DeepL
Subscribe to DeepL Pro to translate larger documents.
Visit www.DeepL.com/pro for more information.

European Commission

Centro Común de Investigación

Repercusiones de la legislación digital de la UE en la educación y la formación

Análisis de la Ley de Servicios Digitales, la Ley de Mercados Digitales, la Ley de Ciberseguridad, la Ley de Ciberresiliencia, la Ley de Gobernanza de Datos y la Ley de Datos

2026

ASPECTOS DESTACADOS

- **La Ley de Servicios Digitales** beneficia a los estudiantes, los educadores y las instituciones educativas al mejorar la seguridad y la transparencia del entorno digital en su conjunto, ya que establece obligaciones para los proveedores de servicios de intermediación digital, incluida la moderación de contenidos y disposiciones especiales para la protección de menores en las plataformas en línea. Las plataformas de muy gran tamaño están sujetas a requisitos más estrictos, mientras que los proveedores más pequeños (fundamentales para el sector de la tecnología educativa de la UE) están exentos de determinados requisitos.
- **La Ley de Mercados Digitales** promueve mercados digitales justos y competitivos al imponer obligaciones y prohibiciones específicas a las plataformas designadas como «guardianas», lo que crea mayores oportunidades para que las empresas de tecnología educativa compitan en condiciones más equitativas. Las instituciones educativas, los estudiantes y los docentes podrían beneficiarse de una mayor variedad de opciones, flexibilidad e innovación en el mercado de la tecnología educativa, así como de derechos mejorados de portabilidad de datos y protección frente a la elaboración de perfiles.
- **La Ley de Ciberseguridad** permite a los proveedores de tecnología educativa (EdTech) obtener la certificación de sus productos, servicios y procesos en el marco de sistemas de certificación de ciberseguridad armonizados y reconocidos en toda la UE. Dichos certificados pueden ayudar a las instituciones educativas a identificar y adquirir herramientas digitales fiables.
- **La Ley de Resiliencia Cibernética** contribuye a que las instituciones educativas se beneficien de un entorno digital más seguro, ya que los desarrolladores de tecnología educativa deben subsanar las vulnerabilidades a lo largo de todo el ciclo de vida de un producto y notificar los incidentes significativos a las autoridades.
- **La Ley de Gobernanza de los Datos** establece marcos para los servicios de intermediación de datos y el altruismo de datos, lo que fomentará la creación de conocimiento gracias a un mayor intercambio de datos valiosos para la investigación en análisis del aprendizaje.
- **La Ley de Datos** otorga a los alumnos y a los educadores un acceso y un uso más justos de los datos generados por los productos conectados (por ejemplo, dispositivos wearables) y los servicios relacionados que utilizan, reforzando la portabilidad, la interoperabilidad y los derechos de los usuarios sobre los datos que contribuyen a generar. Las instituciones educativas también pueden beneficiarse del derecho a cambiar de proveedor de servicios en la nube de forma efectiva.

Antecedentes

La Comisión Europea se ha comprometido a impulsar la transformación digital de los sistemas de educación y formación en toda la UE, tal y como se refleja en iniciativas como el *Plan de Acción para la Educación Digital*[1] y el próximo Paquete de Educación en el marco de la «Unión de las Competencias»(2) .

El «acervo digital» de la UE, también conocido como «código normativo digital», es el conjunto de normas de la UE que regulan las tecnologías digitales emergentes, la ciberseguridad, las plataformas en línea y las comunicaciones electrónicas. En este contexto, es importante tener en cuenta los posibles efectos de dicha normativa en los agentes del ámbito educativo. A efectos de este informe, nos centramos en las implicaciones de seis actos legislativos seleccionados para la educación y la formación (véase la tabla 1). Otras normativas incluidas en el acervo digital, como el Reglamento General de Protección de Datos (RGPD) y la Ley de Inteligencia Artificial, tienen implicaciones adicionales para el sector y merecen un análisis aparte.

Aunque no se han diseñado específicamente para el sector de la educación y la formación, los seis reglamentos tratados en este informe tienen implicaciones para la enseñanza y el aprendizaje —tanto en contextos formales como fuera de ellos—
—, con efectos variables en los distintos agentes del ámbito educativo.

En general, estas leyes contribuyen a crear un entorno digital más seguro y fiable para las instituciones educativas, así como a una mayor protección de los docentes y los alumnos a título individual, prestando especial atención a los menores.

Algunas de estas normas imponen obligaciones a los proveedores de tecnología que —independientemente de su lugar de establecimiento— ponen a disposición de los usuarios de la UE productos o servicios digitales. Entre ellos se incluyen las soