entidad Pública Empresarial Red.es, M.P., para la ejecución del programa "Educa en Digital"* (7 de julio de 2020). https://bit.ly/3XMmtDP

MN4: Ley Ogánica N° 8, *Ley de protección integral a la infancia y la adolescencia frente a la violencia* (4 de junio de 2021). https://bit.ly/4doiVx1

MN7: Gobierno de España. (2021). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia*. https://bit.ly/4eiIxgn

MN10: Orden N° 178, *de la Consejería de Educación, Cultura y Deportes, por la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios* (14 de septiembre de 2022). https://bit.ly/3MZMhr0

MN11: Resolución, *de la Subsecretaría de la Conselleria de Educación, Investigación, Cultura y Deporte, por la que se dictan instrucciones para el cumplimiento de la normativa de protección de datos en los centros educativos públicos de titularidad de la Generalitat* (28 de junio de 2018). https://bit.ly/3Y0kfBL

Otras referencias

Boly Barry, K. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación: Informe de la Relatora Especial sobre el derecho a la educación* (Consejo de Derechos Humanos, 50º período de sesiones, Tema 3 de la agenda, A/HRC/50/32). Naciones Unidas. https://bit.ly/3TL770W

Anexos

Tabla 4

Listado y distribución de los documentos empleados para cada actor

Nº Documento	Centros educativos	Equipos directivos	Profesorado	Alumnado	Familias
MP1	X		X	X	X
MP3	X	X	X	X	
MP5			X	X	
MP6	X		X	X	
MP7			X	X	X
MP8			X	X	
MP9			X	X	
MP10				X	
MP11			X	X	
MP12		X	X	X	
MP14	X	X	X	X	
MN3		X	X		X
MN4	X	X	X		X
MN7			X		
MN10	X	X			
MN11		X			

Fuente: Elaboración propia

1.4. Las Corporaciones Tecnológicas y la protección de la infancia

Las Corporaciones Tecnológicas desempeñan un papel fundamental en la protección de la infancia en el entorno digital. Estas empresas no solo deben cumplir con las normativas legales, sino también asumir una responsabilidad social y educativa que garantice la seguridad y el bienestar de niños y niñas, y respete sus derechos. Al respecto, en el documento "Repercusiones de la digitalización de la educación en el derecho a la educación. Informe de la relatora Especial sobre el derecho a la educación" de la ONU (MP3) se manifiesta que:

> […] las empresas deben prevenir, mitigar y, en su caso, remediar los abusos contra los derechos humanos que causen o a los que contribuyan. Estos Principios Rectores se aplican a todos los Estados y a todas las empresas, tanto transaccionales como de otro tipo, con independencia de su tamaño, sector, ubicación, propietarios y estructura (MP3, 7, 1).

De acuerdo con lo expresado aquí, las Corporaciones Tecnológicas están obligadas a crear y mantener un entorno digital seguro para todo aquel que haga uso de ellas, y en especial para los niños y niñas. Esto implica la implementación de controles de seguridad rigurosos y la protección de la privacidad y de los datos personales. Al mismo tiempo, la Observación General nº25 de las Naciones Unidas (MP1) plantea que:

> El entorno digital abarca empresas que dependen económicamente del procesamiento de datos personales para orientar contenidos generadores de ingresos o de pago, y esos procesos afectan de manera tanto intencional como no intencional las experiencias digitales de los niños (MP1, 12, 2).

Esta cita subraya la importancia de gestionar éticamente la información personal y proteger a los y las menores de posibles abusos.

Las Corporaciones Tecnológicas, por tanto, se sitúan en un marco de responsabilidades sistémico, en el que participan múltiples actores, como Estados, organizaciones no gubernamentales (ONGs), organismos internacionales, y diversos agentes territoriales, donde la colaboración es algo fundamental a la hora de pensar y establecer políticas y prácticas efectivas que protejan a la infancia y la juventud en el entorno digital.

> El carácter transfronterizo y transnacional del entorno digital requiere una fuerte cooperación internacional y regional para garantizar que todas las partes interesadas, incluidos los Estados, las empresas y otros agentes, respeten, protejan y hagan efectivos los derechos de los niños en relación con el entorno digital. Por tanto, es fundamental que los Estados parte cooperen bilateral y multilateralmente con las organizaciones no gubernamentales nacionales e internacionales, los organismos de las Naciones Unidas, las empresas y las organizaciones especializadas en la protección y los derechos humanos de los niños en relación con el entorno digital (MP1, 13, 6-7).

Ahora bien, tras analizar los documentos seleccionados, hemos identificado varias responsabilidades específicas en las que es fundamental centrarse, dado el rol que estas empresas desempeñan en la protección de la infancia en el entorno digital. No se trata de un listado exhaustivo, sino de algunos de los aspectos más destacados que hemos observado en la documentación revisada.

1.4.1. Análisis de la responsabilidad social y educativa

La responsabilidad social y educativa de las Corporaciones Tecnológicas se centra en la creación de un entorno digital seguro y educativo. Un análisis detallado de los documentos revela que estas empresas deben equilibrar sus objetivos comerciales con la protección de los derechos de los niños y niñas:

> Los Estados parte tienen la obligación de proteger a los niños frente a cualquier conculcación de sus derechos por parte de empresas comerciales, lo que incluye al derecho a gozar de protección contra todas las formas de violencia en el entorno digital. Aunque las empresas no estén directamente involucradas en la comisión de actos perjudiciales, pueden causar o propiciar violaciones del derecho de los niños a vivir libres de violencia, por ejemplo, como resultado del diseño y el funcionamiento de sus servicios digitales. Los Estados parte deben establecer leyes y reglamentos destinados a impedir las vulneraciones del derecho a la protección contra la violencia, así como a investigar, juzgar y reparar las vulneraciones que se produzcan en relación con el entorno digital, y deben vigilar y exigir su cumplimiento. (MP1, 4, 12)

Garantizar la seguridad del entorno digital de parte de estas entidades, resulta primordial. Al mismo tiempo, se resalta la necesidad de una gestión ética de los datos y la protección contra el abuso de información personal, más aún, considerando que las Corporaciones Tecnológicas responden a lógicas comerciales diferentes de las educativas:

> Las empresas deben implementar medidas que protejan la privacidad y seguridad de los menores en sus plataformas digitales (MP1, 4, 10-11).

> El entorno digital abarca empresas que dependen económicamente del procesamiento de datos personales para orientarlos contenidos generadores de ingresos o de pago, y esos procesos afectan de manera tanto intencional como no intencional las experiencias digitales de los niños. Muchos de esos procesos entrañan la participación de múltiples socios comerciales, lo que crea una cadena de suministro de actividades comerciales y de procesamiento de datos personales que puede dar lugar a violaciones o vulneraciones de los derechos de los niños, por ejemplo como resultado de características de diseño publicitario que anticipan las acciones del niño y lo guían hacia la búsqueda de contenidos más extremos, de notificaciones automatizadas que pueden interrumpir el sueño o del uso de la información personal o la ubicación de un niño para transmitir contenidos potencialmente nocivos con fines comerciales. (MP1 40, 12, 2).

Por último, respecto a la responsabilidad social y educativa de las Corporaciones Tecnológicas emerge una nueva mirada que incide en la oportunidad de:

> […] establecer un marco legal de rendición de cuentas para los directivos responsables de las plataformas de intercambios de vídeos y distribuidores de contenidos que incumplan con el establecimiento de la obligación de verificación de edad (MP9, 5, 8).

1.4.2. Análisis de la innovación tecnológica

De acuerdo con los documentos revisados, la innovación tecnológica en la protección infantil se presenta tanto en el desarrollo de herramientas específicas como en la implementación de políticas que promuevan tecnologías más seguras (MN3, 2, 5; MN4, 20, 9-10). El marco normativo destaca la importancia de que las empresas desarrollen nuevas soluciones que refuercen la seguridad en línea de los menores. Asimismo, las administraciones públicas deben colaborar con el sector privado para fomentar la creación de entornos digitales seguros, considerando siempre la protección de los niños y adolescentes:

> Las administraciones públicas deberán adoptar medidas para incentivar la responsabilidad social de las empresas en materia de uso seguro y responsable de Internet por la infancia y la adolescencia. Asimismo, fomentarán en colaboración con el sector privado que el inicio y desarrollo de aplicaciones y servicios digitales tenga en cuenta la protección a la infancia y la adolescencia (MN4, 36, 2-3).

En cuanto a la inteligencia artificial (IA), los documentos destacan su uso creciente para identificar y filtrar contenido inapropiado, así como para detectar comportamientos que puedan implicar riesgos de acoso o abuso en línea. Este tipo de innovación tecnológica está cada vez más presente en la protección infantil: "Las tecnologías de IA pueden identificar patrones de comportamiento que indican riesgos para los niños y actuar en consecuencia" (MP1, 56, 9).

No obstante, los marcos analizados subrayan que las tecnologías de filtrado de contenido no deben comprometer el acceso de los menores a oportunidades de aprendizaje. La regulación aboga por una mayor estandarización en el etiquetado de contenidos, con el objetivo de apoyar tanto a los niños y niñas como a sus tutores y tutoras en la selección adecuada de los mismos:

> Las administraciones públicas fomentarán la colaboración con el sector privado para la creación de entornos digitales seguros, una mayor estandarización en el uso de la clasificación por edades y el etiquetado inteligente de contenidos digitales (MN4, 36, 6).

La educación digital también juega un papel fundamental en este contexto, siendo clave en la formación de menores para un uso seguro y responsable del entorno digital, como se destaca en el marco normativo: "La inclusión de la educación digital en el currículo escolar prepara a los niños para un entorno digital seguro y responsable" (MN3, 20, 8).

Otro aspecto crítico es la verificación de edad, identificada como una medida esencial para impedir que los menores accedan a contenido inapropiado. Los documentos señalan que las empresas deben adoptar mecanismos sólidos para cumplir con esta responsabilidad: "Las empresas deben implementar sistemas de verificación de edad robustos para asegurar que los menores no accedan a contenido destinado a adultos" (MN4, 20, 8).

Finalmente, en relación con la inclusión de personas con necesidades especiales, los documentos reflejan que, si bien las empresas tecnológicas se han presentado como solución para mejorar el acceso de las comunidades más necesitadas, la evidencia de que lo logren eficazmente es limitada:

> Las empresas tecnológicas se han ofrecido como la solución para mejorar el acceso y el apoyo a las 'personas más necesitadas'. Sin embargo, hay pocas pruebas de que las empresas atiendan eficazmente a las comunidades de difícil acceso (MP3, 12, 2).

En definitiva, los documentos revisados ponen de manifiesto que la innovación tecnológica debe orientarse hacia la protección de la infancia en el entorno digital, respetando los derechos de la infancia. Tanto el uso de tecnologías como la implementación de políticas efectivas son esenciales para garantizar la seguridad y el acceso adecuado a los contenidos en línea. Asimismo, se destaca la importancia de la educación digital y la verificación de edad como herramientas clave en la protección infantil.

1.4.3 Garantizar el rol protector a las propias familias

La protección de la infancia es una responsabilidad irrenunciable de las familias y tutores (MN7; MN9). Por tanto, las Corporaciones Tecnológicas deben garantizar la presencia de recursos y herramientas de control parental que permitan a los padres, madres y tutores supervisar y gestionar el acceso de sus hijos e hijas a contenido en línea (MN7). Al respecto, uno de los documentos políticos analizados destaca lo siguiente: "Las empresas deben proporcionar herramientas efectivas para que los padres puedan monitorear y controlar las actividades en línea de sus hijos" (MP1, 40, 2).

En este contexto, el reciente Anteproyecto de Ley Orgánica para la protección de menores en entornos digitales (Ministerio de Juventud e Infancia del Gobierno de España, 2024) establece que los fabricantes de dispositivos digitales deberán garantizar que estos cuenten con sistemas de control parental activados por defecto, además de un etiquetado informativo sobre los riesgos asociados:

> Los fabricantes estarán obligados a garantizar que los dispositivos a los que se refiere este artículo incluyan una funcionalidad de control parental de servicios, aplicaciones y contenidos, cuya activación debe producirse por defecto en el momento de la configuración inicial del dispositivo. La inclusión de la funcionalidad, su activación, configuración y actualización serán gratuitas para el usuario (artículo 4 del Título I del anteproyecto de ley).

Adicionalmente, las administraciones públicas, en colaboración con el sector privado y el tercer sector, tienen la responsabilidad de fomentar el desarrollo de contenidos positivos en línea adaptados a diferentes grupos de edad (MP13). Los marcos normativos analizados subrayan la importancia de impulsar códigos de autorregulación y corregulación dentro de la industria para asegurar el uso seguro y responsable de los productos y servicios dirigidos a la infancia y adolescencia. Además, se hace hincapié en la incorporación de mecanismos de control parental y verificación de edad para impedir el acceso de menores a contenidos reservados para adultos:

> Las administraciones públicas, en colaboración con el sector privado y el tercer sector, fomentarán los contenidos positivos en línea y el desarrollo de contenidos adaptados a las necesidades de los diferentes grupos de edad, impulsando entre la industria códigos de autorregulación y corregulación para el uso seguro y responsable en el desarrollo de productos y servicios destinados al público infantil y adolescente. Asimismo, reforzarán la incorporación por parte de la industria de mecanismos de control parental de los contenidos ofrecidos o mediante la puesta en marcha de protocolos de verificación de edad, en aplicaciones y servicios disponibles en Internet para impedir el acceso a los reservados a adultos (MN4, 36, 8).

En síntesis, los documentos analizados subrayan la importancia de que las Corporaciones Tecnológicas no solo desarrollen herramientas seguras, sino que también garanticen que las familias puedan desempeñar el rol esencial que tienen en la protección de la infancia en el entorno digital. El control parental se presenta como una herramienta útil en este sentido para que los padres, madres y tutores puedan supervisar y regular el acceso de los menores a contenidos en línea, actuando como una barrera efectiva frente a los riesgos del entorno digital.

1.4.3. Análisis de la relación con el sistema educativo

Los documentos revisados enfatizan la importancia de la relación entre las Corporaciones Tecnológicas y el sistema educativo para maximizar el impacto positivo de la tecnología en la educación y la protección infantil (MP3, 7, 1). Sin embargo, estas corporaciones tienen la responsabilidad de rendir cuentas sobre sus acciones, tanto en términos de los servicios digitales que ofrecen como de su impacto en el sistema educativo (MP3, 14, 1; MP9, 5, 8).

La colaboración entre las empresas tecnológicas y las instituciones educativas es fundamental para integrar la seguridad digital y la alfabetización tecnológica en los currículos escolares. Los documentos analizados destacan que este tipo de cooperación asegura que el alumnado reciba una educación integral sobre el uso seguro y responsable de la tecnología: "La colaboración entre empresas tecnológicas e instituciones educativas es vital para desarrollar un currículo que incluya la seguridad digital y la alfabetización tecnológica" (MN3, 3, 3).

Junto a lo anterior, las corporaciones deben facilitar programas de formación dirigidos a docentes, con el fin de que puedan transmitir a los estudiantes los conocimientos necesarios

para navegar de manera segura en el entorno digital (MP1, 6, 10). Este tipo de iniciativas es clave para fortalecer el papel de la educación en la protección infantil en el entorno digital.

Por otro lado, el papel de las corporaciones en la provisión de servicios digitales a las escuelas también debe alinearse con el derecho a la participación. La ONU (2022) (MP3) subraya la importancia de que las organizaciones privadas rindan cuentas de su trabajo digital y de que la población pueda participar activamente en la supervisión y los avances en educación digital: "Las organizaciones privadas deben rendir cuentas de su trabajo digital y la población debe poder participar activamente en los avances de la educación digital y supervisarlos" (MP3, 14, 1).

En síntesis, los documentos revisados destacan la necesidad de que las Corporaciones Tecnológicas colaboren de manera activa y transparente con el sistema educativo. Y no solo lo hagan desde la generación y distribución de tecnologías digitales, sino también a la hora de integrar la seguridad digital en los currículos escolares, y de asegurar que el profesorado y alumnado participen activamente en las decisiones sobre la construcción del entorno digital, y que puedan estar adecuadamente preparados para enfrentar los desafíos. Al mismo tiempo, se resalta la importancia de la rendición de cuentas y la disposición que deben tener estas instituciones durante estos procesos.

1.4.4. Síntesis

El análisis de los documentos nos permite establecer que las Corporaciones Tecnológicas tienen un papel vital en la protección de la infancia en el entorno digital. A través de su responsabilidad social y educativa, la innovación tecnológica, la vinculación con las familias y la colaboración con el sistema educativo, estas empresas deben garantizar un entorno digital seguro y beneficioso para la infancia.

Es importante considerar cómo cada una de estas áreas se interrelaciona y potencia mutuamente. La responsabilidad social no solo implica cumplir con la ley, sino también anticiparse a las necesidades emergentes de la seguridad digital y adoptar una postura ética proactiva. La innovación tecnológica y en general, la creación de medios digitales y algoritmos de inteligencia artificial no solo debe responder a los desafíos actuales, sino que también debe adaptarse continuamente para anticipar nuevas amenazas. En esta línea, las Corporaciones Tecnológicas no deben privar a las familias de su derecho y responsabilidad en la protección de la infancia en la sociedad digital. Finalmente, la relación con el sistema educativo es fundamental para asegurar que el alumnado no solo esté protegido en línea, sino que también estén equipados con las habilidades necesarias para navegar por el entorno digital de manera segura y responsable.

En síntesis, las corporaciones deben trabajar con instituciones educativas, familias y menores para desarrollar currículos que integren la seguridad digital, la privacidad y la ética tecnológica desde temprana edad garantizando el derecho a la participación.

Finalmente, a partir de los documentos analizados identificamos que las principales responsabilidades de las Corporaciones Tecnológicas en la protección de la infancia en la sociedad digital son las siguientes:

- Asumir una responsabilidad social y educativa que garantice la seguridad y el bienestar de los menores, y respete sus derechos. Tienen la obligación de prevenir, mitigar y, en su caso, remediar los abusos contra los derechos humanos que causen o a los que contribuyan (MP1, MN7).
- Crear y mantener un entorno digital seguro en especial para los niños y niñas. Esto implica la implementación de controles de seguridad rigurosos, la protección de datos personales, la gestión ética de la información personal y la protección a los y las menores de posibles abusos (MN4, MP9).
- Invertir en la creación de entornos que promuevan oportunidades en la alfabetización digital y la seguridad en línea para niños, niñas y adolescentes desarrollando buenas prácticas en el desarrollo tecnológico y generando oportunidades de aprendizaje al alumnado mediante acciones formativas específicas y la transparencia en el uso de datos (MP3, MN3).
- Proporcionar herramientas efectivas para que los padres puedan monitorear y controlar las actividades en línea de sus hijos. Están obligadas a incluir una funcionalidad de control parental de servicios, aplicaciones y contenidos, cuya activación debe producirse por defecto en el momento de la configuración inicial del dispositivo. La inclusión de la funcionalidad, su activación, configuración y actualización serán gratuitas para el usuario (Anteproyecto de Ley Orgánica para la protección de menores en entornos digitales, 2024) (MN4, MP9).
- Proteger contra todas las formas de violencia en el entorno digital (MN4, MP9).
- Implementar medidas que protejan la privacidad y seguridad de los menores en sus plataformas digitales (MN7, MP1).
- Ofrecer soluciones para mejorar el acceso y el apoyo a las "personas más necesitadas" (MP3, MN3).
- Crear entornos digitales seguros con una mayor estandarización en el uso de la clasificación por edades y el etiquetado inteligente de contenidos digitales, para conocimiento de los niños, niñas y adolescentes y apoyo de los progenitores o tutores. Las empresas deben implementar sistemas de verificación de edad robustos para asegurar que los menores no accedan a contenido destinado a adultos (MN4, MP9).
- Colaborar con las instituciones educativas para desarrollar contenidos curriculares que incluyan la seguridad digital y ofrecer programas de formación para que los docentes puedan enseñar a los estudiantes sobre el uso seguro y responsable de la tecnología (MP3, MN3).

1.4.5 Listado de documentos consultados para la redacción del apartado

MP1: Organización de las Naciones Unidas. (2021). *Observación General Nº 25, relativa a los derechos de los niños en relación con el entorno digital, Convención sobre los Derechos del Niño.* https://bit.ly/4gWWnXx

MP3: Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/4elJBzM

MP9: Pacto de Estado. (2023). Protegiendo a la infancia y la adolescencia en el entorno digital, medidas de consenso para un Pacto de Estado ante la nueva legislatura y la presidencia de España en la Unión Europea. https://bit.ly/3BhnMTq

MN3: Resolución, *de la Subsecretaría, por la que se publica el Convenio entre el Ministerio de Educación y Formación Profesional, el Ministerio de Asuntos Económicos y Transformación Digital y la Entidad Pública Empresarial Red.es, M.P., para la ejecución del programa "Educa en Digital"* (7 de julio de 2020). https://bit.ly/3XMmtDP

MN4: Ley Ogánica N° 8, *Ley de protección integral a la infancia y la adolescencia frente a la violencia* (4 de junio de 2021). https://bit.ly/4doiVx1

MN7: Gobierno de España. (2021). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia*. https://bit.ly/4eiIxgn

MN9: Ley N° 7, Ley de Atención y Protección a la Infancia y la Adolescencia de Castilla-La Mancha (10 de marzo de 2023). https://bit.ly/3BgdqmL

Otras referencias

Ministerio de Juventud e Infancia del Gobierno de España (2024). Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. https://bit.ly/4engYlQ

1.5. El rol de los actores de significación jurídica en la protección de la infancia en la sociedad digital

Este presente apartado presenta el rol de actores de significación jurídica que han sido claramente identificados en el análisis de los documentos normativos y políticos. En esta sección no se incluyen ni la Administración Pública, ni las escuelas, ni las Corporaciones Tecnológicas, ya que estos actores fueron tratados previamente. Los actores descritos a continuación operan en un marco normativo y político internacional, europeo, estatal y autonómico, y su responsabilidad en la protección de la infancia en el entorno digital está definida y respaldada por los convenios, leyes y estrategias examinadas en dichos documentos.

1.5.1 Principales actores identificados

En función del análisis de los documentos normativos y políticos, se identifican organismos internacionales como la Organización de Naciones Unidas (ONU), UNESCO y UNICEF, entre otros, que establecen directrices y comprometen a los Estados miembro a cumplir con normas y estándares que protegen los derechos de la infancia en el entorno digital, haciendo prevalecer el interés superior del niño por sobre cualquier acción comercial o política (MP1; MP2; MP3). De acuerdo con estos documentos, los Estados miembro de la ONU se comprometen a garantizar que la publicidad y comercialización dirigidas a niños y niñas estén claramente diferenciadas de otros contenidos, evitando la perpetuación de estereotipos de género o raza (MP1, 5, 5). Además, se subraya que los Estados deben prohibir la elaboración de perfiles o la selección de niños con fines comerciales, incluidos los registros digitales de características reales o inferidas, así como cualquier práctica de publicidad subliminal o inmersiva que interactúe con menores en entornos de realidad virtual o aumentada (MP1, 5, 4; MP3).

En el ámbito europeo, algunos de los documentos analizados destacan el papel clave del Consejo de Europa, el Parlamento Europeo y la Comisión Europea en la promoción de convenios y regulaciones vinculadas a la protección de la infancia en la sociedad digital. Entre ellos, se mencionan convenios como el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (1981) y el Convenio sobre la Ciberdelincuencia (MP4, MP5), que establecen directrices claras sobre la protección de los datos personales y la lucha contra los delitos en línea. Junto a esto, algunos de los documentos normativos y políticos revisados (MN4, MP5), destacan la Estrategia del Consejo de Europa para los Derechos del Niño (2016-2021), en relación con el énfasis que pone en la necesidad de abordar integralmente la protección de la infancia en la sociedad digital.

El Parlamento Europeo ha jugado un rol destacado en el desarrollo de políticas educativas vinculadas al entorno digital. En colaboración con la Comisión Europea, se han implementado iniciativas como el Plan de Acción de Educación Digital 2021-2027 (Comisión Europea, MP6) y la Propuesta de Resolución sobre la Formulación de la Política de Educación Digital (2021, MP7). Estas iniciativas subrayan la necesidad de dotar a los educadores y estudiantes de competencias digitales adecuadas y de garantizar un entorno digital seguro para el

aprendizaje. Además, la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2022) (MP5) de la Comisión Europea, subraya la importancia de promover una educación digital inclusiva y proteger los derechos de los niños y adolescentes en el entorno digital. Todas estas iniciativas están alineadas con los objetivos establecidos en el Reglamento General de Protección de Datos (2016) y la Directiva sobre Privacidad y Comunicaciones Electrónicas (MP2, MN2, MN1).

En el contexto español, algunos de los documentos revisados (MP8; MP12; MN4; MN6; MN8; MN12) destacan el papel de la Agencia Española de Protección de Datos (AEPD), que es clave en la protección de los datos personales de los menores. Según lo establecido en estos documentos, la AEPD tiene la responsabilidad de garantizar los derechos digitales de los menores y de retirar de forma rápida los contenidos ilícitos, especialmente cuando se refieren a violencia contra la infancia y adolescencia (MN4). La AEPD puede cooperar con otras entidades para promover un entorno digital seguro (MP6).

Las Fuerzas y Cuerpos de Seguridad del Estado, tal como se señala en algunos de los documentos analizados (MN4; MN12; MP11) tienen un rol relevante en la protección de la infancia digital. Se encargan de la detección, prevención y erradicación de la violencia contra la infancia, colaborando con otros actores para garantizar la existencia de canales accesibles y seguros de denuncia. Estos canales están gestionados a través de redes nacionales e internacionales (MN4, 24, 10). Junto a esto, la Ley Orgánica 8/2021 (MN4) indica que cualquier persona que tenga conocimiento de contenidos en Internet que constituyan una forma de violencia contra un menor tiene la obligación de denunciar dicha situación (MN4, 24, 9).

En cuanto al sistema de justicia, los documentos subrayan que su intervención es clave para la protección de los derechos de los menores en entornos digitales. Las actuaciones judiciales deben garantizar la privacidad y la protección de los datos personales de los menores, según lo establecido en la Ley Orgánica 3/2020, de 29 de diciembre, que modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación (MN12).

A nivel autonómico también existen este tipo de actores de significación jurídica, más o menos desarrollados en función de la región, que difieren de la Administración. En concreto, los documentos analizados destacan el rol de la Autoridad Catalana de Protección de Datos (MN8; MP13), encargada de garantizar el derecho a la protección de datos personales dentro de las competencias de la Generalitat. Además, esta entidad puede establecer convenios de colaboración con el *Síndic de Greuges*, síndicos locales y otros organismos de defensa de los derechos de las personas para asegurar una protección efectiva en el entorno digital (MN8).

El *Síndic de Greuges* (Defensor del Pueblo en Cataluña) es reconocido en algunos documentos (MN8; MP13) como una figura clave en la protección de los derechos de los menores en el entorno digital, asegurando que las quejas y denuncias sean atendidas de manera adecuada. Trabaja en colaboración con la Autoridad Catalana de Protección de Datos y otras entidades para garantizar que se respeten los derechos de la infancia en la sociedad digital.

1.5.2 Síntesis

De acuerdo con los documentos normativos y políticos analizados, los actores mencionados desempeñan un papel relevante en la protección de la infancia en el entorno digital. Desde los organismos internacionales, las agencias de protección de datos, hasta las fuerzas de seguridad, la justicia y los defensores del pueblo, todos ellos son actores que también intervienen a la hora de garantizar un entorno seguro para la infancia, conforme a lo establecido en las normativas internacionales, europeas y autonómicas revisadas.

1.5.3 Listado de documentos incluidos

MP1: Organización de las Naciones Unidas. (2021). *Observación General Nº 25, relativa a los derechos de los niños en relación con el entorno digital, Convención sobre los Derechos del Niño.* https://bit.ly/4gWWnXx

MN4: Ley Ogánica N° 8, *Ley de protección integral a la infancia y la adolescencia frente a la violencia* (4 de junio de 2021). https://bit.ly/4doiVx1

MN8: Ley 23/2010, de 1 de octubre, *de la Autoridad Catalana de Protección de Datos*, (8 de octubre de 2010). https://bit.ly/3ZDt85J

MN12: Ley Orgánica N° 3, *Ley por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación* (29 de diciembre de 2020). https://bit.ly/3ZHHXUX

2. Segunda parte. Preguntas sobre las tensiones y acuerdos entre marcos normativos y políticos para la protección de la infancia en la sociedad digital

En el presente apartado, se exponen algunas preguntas que los investigadores e investigadoras del proyecto se plantearon durante la fase de análisis documental con la finalidad de dar respuesta a cómo se debe proteger a la infancia en la sociedad digital, según los documentos normativos y políticos consultados. Para ello, primeramente, se abordan tanto la coherencia entre el marco político y normativo, como la coherencia territorial de los marcos. Seguidamente, se analiza la garantía del derecho a la educación digital en función de los documentos consultados. Por último, se abordan los límites en las responsabilidades y roles de los diferentes actores involucrados en la protección de la infancia en la sociedad digital.

2.1. Análisis de la coherencia entre el marco normativo y el marco político sobre protección de la infancia en la sociedad digital

A partir del listado definitivo de documentos revisados, el presente análisis examina la coherencia entre los marcos normativo y político en relación con el derecho a la educación y a la protección de la infancia en la sociedad digital. Con este fin, hemos puesto el foco en diversos actores esenciales de todo el proceso.

A continuación, se presenta esta reflexión en función de los actores identificados para la protección de la infancia en la sociedad digital: la Administración Pública y actores jurídicos, las instituciones educativas y las Corporaciones Tecnológicas.

2.1.1. Administración Pública y actores de significación jurídica

Este apartado aborda dos dimensiones clave relacionadas con la sociedad digital: el derecho a la educación y la protección de la infancia. Por un lado, se analiza cómo se garantiza el acceso equitativo y seguro a las tecnologías digitales como parte esencial del derecho a la educación. Por otro, se examinan las medidas dirigidas a proteger a los menores en entornos digitales, asegurando sus derechos fundamentales, como la privacidad, la seguridad y la igualdad de oportunidades.

En relación con el **derecho a la educación en la sociedad digital**, se observa coherencia entre el marco político y el marco normativo. Sin embargo, su enfoque difiere:

- El marco político tiene como objetivo principal impulsar iniciativas y desarrollar políticas públicas que guíen y supervisen el desarrollo educativo y la protección de la infancia en la sociedad digital.
- El marco normativo, en cambio, se centra en establecer regulaciones y legislación específica con carácter imperativo, asegurando la implementación de los principios establecidos por el marco político.

Marco político

El marco político aborda aspectos generales de alcance transformador, enfocados en la supervisión y la orientación de las políticas públicas:

- Ámbito global:
    - Impulsar el desarrollo de la dignidad humana en el uso de la tecnología (MP2, 2,3).
    - Garantizar el acceso a la escolarización gratuita y de calidad (MP3, 4,2).
    - Fomentar la autonomía digital para que las personas incidan en el desarrollo de la sociedad (MP3, 5,1; MP3, 9,3).
    - Promover la inversión en el factor humano (profesorado) para garantizar la aplicación del derecho a la educación en la era digital (MP3, 3,4).
- Europa:
    - Declarar la educación como derecho fundamental, incluyendo habilidades digitales (MP6, 10,2).
    - Promover la alfabetización digital para proteger datos y prevenir riesgos asociados a la digitalización (MP7, 6).
    - Reafirmar la relevancia del profesorado presencial frente a la tecnología digital (MP7, 8).
- España:
    - Diseñar estrategias para reducir la brecha digital entre el alumnado (MP8, 42,2).
    - Implementar medidas como el bono social para garantizar la conexión a internet de familias vulnerables (MP10, 31,3).
    - Impulsar la adquisición de competencias digitales tanto en alumnado como en profesorado (MP12, 5,5).

- CCAA:
    - Catalunya:
        - Fomentar competencias para la ciudadanía digital (MP14, 6,1).
        - Adaptar el aprendizaje a los retos del siglo XXI (MP14, 6,2).

Marco normativo

El marco normativo regula de manera específica y detallada la implementación de derechos relacionados con la educación digital:

- España:
    - Garantizar el acceso equitativo al aprendizaje de tecnologías digitales (MN3, 2,4).
    - Asegurar la alfabetización digital diferenciada según las etapas educativas: primaria (MN5, 1,4), secundaria (MN5, 1,5), bachillerato (MN5, 2,1) y formación profesional (MN3, 4,4).
- CCAA:
    - Catalunya:
        - Proteger los derechos de privacidad, datos y acceso a la información (MN8, 5,4).
    - Castilla-La Mancha:
        - Establecer medidas para prevenir la brecha digital, prestando atención a la brecha de género y el alumnado vulnerable (MN9, 50643, 15; MN10, 32782 y MN10, 32783, 11).

En cuanto a la **protección de la infancia en la sociedad digital**, también existe una coherencia general entre ambos marcos, aunque sus enfoques son distintos:

Marco político

- Ámbito global:
    - Evitar la discriminación en el uso de tecnologías digitales y los procesos de automatización (MP1, 4,2).
    - Prohibir la perfilación estadística de menores con fines comerciales (MP1, 5,4).
    - Garantizar el derecho a la privacidad y a la identidad digital (MP3, 4,2; MP3, 6,3; MP3, 14).
- Europa:

    - Promover el empoderamiento de menores a través del uso seguro de tecnología digital (MP5, 7,4).
    - Fomentar la capacidad de toma de decisiones éticas y seguras (MP5, 7,4).
    - Asegurar la protección de datos personales y valores éticos (MP6, 9,5).
- España:
    - Diseñar programas de capacitación en seguridad digital para menores y empresas (MP10, 49,5).
    - Salvaguardar derechos y libertades digitales en paralelo con los del entorno offline (MP10, 124,1).
    - Aplicar el Reglamento General de Protección de Datos (RGPD) de manera integral (MP11, 2,3).
- CCAA:
    - Catalunya:
        - Facilitar a los centros educativos manuales para la protección de datos (MP14, 29,3-5).

Marco normativo

- Europa:
    - Asegurar la especial protección de los datos personales de menores (MN2, 7,38).
    - Comunicar de forma comprensible a los menores toda información que les afecte (MN2, 11,58).
- España:
    - Prevenir la ciberdelincuencia que afecta a menores (MN4, 6,5; MN4, 8,1).
    - Regular el conocimiento de usos y riesgos digitales como estrategia para proteger a la infancia (MN5, 2,6-7).
    - Proteger los derechos de intimidad, honor e imagen de los menores en entornos digitales (MN7, 12,6).
- CCAA:
    - Castilla-La Mancha:
        - Involucrar a las familias en la prevención de violencia digital mediante el ejercicio de la parentalidad positiva (MN9, 50625, 2).

- Valencia:
    - Exigir el consentimiento previo para el tratamiento de datos personales de menores (MN11, 46427, 5).

2.1.2. Instituciones educativas

Analizar la coherencia entre el marco normativo y el marco político en torno a las responsabilidades de la escuela en materia de protección de la infancia en la sociedad digital requiere de una diferenciación entre los actores identificados en estos documentos: el equipo directivo (como responsable de las acciones asignadas a la escuela en su conjunto), la familia y el profesorado.

En relación con el equipo directivo/escuela, se observa una coherencia entre ambos marcos, en tanto identifican como sus funciones: el impulso de proyectos de IA y digitalización en general (MN3 – MN4 _ MN10), la promoción del desarrollo de la competencia digital en docentes y estudiantes (MN3 – MN4 _ MN10) y la prevención de la navegación en línea, con foco en la prevención de la violencia (ciberbullying), y de la vulneración de derechos a la privacidad, exposición a contenidos no apropiados, publicidad, etc. (MN3- MN4).

En el marco político, está contemplado que estas funciones se lleven adelante como parte, por ejemplo, del Plan Digital del Centro, a partir del cual “las escuelas definirán la adecuada integración de la tecnología en el proceso de enseñanza aprendizaje” (MP 12, 17, 4).

En relación con el rol de la familia, las principales funciones asignadas en el marco normativo son el control parental de la navegación on-line, la protección de la privacidad y de los datos personales (MN 2, 3, 4, 6). En línea con ello, el marco político establece que, en el caso de menores de edad, son los padres quienes brindan el consentimiento informado para proteger sus datos y privacidad. No obstante, encarga a los Estados la responsabilidad de exigir a los proveedores tecnológicos que “verifiquen que el consentimiento es informado, consecuente y dado por el padre o cuidador del niño” (MP1,8,3).

Finalmente, en referencia al rol de los docentes, existe una importante coherencia entre el marco normativo y el marco político, en tanto, mientras que el marco normativo se centra en las acciones y roles que deben desempeñar, el marco político plantea las iniciativas y estrategias para hacerlo.

Así, el marco normativo plantea la imperiosa necesidad de que los docentes adquieran "competencias digitales para la enseñanza y transmisión de los valores y derechos en la sociedad digital” (MN 3, 4, 7) y los insta, por tanto, a capacitarse y “[…] actualizar sus competencias para mejorar la capacidad de producción de contenidos digitales, de gestión de sistemas digitales de aprendizaje y evaluación” (MN 8, 45. 7).

Por otra parte, en el marco político, se específica qué se entiende por competencia digital docente (CDD) y los mecanismos para alcanzarla.

La CDD es definida como:

> "les habilitats de caire didàctic i metodològic compaginades amb l'ús instrumental de les tecnologies, posades al servei de l'èxit educatiu de tot l'alumnat" (MP 14, 10, 3).

Para desarrollarla, se entiende que como indispensable, la formación docente, inicial y continua, elemento que involucra en simultáneo el estímulo a la autoformación y a la formación formal promovida desde los centros y desde el Estado.

Este énfasis en la formación docente, presente tanto en el marco político como en el marco normativo, se explica porque hay una compartida cosmovisión de que:

> "la transformación del sistema educativo en clave digital sólo se puede llevar a cabo si se implica a todo el profesorado de una manera sustancial" (MP 12, 15, 16).

2.1.3 Corporaciones Tecnológicas

En lo referente a las Corporaciones Tecnológicas, en el marco normativo se hace referencia a los programas Escuelas Conectadas y Red.es, dos programas estatales que incorporan medidas dirigidas a mejorar la conectividad de los centros, la financiación, el seguimiento y evaluación de los programas, la colaboración público-privada para la prevención de la violencia sobre la infancia, la colaboración con administraciones públicas, fuerzas de seguridad y administración de justicia para retirar a la mayor brevedad contenidos ilegales que supongan violencia contra la infancia y adolescencia, y controlar a los proveedores de servicios de plataformas, que por su peso significativo de mercado, pudieran condicionar el acceso a los usuarios sin condiciones de equidad y transparencia (MN3; MN4; MN7).

Algunas de estas cuestiones relativas al control de contenidos y de los proveedores de servicios también aparecen en el marco político haciendo referencia al control de las empresas tecnológicas para que el procesamiento de los datos de la infancia no pueda dar lugar a violaciones de sus derechos o que los lleven hacia contenidos nocivos con fines comerciales (MP1). Para ello se plantean, entre otras medidas, un esfuerzo coordinado de profesionales, familias y cuidadores (MP11) con los proveedores de servicios para que se garantice que las tecnologías y servicios digitales dirigidos a la infancia mejoren sus oportunidades en materia de cultura, esparcimiento y juego (MP1), la obligación de las empresas de prevenir y mitigar los abusos que causen o a los que contribuyan (MP3), la rendición de cuentas para los directivos responsables de plataformas que incumplan con el establecimiento del deber de verificar la edad (MP9), y la obligación de las empresas digitales de informar de forma clara sobre la adecuación de los contenidos y la finalidad de la recogida

de datos, y de establecer procedimientos claros y adaptados a la edad de los y las menores para que conozcan el tipo datos que suministran y puedan suprimirlos o actualizarlos (MP9).

También se hace referencia en el marco normativo a que las "administraciones públicas deberán adoptar medidas para incentivar la responsabilidad social de las empresas en materia de uso seguro y responsable de Internet por la infancia y adolescencia" (MN3, 36, 2-3). Este aspecto se vuelve a reflejar en el marco político al indicar que los Estados, en colaboración con las empresas y organizaciones no gubernamentales, deben lograr que los proveedores de servicios digitales respeten las normas y códigos relativos a la moderación de los contenidos, pero sin restringir el acceso a la información de la infancia y su libertad de expresión y privacidad (MP1).

Será necesaria la colaboración con las empresas para lograr un sistema de clasificación por edades y contenidos, que sea fácilmente comprensible por niños, niñas, adolescentes y progenitores (MN4). Además de promover la colaboración de empresas, los estados tienen la obligación de garantizar los derechos de la infancia ante su posible violación por parte de las empresas comerciales (MP1). Para ello se apunta a que los Estados deben establecer leyes y reglamentos destinados a impedir su vulneración, y vigilar y exigir su cumplimiento (MP1). Además, se obliga a que los algoritmos y sistemas de tratamiento de automático de datos sean auditados por terceros independientes para evitar sesgos discriminatorios, manipulación y la adicción, de la misma manera que ocurre con los medicamentos (MP9). A esto se añade la obligación de responsabilizarse de los daños que se produzcan por el uso de los algoritmos en los menores, incluidos los de salud mental, a quién los desarrolle, mantenga o aplique (MP9).

En el marco normativo, en general, no se han encontrado medidas concretas para la protección de la infancia en el ámbito educativo más allá de mejorar las infraestructuras digitales de los centros educativos, y la supervisión y evaluación de los programas que, desde distintos programas (como Escuelas Conectas y Red.es), se pueden poner en marcha.

En relación con el marco político, la información al respecto se concentra en el documento MP3 (ONU, 2022), en el que se alude a:

- El cuidado que se debe tener a la hora de implementar tecnologías digitales en los centros educativos por las presiones de empresas del sector, que se mueven con fines de lucro y buscan combinar educación y beneficio, y evaluar sus posibles repercusiones negativas
- Las brechas de acceso en comunidades de difícil acceso que pueden estar provocando las empresas tecnológicas
- El cuidado que hay que tener con la mercantilización de la educación en el que se considera cada elemento de la enseñanza como un servicio comercializable y en la que

se ofrecen servicios separados para infancia y adolescencia en vez de paquetes educativos únicos

- El vínculo entre el sector educativo y el mercado laboral a través de los datos digitales genera preocupación. La digitalización de los itinerarios estudiantiles actúa como un currículum opaco, sin derecho de rectificación, sometiendo a los alumnos a vigilancia constante, donde errores pueden afectar su futuro. Esto podría llevar a que el mercado laboral condicione la educación, priorizando itinerarios útiles para los empleadores y eliminando cursos no considerados relevantes

2.1.4 Síntesis

En relación con el derecho a la educación en la sociedad digital, ambos marcos se alinean para fomentar la alfabetización digital y la protección de datos, asegurando que los menores reciban una formación adecuada y segura. El marco político establece una visión amplia que promueve la dignidad humana, la escolarización gratuita y la inversión en el profesorado, mientras que el marco normativo se especializa en la implementación de estas políticas en el aula, adaptándose a las diferentes etapas educativas. En el ámbito escolar se encuentra cierta coherencia en la normativa educativa, que las prácticas educativas deben confirmar. Se refleja en la voluntad de impulsar una formación integral, atendiendo tanto a las necesidades actuales como futuras de los menores.

En el ámbito escolar, la coherencia se refleja en la integración de competencias digitales, la prevención de riesgos en línea y la protección de la privacidad, destacando el papel crucial de familias y docentes. Además, las Corporaciones Tecnológicas, mediante programas específicos, mejoran la conectividad y colaboran en la protección de la infancia, subrayando la responsabilidad social empresarial y una estricta regulación de datos y contenidos. De este modo, desde el análisis textual de la documentación, ambos marcos tienen como objetivo común y complementario crear un entorno educativo seguro y avanzado, preparando a los menores para los desafíos de la era digital. Fruto de otro análisis sería tratar de qué modo y en qué grado los diversos agentes realmente convierten en realidad las directrices.

Destaca la coherencia o relación entre los aspectos siguientes, entre el marco normativo y político:

a) En relación con la Administración Pública y los actores de significación jurídica:

- El fomento de la alfabetización digital y de la equidad digital.
- La educación digital como derecho.
- Derecho a la privacidad y protección de datos.

b) En relación con la escuela:

- El equipo directivo/escuela debe fomentar la digitalización del centro y prevenir situaciones de violencia digital.
- La familia recibe el encargo de ejercer control parental y proporcionar consentimiento informado de los menores.
- El profesorado debe adquirir la competencia digital docente para fomentar una alfabetización digital crítica del alumnado.

c) En relación con las Corporaciones Tecnológicas

- Colaboración en la digitalización de los centros.
- Colaboración en el control de acceso a los contenidos.

2.1.5 Listado de documentos utilizados

MP1: Organización de las Naciones Unidas. (2021). *Observación General Nº 25, relativa a los derechos de los niños en relación con el entorno digital, Convención sobre los Derechos del Niño.* https://bit.ly/4gWWnXx

MP2: Organización de las Naciones Unidas. (1999). *Observación General nº13 relativa al Derecho a la Educación*. https://bit.ly/47IlfOc

MP3: Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/4elJBzM

MP5: Parlamento Europeo. (2023). *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital*. https://bit.ly/4ekjpWx

MP6: Comisión Europea, Dirección General de Educación, Juventud, Deporte y Cultura, (2023). *Plan de acción de educación digital 2021-2027: mejorar la provisión de capacidades digitales en la educación y la formación*, Oficina de Publicaciones de la Unión Europea. https://bit.ly/47HzzXr

MP7: Parlamento Europeo. (2021). *Propuesta de resolución del Parlamento Europeo: Informe sobre la formulación de la política de educación digital*. https://bit.ly/47Ma8E6

MP8: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 21: Modernización y digitalización del sistema educativo, incluida la educación temprana de 0-3 años*. https://bit.ly/3XIqtoH

MP9: Pacto de Estado. (2023). Protegiendo a la infancia y la adolescencia en el entorno digital, medidas de consenso para un Pacto de Estado ante la nueva legislatura y la presidencia de España en la Unión Europea. https://bit.ly/3BhnMTq

MP10: Gobierno de España. (n.d.). *España Digital 2026.*

MP11: Agencia Española de Protección de Datos. (2024). *Menores, salud digital y privacidad: Estrategia y líneas de acción*. https://bit.ly/3ZHFGcd

MP12: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 19. Plan Nacional de Capacidades Digitales.* https://bit.ly/3ZKocvM

MP13: Generalitat de Catalunya. (2019). *Carta catalana por los derechos y las responsabilidades digitales.* Departament de Polítiques Digitals i Administració Pública. https://bit.ly/3zprudm

MP14: Generalitat de Catalunya. Departament d'Educació. (2020). *Pla d'educació digital de Catalunya 2020-2023*. https://bit.ly/3z33nyv

MP15: Decreto Nº 55, *por el que se establece la política de protección de datos en la Administración de la Junta de Comunidades de Castilla-La Mancha* (6 de junio de 2023). https://bit.ly/4em0BGi

MN2: 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. https://bit.ly/3N1va8j

MN3: Resolución, *de la Subsecretaría, por la que se publica el Convenio entre el Ministerio de Educación y Formación Profesional, el Ministerio de Asuntos Económicos y Transformación Digital y la Entidad Pública Empresarial Red.es, M.P., para la ejecución del programa "Educa en Digital"* (7 de julio de 2020). https://bit.ly/3XMmtDP

MN4: Ley Ogánica N° 8, *Ley de protección integral a la infancia y la adolescencia frente a la violencia* (4 de junio de 2021). https://bit.ly/4doiVx1

MN5: Ministerio de Educación y Formación Profesional. (2019). *Informe sobre el uso seguro y respetuoso de los medios digitales en el currículo básico*. https://bit.ly/4eGngNd

MN6: Ley Orgánica N° 3, *Ley de Protección de Datos Personales y garantía de los derechos digitales* (5 de diciembre de 2018). https://bit.ly/4ds3NPc

MN7: Gobierno de España. (2021). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia*. https://bit.ly/4eiIxgn

MN8: Ley 23/2010, de 1 de octubre, *de la Autoridad Catalana de Protección de Datos*, (8 de octubre de 2010). https://bit.ly/3ZDt85J

MN9: Ley N° 7, *Ley de Atención y Protección a la Infancia y la Adolescencia de Castilla-La Mancha* (10 de marzo de 2023). https://bit.ly/3BgdqmL

MN10: Orden N° 178, *de la Consejería de Educación, Cultura y Deportes, por la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios* (14 de septiembre de 2022). https://bit.ly/3MZMhr0

MN11: Resolución, *de la Subsecretaría de la Conselleria de Educación, Investigación, Cultura y Deporte, por la que se dictan instrucciones para el cumplimiento de la normativa de protección de datos en los centros educativos públicos de titularidad de la Generalitat* (28 de junio de 2018). https://bit.ly/3Y0kfBL

2.2. Coherencia territorial entre marcos normativos. Desde lo macro a lo micro

El presente apartado propone una mirada desde lo macro a lo micro en relación con los marcos políticos y normativos que regulan la protección de la infancia en la sociedad digital. Para ello, se sigue la estructura que se expone a continuación:

- Normativas sobre el uso de plataformas digitales y otras tecnologías.
- Normativas sobre gestión y uso de los datos.
- Normativas sobre la protección de la infancia en la sociedad digital.

Por último, a modo de cierre del apartado, se presenta una breve conclusión respecto a lo que se expone a lo largo del mismo.

2.2.1. Normativas sobre el uso de tecnologías digitales y el tratamiento de los datos

En el Plan de acción de educación digital 2021-2027 de la Comisión Europea (2020) hay un enunciado sobre las garantías del derecho a la educación. En él se destaca el ámbito digital como una dimensión más de la realidad educativa y, por tanto, también sujeta a deberes y derechos:

> La educación es un derecho humano fundamental y el acceso a ella debe estar garantizado, independientemente del entorno en el que se realice: físico, digital o una combinación de ambos. El derecho a una educación y formación inclusivas y de calidad y al aprendizaje permanente es el primer principio del pilar europeo de derechos sociales, mientras que el quinto principio del pilar contempla el derecho de los trabajadores a la formación (MP6, 10, 2).

Esta conciencia del ámbito digital como entorno educativo, desde una mirada política, define el acceso al conocimiento digital como un derecho, es decir, una aspiración educativa que implica, literalmente, según Plan de acción de educación digital 2021-2027, que:

> Todas las personas deben adquirir unos conocimientos básicos de las tecnologías nuevas y emergentes, incluida la inteligencia artificial. Estos conocimientos les serán útiles para interactuar de manera positiva, crítica y segura con estas tecnologías, y a ser conscientes de los problemas potenciales relacionados con la ética, la sostenibilidad medioambiental, la protección de datos y la privacidad, los derechos de los menores, la discriminación y los prejuicios, incluidos los prejuicios basados en el género y la discapacidad, y la discriminación étnica y racial (MP6, 10, 2).

Es más, para la Estrategia de regulación de uso de las tecnologías digitales en la escuela formulada en la Propuesta de resolución del Parlamento Europeo, Informe sobre la formulación de la política de educación digital (Parlamento Europeo), se señala que el

antídoto a la desinformación es la educación digital: “La educación digital podría ayudar a abordar retos como la desinformación, la radicalización, la usurpación de identidad y la usurpación de datos, el ciberacoso y las estafas en línea” (MP7, 28).

Esta educación sobre lo digital implica para el mismo Plan de acción de educación digital 2021-2027 ir más allá del dominio técnico para atender circunstancias que atañen no solo al aprendizaje con tecnología, sino a ámbitos de la vida donde lo digital está comprometido. Esto es, la privacidad, la salud, el desarrollo, etc.

> Considerando que una educación básica en ciberhigiene, ciberseguridad, protección de datos y alfabetización mediática debe adecuarse a la edad y estar orientada al desarrollo de los alumnos con el fin de ayudar a los niños a convertirse en alumnos críticos, ciudadanos activos, usuarios de internet y forjadores de una sociedad digital democrática, a tomar decisiones con conocimiento de causa y a ser conscientes y capaces de afrontar los riesgos asociados a internet, como la desinformación en línea, el acoso y la violación de la seguridad de los datos personales; que deben introducirse programas de enseñanza relativos a la ciberseguridad en los planes de estudios (MP6, 7, párrafo F).

La necesidad de formación también es recogida por la Observación General nº25 de las Naciones Unidas (2021) que señala que:

> Los Estados parte deben asegurarse de que la alfabetización digital esté integrada en la educación escolar como parte de los planes de estudio de la enseñanza básica, desde el nivel preescolar y a lo largo de todos los cursos académicos, y de que dichas pedagogías se evalúen en función de sus resultados. Los planes de estudio deben incluir conocimientos y aptitudes para manejar con seguridad una amplia gama de herramientas y recursos digitales, incluidos los relacionados con el contenido, la creación, la colaboración, la participación, la socialización y la participación cívica. Los planes de estudio también deben incluir la comprensión crítica; la orientación sobre cómo encontrar fuentes de información fiables y cómo identificar la información errónea y otras formas de contenido sesgado o falso, por ejemplo, sobre cuestiones de salud sexual y reproductiva; los derechos humanos, incluidos los derechos del niño en el entorno digital; y las formas disponibles de apoyo y reparación. Deben fomentar la concienciación de los niños sobre las posibles consecuencias adversas de la exposición a riesgos relacionados con contenidos, contactos, conductas y contratos, como ciberagresión, trata de personas, explotación y abusos sexuales y otras formas de violencia, y promover estrategias de adaptación para reducir los daños, así como estrategias destinadas a proteger sus datos personales y los de los demás, y a desarrollar las aptitudes sociales y emocionales de los niños y su capacidad de resiliencia (MP1, 11, 10).

En relación con el uso de tecnologías digitales y el tratamiento de los datos, a nivel global, y para garantizar el derecho al acceso en condiciones de seguridad, la ONU instruye a los

estados que elaboren políticas o normativas basadas en las experiencias de los centros educativos y destinadas a proteger a la infancia contra cualquier tipo de consecuencia derivada del uso de dichas tecnologías. Esta orientación se expone en la Observación General nº 25 de las Naciones Unidas (2021).

> Los Estados parte deben elaborar políticas, normas y directrices basadas en pruebas para las escuelas y otras entidades pertinentes encargadas de la adquisición y utilización de tecnologías y materiales educativos a fin de mejorar la aportación de valiosos beneficios educativos. Las normas relativas a las tecnologías educativas digitales deben garantizar que la utilización de esas tecnologías sea ética y adecuada para los fines educativos y no exponga a los niños a la violencia, la discriminación, el uso indebido de sus datos personales, la explotación comercial u otras conculcaciones de sus derechos, como la utilización de tecnologías digitales para documentar sus actividades y compartir esa información con sus padres o cuidadores sin el conocimiento o consentimiento del niño (MP1, 11, 9).

La idea de un entorno digital justo se manifiesta, a nivel político, en la Declaración Europea sobre los derechos y Principios Digitales para la Década Digital, cuando se señala que "Toda persona debería poder elegir de manera efectiva y libre qué servicios digitales utiliza sobre la base de información objetiva, transparente, fácilmente accesible y fiable" (MP5, 5).

Esta idea implica compromisos, que la UE debe encarar como:

a) velar por un entorno digital seguro y protegido, basado en la competencia leal, en el que los derechos fundamentales estén protegidos, los derechos de los usuarios y la protección de los consumidores en el mercado único digital estén garantizados y las responsabilidades de las plataformas, especialmente los grandes operadores y los guardianes de acceso, estén bien definidas;
b) promover la interoperabilidad, la transparencia, las tecnologías y normas abiertas como forma de reforzar aún más la confianza en la tecnología, así como la capacidad de los consumidores para tomar decisiones autónomas y con conocimiento de causa. (MP5, 5, 13).

En concreto, la propuesta europea, Informe sobre la formulación de la política de educación digital (Parlamento Europeo, 2021), plantea los siguientes riesgos que se deben atender para lograr un entorno digital seguro para la infancia:

> Subraya el desafío que representan los contenidos y actividades nocivos e ilegales en el entorno digital, también en términos de salud mental y bienestar, por ejemplo, el acoso en línea, en particular las ciberamenazas y el ciberacoso, la pornografía infantil y la captación de menores, las violaciones de la seguridad de los datos y la intimidad, los juegos en línea peligrosos, y la desinformación (MP7, 15).

Asimismo, también se menciona la necesidad de integrar la alfabetización digital en el currículum educativo a través de las diferentes etapas escolares.

> Los Estados parte deben asegurarse de que la alfabetización digital esté integrada en la educación escolar como parte de los planes de estudio de la enseñanza básica, desde el nivel preescolar y a lo largo de todos los cursos académicos, y de que dichas pedagogías se evalúen en función de sus resultados. Los planes de estudio deben incluir conocimientos y aptitudes para manejar con seguridad una amplia gama de herramientas y recursos digitales, incluidos los relacionados con el contenido, la creación, la colaboración, la participación, la socialización y la participación cívica. [...] también deben incluir la comprensión crítica; la orientación sobre cómo encontrar fuentes de información fiables y cómo identificar la información errónea y otras formas de contenido sesgado o falso [...]. Deben fomentar la concienciación de los niños sobre las posibles consecuencias adversas de la exposición a riesgos relacionados con contenidos, contactos, conductas y contratos, como ciberagresión, trata de personas, explotación y abusos sexuales y otras formas de violencia, y promover estrategias de adaptación para reducir los daños, así como estrategias destinadas a proteger sus datos personales y los de los demás, y a desarrollar las aptitudes sociales y emocionales de los niños y su capacidad de resiliencia (MP1, 11, 10).

Respecto al uso de plataformas digitales y otro tipo de tecnologías digitales, encontramos que, a nivel europeo, se garantiza el acceso amplio y asequible a este tipo de recursos y se establecen directrices en relación con el tratamiento de datos: “El acceso a las redes móviles digitales está ya disponible y resulta asequible para un público muy amplio. Estas redes digitales poseen gran capacidad y abren posibilidades en materia de tratamiento de los datos personales” (MN1, 1, 5). En este sentido, desde el año 2002 que se publica la Directiva 2002/58/CE del Parlamento europeo y del consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, se es consciente de la penetración de plataformas externas en redes públicas que requiere de actuaciones específicas: “Actualmente se están introduciendo en las redes públicas de comunicación de la Comunidad nuevas tecnologías digitales avanzadas que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios” (MN1, 1, 5). Más tarde, en el año 2016, se establece el 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 y por el que se deroga la Directiva 95/46/CE. Este Reglamento pone de manifiesto la ausencia de una evaluación de impacto sobre la penetración de plataformas digitales en términos de protección de datos, aunque en el mismo documento se considera estrictamente necesaria.

> Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales (MN2, 53).

Sin embargo, ¿qué sucede a nivel estatal? En relación con este mismo aspecto, a nivel estatal se ha podido ver la demanda de un uso intensivo de dichas tecnologías, tanto en lo que se refiere a dispositivos como a redes, dentro y fuera del aula, tal y como se expone en los siguientes extractos de la Resolución de 7 de julio de 2020, para la ejecución del programa "Educa en Digital": Puesta a disposición de aplicaciones, herramientas y recursos curriculares que faciliten la educación digital, tanto presencial en el centro, como desde el hogar (MN3, 6, 7).

> El proceso de transformación digital de la educación en España requiere (...) de herramientas telemáticas de comunicación y colaboración y de dispositivos y conexiones a Internet por parte tanto de personal docente como del alumnado, y está demandando hacer un uso intensivo de las TIC, tanto en el aula, como en los formatos no presenciales (MN3, 2, 5).

Asimismo, la Administración Pública tiene la misión de elaborar un Plan de Digitalización y Competencias Digitales para crear Recursos Educativos en Abierto, aportar equipamiento y mejorar las competencias digitales tanto de alumnado como de los y las docentes con la finalidad de favorecer la inclusión digital (MN3).

El Ministerio de Educación y Formación Profesional está elaborando un ambicioso Plan de Digitalización y Competencias Digitales, que persigue como objetivos básicos:

> 1. Mejorar la Competencia Digital Educativa, que incluye la del alumnado, la del profesorado y la de los centros educativos.
>
> 2. Implantar el Plan Digital de Centro Educativo aportando equipamiento, transformando espacios, aportando formación y aplicando métodos de Inteligencia Artificial para facilitar el proceso de enseñanza- aprendizaje.
>
> 3. Crear Recursos Educativos Abiertos (REA) en formato digital.
>
> 4. Fomentar el uso de metodologías y competencias digitales avanzadas. (MN3, 4, 4)

Junto a esto, también se demanda al poder público, en la Carta de Derechos Digitales del Gobierno de España (2021), el compromiso de asegurar condiciones equitativas y potestad de control sobre los proveedores de plataformas, especialmente a sobre los que, por su posición privilegiada de mercado, tienen mayor poder condicionante, tal y como se expresa en el siguiente fragmento.

> Con el fin de asegurar a usuarios finales y profesionales condiciones equitativas y transparentes de acceso a contenidos, bienes y servicios, o a la oferta de los mismos, los poderes públicos podrán controlar a los guardianes de acceso o proveedores de servicios de plataformas que por su peso significativo de mercado, sea cual fuere el origen de tal peso, pudieran condicionar dicho acceso, en los términos previstos en la normativa europea (MN7, 16, 4).

En este sentido, se adoptarán medidas para incentivar la responsabilidad social de las empresas proveedoras de servicios digitales dirigida a proteger la privacidad y seguridad de los usuarios, garantizar la accesibilidad y equidad digital, ser transparentes en el uso de algoritmos y moderar adecuadamente el contenido en sus plataformas. De igual modo, se fomentará la creación de contenidos positivos en línea, seguros y adaptados a distintas necesidades.

> Las administraciones públicas deberán adoptar medidas para incentivar la responsabilidad social de las empresas en materia de uso seguro y responsable de Internet por la infancia y la adolescencia. Asimismo, fomentarán en colaboración con el sector privado que el inicio y desarrollo de aplicaciones y servicios digitales tenga en cuenta la protección a la infancia y la adolescencia (MN4, 36, 2-3).

En relación con este mismo aspecto, pero a nivel autonómico encontramos diferentes posturas. Por un lado, en lo que respecta a Castilla-La Mancha, vemos cómo siguen las directrices que se establecen a nivel estatal y promueven el acceso a tecnologías digitales, aun así, van un paso más allá y pretenden adaptar este acceso a la edad y el grado de maduración de las personas menores de edad[12].

> El acceso a los medios telemáticos y al desarrollo de los conocimientos y competencias digitales, evitando la brecha digital de las personas más vulnerables y promoviendo un uso razonable de las tecnologías de la información y la comunicación, de acuerdo a la edad y la maduración de cada persona menor de edad (MN9, 50643, 15).

Además, en Castilla-La Mancha también se apuesta por la promoción de herramientas de gestión que sean capaces de garantizar el cumplimiento de la Ley de Protección de Datos (LOPDGDD), tal y como se menciona en la Orden 178/2022, de 14 de septiembre, de la Consejería de Educación, Cultura y Deportes, por la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios.

> Promover el uso de las herramientas de gestión que ofrece la consejería competente en materia de educación, sobre todo en los ámbitos de organización, información y comunicación, garantizando el cumplimiento de la LOPDGDD (Ley Orgánica de Protección de Datos personales y Garantía de Derechos Digitales) (MN10, 32783, 4).

[12] Mientras que en los documentos consultados referentes a Catalunya y Valencia no se hace referencia a este aspecto

Por otro lado, la Comunitat Valenciana otorga a la Generalitat la potestad de control de todos los datos y prohíbe el uso de sistemas externos:

> Queda prohibido, transmitir o alojar información propia de la Administración de la Generalitat en sistemas de información externos (por ejemplo, on cloud), salvo autorización expresa de la conselleria competente en materia de educación, verificando el correspondiente acuerdo de confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización. Por tanto, deberán emplearse las herramientas educativas que ponga a disposición de los centros la conselleria competente en materia de educación. (MN11, 46436, 2).

2.2.2. Normativas sobre gestión y uso de los datos generados en entornos digitales

Hay que destacar que en mayo de 2018 entró en aplicación en el ámbito de la Unión Europea el Reglamento General de Protección de Datos (RGPD), que señala que:

> 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. Los responsables han de tener en cuenta los riesgos derivados del tratamiento de los datos de los y las menores en las evaluaciones de impacto (MP9, 2,3).

Ahora bien, cuantos más sean los datos, o la exposición a ellos, mayor es la necesidad de cuidar el sesgo de codificación y discriminación. Como subraya el documento Repercusiones de la digitalización de la educación en el derecho a la educación. Informe de la relatora Especial sobre el derecho a la educación, Boly Barry, ONU (2022):

> los sistemas de inteligencia artificial dan resultados sesgados, La tecnología de los motores de búsqueda no es neutral, puesto que procesa macrodatos y prioriza los resultados con la mayor cantidad de clics dependiendo tanto de las preferencias del usuario como de la ubicación. Por lo tanto, un motor de búsqueda puede convertirse en una cámara de resonancia que mantiene los prejuicios del mundo real y afianza aún más estos prejuicios y estereotipos en línea (MP3, 16,6).

Es más, en ese mismo documento, se insta a promover una equidad digital que tenga en cuenta a las minorías.

> La plena participación en los procesos de digitalización de las comunidades, incluidas las minorías y los pueblos indígenas, es fundamental para garantizar el respeto de los derechos culturales y la diversidad cultural en la educación y permitir la recopilación de datos genuinos. Por lo tanto, esa participación debe tener lugar en la fase de conceptualización, antes de la recogida de datos (MP3, 17,2).

A nivel estatal, encontramos que los documentos en los que se basa la regulación del tratamiento de los datos personales son:

> El tratamiento de los datos personales [...] se sujetará a la normativa nacional y comunitaria en materia de protección de datos, en especial, a la Ley Orgánica 3/2018,

> de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y al 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 y por el que se deroga la Directiva 95/46/CE (MN3, 12, 3).

En este sentido, la legislación legitima y faculta a la Agencia Española de Protección de Datos en velar por los datos personales y derechos de las personas menores de edad en los entornos digitales (MN4). Asimismo, se establece el compromiso de hacer públicos los datos sobre violencia hacia la infancia y la adolescencia en contextos digitales de forma anual.

> Los resultados del informe anual de evaluación, que contendrá los datos estadísticos disponibles sobre violencia hacia la infancia y la adolescencia, se harán públicos para general conocimiento, y deberán ser tenidos en cuenta para la elaboración de las políticas públicas correspondientes (MN4, 25, 9).

También, se establece la necesidad de una inserción en igualdad de condiciones del alumnado en la sociedad digital y su aprendizaje para un uso seguro y respetuoso con los derechos de las personas.

> Las administraciones públicas garantizarán la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales, conforme a lo previsto en el artículo 83 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. [...] Específicamente, las administraciones públicas promoverán dentro de todas las etapas formativas el uso adecuado de Internet (MN4, 30, 8 y 31, 1).

Para ello, las personas deben ser informadas de cuándo se recogen sus datos, así como del uso que se les dará y de sus derechos a la oposición, rectificación y olvido.

> Toda persona tiene derecho a ser informada en el momento de la recogida de los datos sobre su destino y los usos que se hagan de los mismos, a acceder a los datos recogidos que le conciernan y a ejercer sus derechos de rectificación, oposición, cancelación, portabilidad de los datos, y derecho a la supresión (derecho al olvido) en los términos previstos en la normativa de protección de datos nacional y europea (MN7, 9, 4).

Adicionalmente, se prohíbe el tratamiento de los datos de personas menores de edad, especialmente, en el caso del establecimiento de perfiles de personalidad en entornos digitales

> Salvo en las excepciones previstas en las leyes, están prohibidos los tratamientos de la información de personas menores orientados a establecer perfiles de personalidad

> en entornos digitales. Ninguna práctica de perfilado podrá dirigirse a manipular o perturbar la voluntad de personas menores, incluido el perfilado con fines publicitarios (MN7, 13, 1).

En este sentido, con la finalidad de conocer los efectos de este tipo de prácticas, así como al acceso y consumo de contenidos digitales, la Carta de Derechos Digitales del Gobierno de España (2021) establece lo siguiente:

> Se impulsará el estudio del impacto en el desarrollo de la personalidad de personas menores derivado del acceso a entornos digitales, así como a contenidos nocivos o peligrosos. Dicho estudio prestará particular atención a sus efectos en la educación afectivo-sexual, las conductas dependientes, la igualdad, la orientación sexual e identidad de género, así como a los comportamientos antidemocráticos, racistas, xenófobos, capacitistas, machistas, discriminatorios o propios del discurso de odio (MN7, 13, 4).

Además, a nivel estatal, se adoptarán medidas para corregir los sesgos de género provocados por los algoritmos.

> El derecho y el principio a la igualdad inherente a las personas será aplicable en los entornos digitales, incluyendo la no discriminación y la no exclusión. En particular, se promoverá la igualdad efectiva de mujeres y hombres en entornos digitales. Se fomentará que los procesos de transformación digital apliquen la perspectiva de género adoptando, en su caso, medidas específicas para garantizar la ausencia de sesgos de género en los datos y algoritmos usados (MN7, 12, 1).

En relación con esta temática, pero a nivel autonómico, es preciso considerar diversos aspectos. Por un lado, siguiendo lo que se designa a nivel estatal, las Comunidades Autónomas han establecido una autoridad competente en materia de protección de datos y protección de los derechos de las personas: la Autoritat Catalana de Protecció de Dades, la Conselleria d'Educació en Valencia y el Comité Regional de Protección de Datos en Castilla-La Mancha (MN8; MN11; MP15). Por otro, en el caso de la Comunitat Valenciana, se establece que las personas autorizadas por la administración encargadas del tratamiento de datos solamente podrán usarlos en el ejercicio de las funciones que tengan encomendadas.

> Los centros y la conselleria competente en materia de educación tomarán medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratar dichos datos en el ejercicio de las funciones que tenga asignadas (MN11, 46428, 4).

Asimismo, en el caso de la legislación autonómica valenciana desarrollan la importancia de obtener el consentimiento de los padres, madres o tutores/as legales de los menores, recogido en el artículo 7 de la LOPDPGDD para hacer uso de dichas herramientas y para la publicación de contenido en redes sociales donde aparezca información del menor.

> Dada la información que se contiene en los dispositivos con acceso a internet, así como la trazabilidad que se puede realizar de la navegación efectuada por los usuarios, el acceso al contenido de estos dispositivos del alumnado, incluyendo su clave, supone un acceso a datos de carácter personal que requiere el consentimiento de los interesados o de sus familiares si se trata de menores (MN11, 46430, 3).
>
> La publicación de datos personales en redes sociales por parte de los centros educativos requiere contar con el consentimiento inequívoco de las personas implicadas, a las que habrá que informar previamente de manera clara de los datos que se van a publicar, en qué redes sociales, con qué finalidad, quién puede acceder a los datos, así como de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición (MN11, 46437, 2).

2.2.3. Normativas sobre el derecho y la protección de la infancia en entornos digitales

Como se ha indicado anteriormente, a Unión Europea reconoce una protección específica a las personas menores de edad, particularmente cuando se trata del uso de sus datos con fines comerciales. En este sentido, se debe ofrecer toda la información relativa a sus derechos en el mundo digital a niños, niñas y jóvenes adaptada en función de su edad:

> dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender (MN2, 11, 58).

Además, en este caso, el consentimiento es especialmente revocable al no ser, los y las menores, plenamente conscientes de los riesgos (MN2).

Además, en la Declaración Europea sobre los derechos y Principios Digitales para la Década Digital (2022), se señala respecto a la protección y empoderamiento de los niños y jóvenes en el entorno digital que:

> Debería empoderarse a los niños y los jóvenes para que puedan tomar decisiones seguras y con conocimiento de causa y expresar su creatividad en el entorno digital.21.Los materiales y servicios adaptados a cada edad deberían mejorar las experiencias, el bienestar y la participación de niños y jóvenes en el entorno digital.22.Debe prestarse especial atención al derecho de los niños y los jóvenes a ser protegidos frente a todo tipo de delincuencia cometida o facilitada a través de tecnologías digitales (MP5, 5,4).

A nivel estatal, los documentos consultados se basan en la idea de que la tecnología digital enriquece el aprendizaje y se habla de garantizar el derecho al acceso a la tecnología en la infancia.

> La tecnología digital enriquece el aprendizaje en una variedad de formas y ofrece oportunidades para ello, que deben ser accesibles para todos… Una de las piezas clave de la educación digital consiste en garantizar la igualdad y la calidad del acceso y las infraestructuras (MN3, 2, 4).

Asimismo, otro aspecto que se vincula al anterior y al que se hace referencia es la alfabetización digital en todas las etapas educativas orientada hacia un uso seguro de las tecnologías digitales, especialmente en aquello relacionado con la protección de la intimidad. En función de la etapa educativa se irán garantizando usos más participativos, críticos y creativos de estas tecnologías (MN3, MN4, MN5).

> Asimismo, las administraciones públicas impulsarán campañas específicas de sensibilización para promover un uso seguro y responsable de Internet, desde un enfoque de aprovechamiento de las oportunidades y su uso en positivo, incorporando la perspectiva y opiniones de los propios niños, niñas y adolescentes (MN4, 26, 2).

Para ello, se han de tener en cuenta variables sociales, económicas y educativas, entre otras a la hora de valorar los riesgos y escenarios de violencia a los que pueden estar expuestos, "Esta ley combate la violencia sobre la infancia y la adolescencia desde una aproximación integral, en una respuesta extensa a la naturaleza multidimensional de sus factores de riesgo y consecuencias" (MN4, 8, 1). En esta visión integral no solo cabe la atención a los casos de violencia, discriminación o acoso, sino además se busca dar voz a los niñas y niños sobre estos hechos, así como tener especial atención en los siguientes casos específicos: la discapacidad, el racismo, la orientación sexual o la expresión de género.

> Deberán contemplar actuaciones específicas cuando el acoso tenga como motivación la discapacidad, el racismo o el lugar de origen, la orientación sexual, la identidad o expresión de género. De igual modo, dichos protocolos deberán contemplar actuaciones específicas cuando el acoso se lleve a cabo a través de las nuevas tecnologías de las personas menores de edad o dispositivos móviles y se haya menoscabado la intimidad y reputación (MN4, 39, 8 y 40, 1).

Este aspecto sigue la línea de lo recogido en la Convención de los Derechos del Niño y, además, busca elaborar protocolos de actuación que prevengan riesgos y abusos que atenten contra su integridad, su intimidad o su honor. Del mismo modo, en el ámbito educativo, se habilitarán canales para que los propios menores puedan denunciar conductas de este tipo.

> La regulación propuesta profundiza y completa el marco establecido en el artículo 124 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, al establecer junto al plan de convivencia recogido en dicho artículo, la necesidad de protocolos de actuación frente a indicios de abuso y maltrato, acoso escolar, ciberacoso, acoso sexual, violencia de género, violencia doméstica, suicidio, autolesión y cualquier otra forma de violencia. Para el correcto funcionamiento de estos protocolos se constituye un coordinador o coordinadora de bienestar y protección, en todos los centros educativos. También se refleja la necesaria capacitación de las personas menores de edad en materia de seguridad digital (MN4, 9, 10).

Otro aspecto remarcable al que se hace referencia a nivel estatal es la prevención de conductas nocivas. En este sentido, se propone lo siguiente a través de la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia.

> Las administraciones públicas trabajarán para conseguir que en los envases de los instrumentos de las nuevas tecnologías deba figurar un aviso mediante el que se advierta de la necesidad de un uso responsable de estas tecnologías para prevenir conductas adictivas específicas. Así mismo, se recomienda a las personas adultas responsables de la educación de la infancia y adolescencia la vigilancia y responsabilidad en el uso adecuado de estas tecnologías (MN4, 36, 9).

En lo que respecta a las diferentes comunidades autónomas, estas recogen la protección de la infancia en entornos digitales siguiendo las directrices que propone el Gobierno de España, aunque cada una haciendo énfasis en diferentes cuestiones.

En Catalunya se sigue el camino que se establece a nivel estatal, "Promover, en el ámbito de sus competencias, la divulgación de los derechos de las personas con relación a la protección de datos y el acceso a la información, y la evaluación del impacto sobre la privacidad" (MN8, 5, 4).

Por su parte, Castilla-La Mancha procura evitar la brecha digital de las personas más vulnerables y también la brecha digital de género, tal y como se apuntaba a nivel estatal, a través de la promoción de un uso de las tecnologías adecuado en función de la edad y de la cesión de dispositivos tecnológicos y acceso a internet para el alumnado (MR9; MR10), tal y como se expresa en el siguiente fragmento: "organizar un procedimiento de cesión de dispositivos tecnológicos y acceso a Internet para el alumnado del centro, prestando especial atención al alumnado en situación de vulnerabilidad para facilitar la accesibilidad al aprendizaje" (MN10, 32783, 11).

En la Comunitat Valenciana se especifican algunas normativas concretas, como, por ejemplo, la prohibición de grabar como parte de la función docente, exceptuando algunos casos.

> No se permite la grabación de imágenes como parte del ejercicio de la función educativa de la que es responsable el centro docente. No obstante, en aquellos casos en los que el interés superior del menor estuviera comprometido, como en caso de accidentes o indisposiciones en una excursión escolar, y con la finalidad de informar y tranquilizar a las madres y los padres, titulares de la patria potestad, se podrían captar las imágenes y enviárselas (MN11, 46430, 7).

No obstante, en Valencia, en casos de violencia contra los y las menores, los centros educativos deberán adoptar otras medidas que se exponen a continuación.

> No obstante, en situaciones en las que pudiera estar presente el interés público, como cuando se ponga en riesgo la integridad de alguna alumna o alumno (situaciones de ciberacoso, sexting, grooming o de violencia de género) el centro educativo podría, previa ponderación del caso y conforme al protocolo que tenga establecido, acceder a dichos contenidos sin el consentimiento de las personas implicadas (MN11, 46430, 4).
>
> La norma específica sobre medidas de protección integral de violencia de género establece que en actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los

de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia. En consecuencia, los centros educativos deberán proceder con especial cautela a tratar los datos de los menores que se vean afectados por estas situaciones (MN11, 46430).

2.2.4. Síntesis

Como se ha podido ver, es evidente que los documentos consultados siguen una misma línea, es decir, por lo general, lo que se propone a nivel global, se propone a nivel europeo y posteriormente a nivel estatal y autonómico. En cuanto a los documentos normativos, se aprecia una mayor concordancia entre ellos, ya que, al tratarse de normas generales, es imperativo que estas se ajusten en cada uno de los niveles inferiores para seguir las directrices establecidas por el organismo superior. Sin embargo, no sucede lo mismo, en algunos casos, al hablar de documentos de carácter político, pues estos son archivos con una finalidad de tipo práctica, y resulta más complicado continuar la línea de lo que proponen los organismos superiores cuando se trata de aplicarlo a realidades concretas.

2.2.5 Listado de documentos utilizados

MP1: Organización de las Naciones Unidas. (2021). *Observación General Nº 25, relativa a los derechos de los niños en relación con el entorno digital, Convención sobre los Derechos del Niño.* https://bit.ly/4gWWnXx

MP3: Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/4elJBzM

MP5: Parlamento Europeo. (2023). *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital.* https://bit.ly/4ekjpWx

MP6: Comisión Europea, Dirección General de Educación, Juventud, Deporte y Cultura, (2023). *Plan de acción de educación digital 2021-2027: mejorar la provisión de capacidades digitales en la educación y la formación*, Oficina de Publicaciones de la Unión Europea. https://bit.ly/47HzzXr

MP7: Parlamento Europeo. (2021). *Propuesta de resolución del Parlamento Europeo: Informe sobre la formulación de la política de educación digital*. https://bit.ly/47Ma8E6

MP9: Pacto de Estado. (2023). Protegiendo a la infancia y la adolescencia en el entorno digital, medidas de consenso para un Pacto de Estado ante la nueva legislatura y la presidencia de España en la Unión Europea. https://bit.ly/3BhnMTq

MN1: Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).* https://bit.ly/4gH40B8

MN2: 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://bit.ly/3N1va8j

MN3: Resolución, *de la Subsecretaría, por la que se publica el Convenio entre el Ministerio de Educación y Formación Profesional, el Ministerio de Asuntos Económicos y Transformación Digital y la Entidad Pública Empresarial Red.es, M.P., para la ejecución del programa "Educa en Digital"* (7 de julio de 2020). https://bit.ly/3XMmtDP

MN4: Ley Ogánica N° 8, *Ley de protección integral a la infancia y la adolescencia frente a la violencia* (4 de junio de 2021). https://www.boe.es/eli/es/lo/2021/06/04/8/con

MN5: Ministerio de Educación y Formación Profesional. (2019). *Informe sobre el uso seguro y respetuoso de los medios digitales en el currículo básico*. https://bit.ly/4eGngNd

MN6: Ley Orgánica N° 3, *Ley de Protección de Datos Personales y garantía de los derechos digitales* (5 de diciembre de 2018). https://bit.ly/4ds3NPc

MN7: Gobierno de España. (2021). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia*. https://bit.ly/4eiIxgn

MN8: Ley 23/2010, de 1 de octubre, *de la Autoridad Catalana de Protección de Datos*, (8 de octubre de 2010). https://bit.ly/3ZDt85J

MN9: Ley N° 7, *Ley de Atención y Protección a la Infancia y la Adolescencia de Castilla-La Mancha* (10 de marzo de 2023). https://bit.ly/3BgdqmL

MN10: Orden N° 178, *de la Consejería de Educación, Cultura y Deportes, por la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios* (14 de septiembre de 2022). https://bit.ly/3MZMhr0

MN11: Resolución, *de la Subsecretaría de la Conselleria de Educación, Investigación, Cultura y Deporte, por la que se dictan instrucciones para el cumplimiento de la normativa de protección de datos en los centros educativos públicos de titularidad de la Generalitat* (28 de junio de 2018). https://bit.ly/3Y0kfBL

2.3. Garantía del derecho a la educación en la sociedad digital

A continuación, se analiza el fenómeno de la garantía del derecho a la educación en la sociedad digital, explorando si se trata de derechos distintos o si el derecho a la educación digital es una extensión del derecho a la educación tradicional. Se presenta información proporcionada por el marco normativo y político, destacando la necesidad de que la educación digital esté en consonancia con los derechos fundamentales y los valores constitucionales. En términos generales se subraya la importancia de preparar a los docentes con competencias digitales y de garantizar la igualdad en el acceso a la tecnología para evitar la brecha digital.

Desde una perspectiva metodológica, se utilizan las siguientes preguntas para analizar el marco normativo y político:

1. ¿Son el derecho a la educación y el derecho a la educación digital derechos distintos? Esta pregunta es fundamental para comprender si la sociedad digital ha creado un nuevo paradigma en la educación o si simplemente ha transformado el existente, permitiendo un análisis más profundo de las implicaciones legales y sociales de ambos conceptos.
2. ¿Qué es la sociedad digital y cómo influye en la garantía del derecho a la educación? Este cuestionamiento permite explorar el efecto de la tecnología y la digitalización en el acceso y la calidad de la educación, identificando tanto oportunidades como barreras que deben ser abordadas.
3. ¿Cómo aparece regulado el derecho a la educación digital a nivel europeo y en la legislación estatal? Examinar la regulación proporciona una visión clara de las políticas y normas que respaldan o dificultan la implementación efectiva del derecho a la educación digital, ofreciendo una comparación entre diferentes niveles legislativos.
4. ¿Qué dicen sobre el derecho a la educación digital las legislaciones autonómicas? Analizar las legislaciones autonómicas permite identificar las variaciones territoriales y entender cómo se adapta el marco normativo a contextos locales específicos, destacando las mejores prácticas y áreas que requieren mayor atención.

2.3.1 ¿Son el derecho a la educación y el derecho a la educación en la sociedad digital derechos distintos?

El derecho a la educación digital es una expansión del derecho a la educación orientada a preparar y proteger al alumnado para la realidad digital actual. El derecho a la educación digital debe estar en concordancia con los derechos fundamentales y los valores constitucionales, que a su vez inspiran todas las actividades formativas promovidas por los poderes públicos. La Administración Pública tiene, en este sentido, un rol relevante, tal como se aprecia a continuación (MN12, 52, 4-5):

> Las Administraciones públicas velarán por el acceso de todos los estudiantes a los recursos digitales necesarios, para garantizar el ejercicio del derecho a la educación de todos los niños y niñas en igualdad de condiciones.
> En todo caso, las tecnologías de la información y la comunicación (TIC) y los

recursos didácticos que se empleen, se ajustarán a la normativa reguladora de los servicios y sociedad de la información y de los derechos de propiedad intelectual, concienciando en el respeto de los derechos de terceros.

Para la consecución del fin mencionado, se potencia que el profesorado adquiera competencias digitales, y enseñe y transmita los valores y derechos referidos (MN7. 18, 13-14; MN12, 52, 3). De esta forma, "las administraciones públicas deben garantizar la inserción del alumnado a la sociedad digital, promoviendo en todas las etapas formativas el uso adecuado de internet" (MN4. 30, 8 y 31, 1).

Es clave garantizar la igualdad y la calidad en el acceso a las herramientas digitales (MN3. 2, 4). Con ello se puede evitar la brecha digital de las personas más vulnerables y, al mismo tiempo, promover un uso razonable de la información y la comunicación, de acuerdo con la edad y la madurez de cada persona menor de edad (MN9, 50643, 15). Otro aspecto relevante, tiene que ver con la necesidad de disminuir también la brecha digital de género (MN10, 32782).

Dentro de los objetivos de la educación en todos los niveles, además, es posible encontrar finalidades vinculadas al desarrollo de la competencia digital, referidas al uso creativo, crítico y seguro de las tecnologías de la información y la comunicación para alcanzar los objetivos relacionados con el trabajo, la empleabilidad, el aprendizaje, el uso del tiempo libre, la inclusión y participación en la sociedad (MN5. 2, 5). Así, por ejemplo, en la educación primaria se identifica el objetivo de que el alumnado se inicie en la utilización de las tecnologías de la información y la comunicación, desarrollando un espíritu crítico ante los mensajes que reciben y elaboran (MN5. 1, 4). En la educación secundaria obligatoria, se señala la necesidad de que el alumnado desarrolle destrezas básicas en la utilización de tecnología y las fuentes de información para adquirir nuevos conocimientos con sentido crítico (MN5. 1, 5). Y, en bachillerato, se busca la utilización con solvencia y responsabilidad de las tecnologías de la información y la comunicación (MN5. 2, 1).

El derecho de educación digital, al ser entendido como la expansión del concepto del derecho de educación, implica incluir las competencias, habilidades y el acceso digital como forma de apoyo al desarrollo de este derecho (MP3. 5, 5). En este contexto se persigue la autonomía digital, entendida como la capacidad de controlar y adaptarse a un mundo digital con competencias y responsabilidad digitales (MP3. 9, 3), fomentando habilidades, destrezas, el desarrollo de la personalidad humana, la participación efectiva en la sociedad libre y la capacidad de las sociedades para decidir sobre su propio desarrollo (MP3. 5, 1).

La educación, en todos sus niveles, debe cumplir con cuatro características interrelacionadas: disponibilidad, accesibilidad, aceptabilidad y adaptabilidad. Dentro de esas cuatro características, se entiende la tecnología como una condición de disponibilidad y accesibilidad material (MP2. 3). Así, el acceso digital se entiende como parte del derecho a la educación. En este sentido, toda persona tiene el derecho y la responsabilidad de educarse y educar sobre y a través de las tecnologías digitales y de los nuevos derechos y las nuevas estructuras (MP13. 18, 9), incluida la inteligencia artificial. Lo anterior se considera necesario para interactuar de manera positiva, crítica y segura con la tecnología, siendo conscientes de los

potenciales problemas éticos, medioambientales, sobre protección de datos y privacidad, entre otros (MP6. 10, 2).

Sin embargo, el desarrollo de la educación digital, enmarcado en los derechos sociales, debe ir vinculado al deber de los Estados a establecer una dirección activa y deliberada a fin de producir cambios positivos para mejorar la aplicación del derecho de educación (MP3. 4, 1), de la modernización de los planes de estudios y de los métodos de aprendizaje y de enseñanza existentes (MP7. 15), además de invertir en el factor humano, especialmente en los docentes, que siguen siendo, en el contexto digital, esenciales para la aplicación del derecho a la educación (MP3. 3, 4) (MP7. 9).

La idea de que el derecho a la educación digital no es otra cosa que una expansión del derecho a la educación se refuerza con el hecho de que le son aplicables los mismos instrumentos a ambos, como el artículo 26 de la Declaración Universal de Derechos Humanos, los artículos 13 y 14 del Pacto Internacional de Derechos Económicos, Sociales y Culturales, los artículos 28 y 29 de la Convención sobre los Derechos del Niño, así como la convención relativa a la Lucha contra las Discriminaciones en la Esfera de la Enseñanza de la UNESCO (MP3. 4, 4).

2.3.2 ¿Qué es la sociedad digital y cómo influye en la garantía del derecho a la educación?

La sociedad digital representa una expansión del mundo, y el derecho a la educación debe garantizar el acceso a ese mundo expandido a través, entre otras cosas, del aprendizaje del uso de los medios digitales. Por ello, las administraciones públicas deben promover dentro de todas las etapas formativas el uso adecuado de Internet, que debe respaldarse en un profesorado adecuadamente formado para ello (MN7. 18, 13-14).

Si lo que se persigue es consolidar una sociedad digital democrática, la educación debe introducir programas de enseñanza relativos a la ciberseguridad en los planes de estudio, considerando una ciberhigiene, ciberseguridad, protección de datos y alfabetización mediática adecuada a la edad. Según la Ley Orgánica 3/2020 (MN12):

> El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales (MN12, 82,6).

En esta línea, más allá de los conocimientos instrumentales a que se ha hecho mención antes, la educación debe orientar al estudiantado para convertirse en un/a ciudadano/a crítico, capaz de tomar decisiones conscientes de los riesgos asociados a internet, como la desinformación en línea, el acoso y la violación de la seguridad de los datos personales (MP7. 6). En este sentido, y en relación con los derechos constitucionales, cobra importancia la garantía de la intimidad personal y familiar y la protección de datos personales, conforme a lo previsto en el artículo 83 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (MN4. 30, 8 y 31, 1).

2.3.3 ¿Cómo aparece regulado el derecho a la educación digital a nivel europeo y en la legislación estatal?

El proceso de transformación digital de la educación debe incluir medidas para garantizar el acceso igualitario a las tecnologías y a la formación en competencias digitales. Es esencial que todo el alumnado tenga acceso a dispositivos y recursos digitales adecuados, que enriquezcan el aprendizaje y la enseñanza. Este derecho se asegura a través de la puesta a disposición de aplicaciones, herramientas y recursos digitales específicos para facilitar el acceso a la educación digital (MN3. 2, 5; MN3. 6, 7).

El principio de igualdad, que prevalece sea cual sea el contexto del alumnado, debe garantizar las mismas oportunidades de acceso a los recursos digitales. Esto está alineado con la normativa europea que promueve el acceso equitativo a las tecnologías digitales (MN7. 12, 1).

Además, el artículo 83 de la Ley Orgánica 3/2018 establece que todo el alumnado tiene derecho a recibir una educación que incluya competencias digitales, garantizando así su formación integral en el uso de medios digitales y la protección de datos personales (MN6. 49-50).

Para responder a este desafío sin precedentes, resulta fundamental que la Administración Pública implemente políticas que promuevan el acceso equitativo a las tecnologías digitales en el ámbito educativo (MP10. 3, 4; MP10. 4, 1). En consonancia con lo que marcan los distintos documentos normativos revisados, España ha desplegado distintas iniciativas orientadas a esta transformación digital, con una base sólida de infraestructuras y un compromiso claro con la digitalización en todos los sectores, incluida la educación. En este sector en concreto, desde la primera década del siglo XXI se han llevado a cabo importantes inversiones a través de programas estatales como el de Escuela 2.0 y otros a nivel regional.

Para encauzar el proceso de transformación digital en la educación, se requiere un esfuerzo coordinado entre las distintas administraciones y actores educativos. Esto incluye establecer directrices claras y proporcionar los recursos necesarios para que todos los centros educativos puedan integrar las tecnologías digitales en sus procesos de enseñanza y aprendizaje (MP10. 4, 2; MP10. 14, 4).

2.3.4 ¿Qué dicen sobre el derecho a la educación digital las legislaciones autonómicas?

La legislación autonómica de Catalunya pone especial énfasis en la protección de datos y el uso seguro de tecnologías digitales en el ámbito educativo. La Autoridad Catalana de Protección de Datos proporciona directrices específicas para el uso ético y seguro de las tecnologías digitales en la educación, asegurando que se respeten los derechos de privacidad de los estudiantes (MN8. 9, 10).

Catalunya, además, destaca en su legislación autonómica la importancia de modernizar las infraestructuras educativas para integrar las nuevas tecnologías digitales, asegurando que los estudiantes tengan acceso a herramientas digitales avanzadas. Este enfoque busca garantizar un acceso equitativo a las tecnologías digitales, promoviendo la inclusión y la igualdad de oportunidades en el ámbito educativo (MP10. 4, 1).

La Junta de Comunidades de Castilla-La Mancha, en el ámbito de sus competencias, establece las medidas específicas adecuadas destinadas a la atención y protección a la infancia y la adolescencia, con el fin de promover y garantizar el disfrute pleno de los derechos reconocidos en el ordenamiento jurídico, así como el cumplimiento de los deberes y obligaciones (MN9. 50632,4). Además, esta comunidad actualiza y redefine el marco global de atención a la infancia y a las familias, en el marco de la parentalidad positiva, consolidando los apoyos e intervenciones de tipo preventivo, tanto los dirigidos al conjunto de la ciudadanía como los orientados a la atención especializada en determinadas situaciones. Pretende pues, poner el acento en el apoyo y acompañamiento a las familias, y a los propios niños, niñas y adolescentes, para su adecuado y armónico desarrollo en una sociedad libre de violencia contra la infancia y la adolescencia que asegure su futuro como personas adultas e integradas en su comunidad. Pone especialmente el foco en la prevención y atención, adecuándose a los tiempos actuales y a nuevas realidades relacionadas con el acceso y uso de nuevas tecnologías (MN9. 50625, 2).

2.3.5 Síntesis

En los documentos analizados, el derecho a la educación digital aparece como una expansión necesaria del tradicional derecho a la educación, proponiendo una adaptación de éste a la realidad actual y alineándose con los derechos fundamentales y los valores constitucionales. Por tanto, se señala como indispensable preparar y dotar al profesorado de competencias digitales y garantizar el acceso equitativo a la tecnología para evitar la brecha digital. Además, se destaca la importancia de la ciberseguridad y la alfabetización mediática, como señala la regulación del derecho a la educación digital a nivel europeo y estatal, con un enfoque particular en la igualdad de acceso a las tecnologías.

A nivel autonómico, la legislación en comunidades autónomas como Catalunya y Castilla-La Mancha enfatiza la protección de datos y el uso seguro de tecnologías digitales en el ámbito educativo. La normativa autonómica también pone énfasis en modernizar las infraestructuras educativas para integrar las nuevas tecnologías en las prácticas educativas cotidianas, asegurando que todos los estudiantes tengan acceso a herramientas digitales avanzadas. Con este enfoque, la legislación busca promover una educación digital inclusiva y equitativa, asegurando que todos los estudiantes, independientemente de su contexto, tengan las mismas oportunidades de acceso a los recursos digitales para su desarrollo integral y su participación efectiva en la sociedad digital.

2.3.6 Listado de documentos incluidos

MP2: Organización de las Naciones Unidas. (1999). *Observación General nº13 relativa al Derecho a la Educación*. https://bit.ly/3zCXv1o

MP3: Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/4elJBzM

MP6: Comisión Europea, Dirección General de Educación, Juventud, Deporte y Cultura, (2023). *Plan de acción de educación digital 2021-2027: mejorar la provisión de capacidades digitales en la educación y la formación*, Oficina de Publicaciones de la Unión Europea. https://bit.ly/47HzzXr

MP7: Parlamento Europeo. (2021). *Propuesta de resolución del Parlamento Europeo: Informe sobre la formulación de la política de educación digital*. https://bit.ly/47Ma8E6

MP8: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 21: Modernización y digitalización del sistema educativo, incluida la educación temprana de 0-3 años*. https://bit.ly/3XIqtoH

MP10: Gobierno de España. (n.d.). *España Digital 2026.*

MP13: Generalitat de Catalunya. (2019). *Carta catalana por los derechos y las responsabilidades digitales.* Departament de Polítiques Digitals i Administració Pública. https://bit.ly/3Bks10t

MN3: Resolución, *de la Subsecretaría, por la que se publica el Convenio entre el Ministerio de Educación y Formación Profesional, el Ministerio de Asuntos Económicos y Transformación Digital y la Entidad Pública Empresarial Red.es, M.P., para la ejecución del programa "Educa en Digital"* (7 de julio de 2020). https://bit.ly/3XMmtDP

MN4: Ley Ogánica N° 8, *Ley de protección integral a la infancia y la adolescencia frente a la violencia* (4 de junio de 2021). https://bit.ly/4doiVx1

MN5: Ministerio de Educación y Formación Profesional. (2019). *Informe sobre el uso seguro y respetuoso de los medios digitales en el currículo básico*. https://bit.ly/4eGngNd

MN6: Ley Orgánica N° 3, *Ley de Protección de Datos Personales y garantía de los derechos digitales* (5 de diciembre de 2018). https://bit.ly/4ds3NPc

MN7: Gobierno de España. (2021). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia*. https://bit.ly/4eiIxgn

MN8: Ley 23/2010, de 1 de octubre, *de la Autoridad Catalana de Protección de Datos*, (8 de octubre de 2010). https://bit.ly/3ZDt85J

MN9: Ley N° 7, *Ley de Atención y Protección a la Infancia y la Adolescencia de Castilla-La Mancha* (10 de marzo de 2023). https://bit.ly/3BgdqmL

MN10: Orden N° 178, *de la Consejería de Educación, Cultura y Deportes, por la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios* (14 de septiembre de 2022). https://bit.ly/3MZMhr0

2.4. Protección de la infancia en la sociedad digital ¿Dónde termina la responsabilidad de un actor y donde comienza la del otro?

La protección de la infancia en la sociedad digital es una responsabilidad compartida que requiere la participación coordinada de diversos actores, entre ellos la Administración Pública, las escuelas y las corporaciones digitales. Como hemos visto a la largo de este informe, cada uno de estos actores tiene responsabilidades y/o líneas de acciones específicas que, cuando se combinan de manera efectiva, pueden crear un entorno seguro para la infancia.

A partir del análisis del marco político y normativo llevado a cabo en el primer apartado de este documento, se detallan algunas de las principales responsabilidades específicas de cada actor, junto con las áreas de complementariedad e interposición de sus funciones y los vacíos identificados en sus acciones.

2.4.1. Responsabilidades y Acciones de la Administración Pública, la Escuela y las Corporaciones Tecnológicas.

La Administración Pública, las Escuelas y las Corporaciones Digitales tienen responsabilidades y líneas de acción específicas y complementarias en el contexto de la protección de la infancia en la sociedad digital. La siguiente tabla sintetiza las diversas líneas de acciones y/o responsabilidades que recogen los resúmenes del apartado 1.2. Administración Pública, 1.3. Escuelas y 1.4. Corporaciones Tecnológicas, distribuidas según las categorías: digitalización de la educación, protección de datos y ciberseguridad, tecnologías digitales en el currículo educativo y competencia digital del profesorado, con la finalidad de ordenar las líneas de acción o responsabilidades de los actores mencionados.

Tabla 1

Síntesis de las líneas de acción y/o responsabilidades de la Administración Pública, Escuela y Corporaciones Tecnológicas.

Dimensión	Administración Pública	Escuela	Corporaciones Tecnológicas
Digitalización de la Educación	Proveer educación pública, gratuita y de calidad, regulando la participación de actores privados (MP3, 6, 6). Invertir en digitalización de la educación y formación profesional, incluyendo infraestructuras, equipos y conectividad (MP10, 15, 3; MN3, 4, 4; MP10, 122, 5; MN12, 52, 4). Crear planes de acceso a Internet para superar brechas	Fomentar el uso de tecnologías digitales en enseñanza-aprendizaje para desarrollar la competencia digital del alumnado y profesorado (MN10, 32780, 5; MN12, 52, 2). El equipo directivo debe liderar proyectos tecnológicos, incluyendo IA, para personalizar itinerarios de aprendizaje y analizar la	Proporcionar servicios digitales que faciliten el aprendizaje (MP3, 14, 1). Colaborar estrechamente con estados, ONGs, agentes diversos y Corporaciones Tecnológicas para establecer políticas efectivas (MP1, 13, 6-7).

	digitales (MN6, 54, 5-6; MN9, 23, 15). Proporcionar servicios digitales y recursos a los centros educativos para mejorar la actividad educativa, incluyendo aplicaciones didácticas, contenidos educativos de calidad y servicios de registro académico (MP14, 10, 1; MN11, 46425, 2; MN12, 42, 1).	evolución del alumnado (MN3, 6, 9). El profesorado debe aplicar metodologías digitales y TIC en su labor diaria, e innovar en los procesos de enseñanza-aprendizaje (MN3, 6, 8; MP14, 23, 2). Las familias deben apoyar el desarrollo educativo digital de los hijos e hijas (MN3, 6, 5).	Desarrollar soluciones tecnológicas efectivas para mejorar la seguridad y bienestar en línea de la infancia (MN4, 36, 2-3).
Protección de Datos y Ciberseguridad	Monitorear y proteger el tratamiento de datos personales (MP1, 8, 4). Recopilar datos sobre el impacto del entorno digital en la infancia (MP1, 6, 1). Promover el intercambio de información y buenas prácticas sobre protección de datos (MN4, 20, 11). Garantizar protección de derechos fundamentales en entornos digitales (MN7, 12, 6). Adherirse a los principios de protección de datos según el RGPD (MP15, 20836, 5; MN12, 51, 7) Coordinar respuestas a ciberincidentes y gestionar eventos de seguridad centralizados mediante el Centro de Operaciones de Ciberseguridad (MP10, 52, 2-3).	Los centros educativos deben implementar buenas prácticas de ciberseguridad y colaborar con agentes como la Agencia de Protección de Datos (MP14, 29, 2). Los centros educativos deben adoptar medidas para proteger al alumnado de situaciones de violencia (MN4, 25, 3; MN4, 24, 7-8; MN12, 82, 6). Los equipos directivos tienen la responsabilidad de mantener la confidencialidad de los datos del alumnado, (MN11, 13, 1-3; MN4, 32, 2). El profesorado debería garantizar la salud digital y prevenir el uso indebido y/o adictivo de las TIC mediante formación específica en seguridad y uso responsable de Internet (MN4, 19, 5). Las familias deben utilizar mecanismos de control parental y herramientas de denuncia y bloqueo para proteger a los hijos e hijas (MN4, 36, 7). Las familias deben otorgar o denegar el consentimiento informado (MP1, 8, 3-4).	Implementar medidas para proteger la privacidad y seguridad de los menores (MP1, 4, 10-11). Asegurar que los dispositivos digitales cuenten con sistemas de control parental activados por defecto (MP1, 40, 2). Desarrollar productos adaptados a diferentes grupos de edad y mecanismos de verificación de edad (MN4, 36, 8).

Tecnologías Digitales en el Currículo Educativo	Incluir competencias digitales en el currículo educativo (MN5, MN6, MN12, MP12, MP14). Abordar el uso seguro y responsable de las TIC en todas las materias y etapas educativas, desde Educación Primaria hasta Bachillerato (MN5, 1, 1). Promover la competencia digital en educación y la formación de docentes (MP12, 4-5; MN12, 52, 3). Incorporar competencias digitales y elementos relacionados con riesgos del uso inadecuado de TIC en asignaturas de libre configuración (MN6, 49, 12).	Colaborar con sector tecnológico, ciudadanía, universidades y Administración Pública para garantizar el acceso universal al alumnado (MP1, 3, 12). Liderar pedagógicamente el proceso de transformación digital en las escuelas (MP14, 28, 3). El profesorado debería desarrollar integralmente la Competencia Digital Docente (CDD)(MP14, 23, 3). El profesorado debería facilitar el desarrollo de competencias y espacios seguros en Internet para promover la participación social y cívica de niños, niñas y adolescentes (MP9, 4, 5). Apoyar a los hijos en su desarrollo educativo digital mediante formación y acompañamiento (MN4, 35, 8; MP7, 15).	Colaborar con instituciones educativas para desarrollar contenidos curriculares que incluyan seguridad digital y alfabetización tecnológica (MN3, 3, 3). Ofrecer programas de formación para que los docentes puedan enseñar al alumnado sobre el uso seguro y responsable de la tecnología (MP1, 6, 10).
Competencia Digital del Profesorado	Garantizar que el profesorado adquiera competencias digitales y reciba la formación necesaria (MN6, 49-50). Desarrollar y adoptar marcos de competencia digital docentes, como DigCompEdu (MP14, 8, 3-4). Facilitar la formación continua del profesorado, coordinando con universidades y fomentando redes docentes (MP8, 12, 3; MP14, 23, 1-6; MN12, 77, 8).	El profesorado debe poseer competencias digitales (MP6, 10, 6; MP7, 22, 1). Los equipos directivos deberían acompañar al profesorado en el desarrollo de proyectos basados en tecnología, asegurando que los docentes reciban el apoyo necesario para integrar efectivamente las tecnologías digitales en el proceso educativo (MN3, 6, 9; MN12, 52, 2).	Ofrecer programas de formación para que el profesorado pueda enseñar sobre el uso seguro y responsable de la tecnología (MN3, 3, 3; MN12, 50, 3).

Fuente: Elaboración propia

Podemos observar que en la dimensión “digitalización de la educación”, la Administración Pública se centra en proporcionar recursos, infraestructura y acceso equitativo a Internet, superando las brechas digitales y asegurando una educación de calidad para todo el alumnado. La Escuela, por su parte, debe fomentar el uso de tecnologías digitales en el aula, liderar proyectos tecnológicos y apoyar el desarrollo educativo digital de los alumnos a través

de metodologías innovadoras y prácticas pedagógicas avanzadas. Las Corporaciones Tecnológicas complementan estos esfuerzos al proporcionar servicios digitales y colaborar estrechamente con diversos actores para desarrollar soluciones tecnológicas efectivas que mejoren la seguridad y el bienestar de la infancia.

En cuanto a la dimensión “protección de datos y ciberseguridad”, la Administración Pública tiene la responsabilidad de monitorear el tratamiento de datos personales y promover buenas prácticas de protección de datos, asegurando el cumplimiento de las regulaciones y coordinando respuestas a ciberincidentes. Las Escuelas deben implementar buenas prácticas de ciberseguridad, proteger al alumnado de situaciones de violencia y mantener la confidencialidad de los datos del alumnado. Las Corporaciones Tecnológicas deben implementar medidas robustas para proteger la privacidad y seguridad de los menores, asegurando que los dispositivos digitales cuenten con sistemas de control parental y desarrollando productos adaptados a las necesidades de diferentes grupos de edad.

En la integración de tecnologías digitales en el currículo educativo, la Administración Pública debe incluir competencias digitales en el currículo y promover la competencia digital en la educación, asegurando que los docentes reciban la formación necesaria. Las Escuelas deben colaborar con diversos actores para garantizar el acceso universal a las tecnologías, liderar el proceso de transformación digital y desarrollar la Competencia Digital Docente. Las Corporaciones Tecnológicas deben colaborar con las instituciones educativas para desarrollar contenidos curriculares que incluyan la seguridad digital y la alfabetización tecnológica, ofreciendo programas de formación para los docentes.

Finalmente, en lo que respecta a la competencia digital del profesorado, la Administración Pública debe garantizar que el profesorado adquiera competencias digitales a través de marcos de competencia digital como DigCompEdu y facilitar su formación continua. Los equipos directivo de los centros educativos deben apoyar a los docentes en el desarrollo de proyectos tecnológicos y asegurar que reciban el apoyo necesario para integrar efectivamente las tecnologías digitales en el proceso educativo. Las Corporaciones Tecnológicas deben ofrecer programas de formación que capaciten a los docentes para enseñar sobre el uso seguro y responsable de la tecnología.

Resumiendo, se observa que la Administración Pública tiene una responsabilidad primordial en la creación y promoción de políticas que aseguren un uso ético y efectivo de las tecnologías digitales en la educación. Esto incluye no solo garantizar la no discriminación y la igualdad en el acceso a la tecnología y la conectividad a Internet, sino también asegurar que la educación sea pública, gratuita y de calidad, con una inversión adecuada en la digitalización del sistema educativo. Esto abarca desde la infraestructura hasta la formación continua de docentes, incluyendo la provisión de equipos y la conectividad necesaria (MN6, 49-50). Además, la Administración Pública debe desempeñar un rol activo en la supervisión y monitoreo del

cumplimiento de las leyes y políticas establecidas, garantizando que se respeten los derechos digitales de los menores y se proteja su integridad en el entorno digital.

Por su parte, las Escuelas tienen la responsabilidad de implementar metodologías de enseñanza-aprendizaje adaptadas al entorno digital, promoviendo la alfabetización digital tanto entre los estudiantes como entre los docentes. Esto implica la integración de competencias digitales en los currículos educativos, la protección de los datos del alumnado, y la adopción de medidas para prevenir la violencia en línea. Las escuelas deben innovar constantemente en los procesos educativos mediante el uso de Tecnologías de la Información y la Comunicación (TIC), asegurando que los recursos educativos digitales sean de alta calidad y que el entorno digital en el que operan los estudiantes sea seguro y propicio para el aprendizaje responsable (MP1, 6, 1).

En cuanto a las Corporaciones Tecnológicas, su responsabilidad radica en el desarrollo de contenidos curriculares que incluyan la seguridad digital y en la oferta de programas de formación para docentes. Además, deben proporcionar herramientas y soluciones que mejoren tanto el acceso como la seguridad en línea, implementando medidas robustas de protección de datos y privacidad en sus plataformas. Es fundamental que estas corporaciones faciliten el control parental y aseguren el consentimiento informado para el uso de datos personales de menores. Su responsabilidad también incluye la provisión de recursos tecnológicos y el apoyo en la capacitación de educadores, colaborando estrechamente con las instituciones educativas y la Administración Pública para garantizar que la tecnología sea un aliado y no un riesgo para la infancia (MN7, 14, 3-4; MN7, 18-19).

2.4.2. Vacíos en las acciones de la Administración Pública, las Escuelas y las Corporaciones Digitales en la Protección de la Infancia en la sociedad digital.

En el ámbito de la protección de la infancia en la sociedad digital, identificamos algunos vacíos en las acciones de la Administración Pública, las Escuelas y las Corporaciones Digitales. A continuación, se presentan estos vacíos y su impacto:

En los textos analizados se menciona que la Administración Pública debe promover la formación continua (MN6, 49-50), pero consideramos que existe un vacío en la coordinación de esta formación en ciberseguridad y uso seguro de tecnologías digitales entre la Administración Pública, las Escuelas y las Corporaciones Tecnológicas. Esta falta de claridad podría llevar a inconsistencias en la formación y actualización de conocimientos tanto para el profesorado como el alumnado.

También se menciona que la Administración Pública es responsable de realizar investigaciones periódicas sobre el impacto digital en la infancia (MP1, 6, 1); aunque se menciona la realización de investigaciones por parte de la Administración Pública, no hay una mención clara de cómo los resultados de estas investigaciones se comparten con las Escuelas y Corporaciones Tecnológicas.

La Administración Pública debe abordar las brechas digitales y de género (MN7, 14, 3-4; MN7, 18-19); aunque se menciona la lucha contra la brecha digital de género y la dotación de equipamiento, no se especifica claramente cómo se garantiza la inclusión digital para estudiantes con discapacidades o en zonas rurales. Esta falta de especificidad podría resultar en una falta de recursos o apoyo para estos grupos vulnerables, persistiendo de esa manera en la exclusión digital.

También existe un vacío en las responsabilidades de las Corporaciones Tecnológicas en relación con la ciberseguridad, porque solo hay menciones de responsabilidad en este aspecto en las Administraciones Públicas y las Escuelas.

2.4.3. Síntesis

Podemos concluir que, aunque exista un marco general de responsabilidades de la Administración Pública, las escuelas y las corporaciones, también existen áreas donde las responsabilidades no están claramente definidas o donde hay vacíos en la coordinación y aplicación práctica. Es importante que estos vacíos sean abordados para asegurar la protección de la infancia en la sociedad digital.

Luego del análisis podemos responder a la pregunta inicial: ¿dónde termina la responsabilidad de un actor y dónde comienza la del otro? Diremos que la Administración Pública inicia su responsabilidad en materia de Protección de la Infancia con la creación y promoción de políticas que aseguren un uso ético y efectivo de las tecnologías digitales en la educación, que incluye garantizar la no discriminación y la igualdad en el acceso a la tecnología y conectividad a Internet. Además, debe proveer los recursos para que la educación sea pública, gratuita y de calidad, invirtiendo en la digitalización de la educación y formación a los docentes, incluyendo infraestructuras, equipos y conectividad. La responsabilidad de la Administración Pública se extiende hasta la supervisión y el monitoreo de las leyes y políticas establecidas.

La responsabilidad de las escuelas comienza con la implementación de metodologías de enseñanza-aprendizaje adaptadas al entorno digital, promoviendo la alfabetización digital entre estudiantes y docentes, integrando las competencias digitales en los currículos educativos, protegiendo los datos del alumnado y adoptando medidas contra la violencia en línea. Además, implica innovar en los procesos educativos mediante el uso de tecnologías digitales, proporcionando servicios y recursos educativos de calidad al alumnado, y garantizando un entorno seguro y responsable para el uso de estas tecnologías.

Las Corporaciones Tecnológicas comienzan su responsabilidad en el desarrollo de contenidos curriculares que incluyan la seguridad digital y la oferta de programas de formación para docentes, proporcionando herramientas y soluciones para mejorar el acceso y la seguridad en línea, implementando medidas de protección de datos y privacidad en sus plataformas, facilitando el control parental y el consentimiento informado para el uso de datos personales de menores. Por ello, su responsabilidad llega hasta la provisión de esos recursos tecnológicos

y el apoyo en la formación de educadores, colaborando con las instituciones educativas y la Administración Pública.

La Administración Pública, las Escuelas y las Corporaciones Tecnológicas tienen responsabilidades distintas pero complementarias en la protección de la infancia en la sociedad digital. La Administración Pública lidera con la creación de políticas y la supervisión de la protección de datos, las Escuelas implementan y educan, y las Corporaciones Tecnológicas proporcionan las herramientas y colaboran en la capacitación y protección de los menores.

2.4.2 Listado de documentos utilizados

MP1: Organización de las Naciones Unidas. (2021). *Observación General Nº 25, relativa a los derechos de los niños en relación con el entorno digital, Convención sobre los Derechos del Niño.* https://bit.ly/4gWWnXx

MP3: Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/3XVI7GV

MP6: Comisión Europea, Dirección General de Educación, Juventud, Deporte y Cultura, (2023). *Plan de acción de educación digital 2021-2027: mejorar la provisión de capacidades digitales en la educación y la formación*, Oficina de Publicaciones de la Unión Europea. https://bit.ly/47HzzXr

MP7: Parlamento Europeo. (2021). *Propuesta de resolución del Parlamento Europeo: Informe sobre la formulación de la política de educación digital*. https://bit.ly/47Ma8E6

MP8: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 21: Modernización y digitalización del sistema educativo, incluida la educación temprana de 0-3 años*. https://bit.ly/3XIqtoH

MP9: Pacto de Estado. (2023). Protegiendo a la infancia y la adolescencia en el entorno digital, medidas de consenso para un Pacto de Estado ante la nueva legislatura y la presidencia de España en la Unión Europea. https://bit.ly/3BhnMTq

MP10: Gobierno de España. (n.d.). *España Digital 2026.*

MP12: Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia: Componente 19. Plan Nacional de Capacidades Digitales.* https://bit.ly/3ZKocvM

MP14: Generalitat de Catalunya. Departament d'Educació. (2020). *Pla d'educació digital de Catalunya 2020-2023*. https://bit.ly/3z33nyv

MP15: Decreto Nº 55, *por el que se establece la política de protección de datos en la Administración de la Junta de Comunidades de Castilla-La Mancha* (6 de junio de 2023). https://bit.ly/4em0BGi

MN3: Resolución, *de la Subsecretaría, por la que se publica el Convenio entre el Ministerio de Educación y Formación Profesional, el Ministerio de Asuntos Económicos y Transformación Digital y la Entidad Pública Empresarial Red.es, M.P., para la ejecución del programa "Educa en Digital"* (7 de julio de 2020). https://bit.ly/3XMmtDP

MN4: Ley Ogánica N° 8, *Ley de protección integral a la infancia y la adolescencia frente a la violencia* (4 de junio de 2021). https://bit.ly/4doiVx1

MN5: Ministerio de Educación y Formación Profesional. (2019). *Informe sobre el uso seguro y respetuoso de los medios digitales en el currículo básico*. https://bit.ly/4eGngNd

MN6: Ley Orgánica N° 3, *Ley de Protección de Datos Personales y garantía de los derechos digitales* (5 de diciembre de 2018). https://bit.ly/4ds3NPc

MN7: Gobierno de España. (2021). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia*. https://bit.ly/4eiIxgn

MN9: Ley N° 7, *Ley de Atención y Protección a la Infancia y la Adolescencia de Castilla-La Mancha* (10 de marzo de 2023). https://bit.ly/3BgdqmL

MN10: Orden N° 178, *de la Consejería de Educación, Cultura y Deportes, por la que se regula la elaboración del Plan digital de los centros educativos sostenidos con fondos públicos no universitarios* (14 de septiembre de 2022). https://bit.ly/3MZMhr0

MN11: Resolución, *de la Subsecretaría de la Conselleria de Educación, Investigación, Cultura y Deporte, por la que se dictan instrucciones para el cumplimiento de la normativa de protección de datos en los centros educativos públicos de titularidad de la Generalitat* (28 de junio de 2018). https://bit.ly/3Y0kfBL

MN12: Ley Orgánica N° 3, *Ley por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación* (29 de diciembre de 2020). https://bit.ly/3ZHHXUX

Conclusiones

El presente informe se ha construido a partir del análisis de 32 documentos que forman parte del marco normativo y político vigente en torno a la protección de la infancia en la sociedad digital. La revisión y organización de la información nos permitió identificar y definir a los actores clave que participan en este proceso. Al mismo tiempo, se han abordado algunas preguntas que han emergido en torno a la intersección de marcos y responsabilidades.

En relación con la primera parte del trabajo, la información se ha organizado en torno a cuatro de los actores clave en la protección de la infancia:

Administración Pública:

> La Administración Pública tiene la responsabilidad de diseñar y ejecutar políticas que garanticen la protección de los menores en el entorno digital. Según los marcos normativos, la Administración debe asegurar el acceso equitativo a tecnologías, promover la alfabetización digital y velar por la seguridad de los datos personales de los menores. Además, es responsable de regular y supervisar las acciones de otros actores involucrados, como las Corporaciones Tecnológicas, para que se ajusten a los derechos de la infancia. El rol de la Administración Pública incluye también la formación de educadores/as y ciudadanos/as para un uso responsable y seguro de las tecnologías.

Escuelas:

> Las instituciones educativas son otro actor clave en la protección de la infancia. Se les asigna la tarea de implementar competencias digitales en el currículo escolar, formando a los estudiantes en el uso ético y seguro de las tecnologías. Las escuelas deben garantizar que todos los alumnos, independientemente de su situación socioeconómica, tengan acceso a los recursos digitales necesarios para su desarrollo educativo. Asimismo, se espera que colaboren estrechamente con la Administración Pública para aplicar las normativas en cuanto a la protección de los datos y el manejo seguro de las plataformas digitales.

Corporaciones Tecnológicas:

> Las grandes empresas tecnológicas tienen un papel crucial en la provisión de plataformas y herramientas educativas, y están obligadas a garantizar la seguridad y privacidad de los menores. Las Corporaciones Tecnológicas deben cumplir con normativas de protección de datos y asegurar que las plataformas que ofrecen no expongan a los niños a riesgos como el ciberacoso o la explotación de sus datos personales. También se les exige colaborar con las escuelas y la Administración Pública para integrar herramientas que promuevan la alfabetización digital y el aprendizaje seguro.

Actores de significación jurídica:

> Este grupo incluye a entidades como tribunales, autoridades de protección de datos y organismos de control, cuya función es garantizar que se cumpla con el marco legal que protege a los menores en el entorno digital. Estos actores son responsables de supervisar la implementación y el cumplimiento de leyes relacionadas con la privacidad, la seguridad en línea y los derechos digitales de los niños. Su papel también incluye la evaluación de casos de vulneración de derechos y la imposición de sanciones cuando sea necesario.

En conjunto, estos actores forman un ecosistema interconectado en el que las acciones y decisiones impactan directamente en la protección de la infancia en la sociedad digital.

En relación con la segunda parte, algunas de las ideas más relevantes de las cuatro preguntas planteadas son:

1. ¿El derecho a la educación y el derecho a la educación digital son derechos distintos?
   Los documentos analizados afirman que el derecho a la educación digital es una extensión necesaria del derecho general a la educación. A medida que las tecnologías se integran en los sistemas educativos, se hace indispensable garantizar que todos los estudiantes tengan acceso a herramientas digitales. La educación digital, por lo tanto, debe ser un derecho en sí mismo, con el fin de asegurar la igualdad de oportunidades y el acceso a recursos que permitan el desarrollo de competencias necesarias para la vida en la era digital.

2. ¿Qué es la sociedad digital y cómo influye en la garantía del derecho a la educación?
   La digitalización ha transformado el acceso y la naturaleza misma de la educación. El uso de plataformas digitales y herramientas tecnológicas abre nuevas oportunidades para la enseñanza y el aprendizaje, pero también plantea retos relacionados con la brecha digital y la protección de los menores en línea. De acuerdo con el análisis llevado a cabo, la digitalización exige que las políticas educativas incluyan medidas que aseguren un acceso equitativo a la tecnología y protejan a los menores de riesgos como la exposición a contenidos inapropiados o la explotación de sus datos.

3. ¿Cómo se regula el derecho a la educación digital a nivel europeo y en la legislación nacional?
   Del análisis documental se plantea que, a nivel europeo, el derecho a la educación digital está regulado por directrices que promueven la alfabetización digital, el acceso equitativo a la tecnología y la protección de los menores. En la legislación española, se pone un énfasis especial en la integración de competencias digitales en los currículos escolares y la provisión de infraestructuras que garanticen el acceso a recursos digitales para todos los estudiantes. Las leyes estatales y autonómicas buscan además establecer medidas de protección de datos y ciberseguridad para salvaguardar los derechos de los menores.

4. ¿Qué dicen sobre el derecho a la educación digital las legislaciones autonómicas? Las legislaciones autonómicas varían en cuanto a su enfoque, pero todas coinciden en la necesidad de garantizar el acceso igualitario a tecnologías digitales en el ámbito educativo. Normativas como la Ley N° 7 de Castilla-La Mancha subrayan la importancia de proporcionar los recursos necesarios para asegurar que los estudiantes más vulnerables también puedan acceder a la educación digital. En general, estas legislaciones ponen énfasis en reducir la brecha digital y en promover un uso seguro y responsable de las tecnologías.

En síntesis, este informe destaca que la protección de la infancia en la sociedad digital es una tarea multidimensional, en la que participan múltiples actores, cada uno con roles y responsabilidades definidos. La Administración Pública, las escuelas, las Corporaciones Tecnológicas y los actores de significación jurídica deben coordinar esfuerzos para garantizar que los menores puedan navegar y aprender en entornos digitales de forma segura.

Referencias

Castañeda, L., Salinas, J., & Adell-Segura, J. (2020). Hacia una visión contemporánea de la Tecnología Educativa. *Digital Education Review*, 37, 240-268. https://doi.org/10.1344/der.2020.37.240-268

Latorre, A., Del Rincón, D., & Arnal, J. (1996). *Bases Metodológicas de la Investigación Educativa*. Hurtado Ediciones.

Massot, I., Dorio, I., & Sabariego, M. (2009). Estrategias de análisis y recogida de información. En R. Bisquerra, (Ed.), *Metodología de la investigación educativa* (pp. 330-366). La Muralla.

Pangrazio, L., & Selwyn, N. (2020) Towards a school-based critical data education. *Pedagogy, Culture & Society,* 1–18. https://doi.org/10.1080/14681366.2020.1747527

Parcerisa, L., Jacovkis Halperin, J., Rivera Vargas, P., & Herrera Urízar, G. (2022). Corporaciones tecnológicas, plataformas digitales y privacidad: comparando los discursos sobre la entrada de las BigTech en la educación pública. *Revista Española de Educación Comparada,* 42, 221-239. https://doi.org/10.5944/reec.42.2023.34417

Perrotta, C., Gulson, K. N., Williamson, B., & Witzenberger, K. (2021). Automation, APIs and the distributed labour of platform pedagogies in Google Classroom. *Critical Studies in Education, 62*(1), 97-113. https://doi.org/10.1080/17508487.2020.1855597

Relatora Especial de las Naciones Unidas. (2022). *Repercusiones de la digitalización de la educación en el derecho a la educación Informe de la Relatora Especial sobre el derecho a la educación, Koumbou Boly Barry*. https://bit.ly/4elJBzM

Rivera-Vargas, P., Jacovkis, J., Herrera-Urízar, G., Calderón-Garrido, D., Miño-Puigcercós, R., Parcerisa, L., Folguera, S., Moreno, A., Massot, B., Passerón, E., Alonso, C., Gasull-Figueras, L., & Rilo-Borredà, C. (2023). *Plataformas digitales BigTech del sistema educativo catalán y derechos de la infancia: amenazas y retos*. Informe final proyecto edDIT *"Corporacions tecnològiques, plataformes educatives digitals i garantia dels drets de la infància amb enfocament de gènere"*, aFFaC y Esbrina Recerca Universitat de Barcelona. http://hdl.handle.net/2445/192941

Yeung, K. (2018). Five Fears about Mass Predictive Personalisation in an Age of Surveillance Capitalism. *International Data Privacy Law,* 8, 258-269. https://doi.org/10.1093/idpl/ipy020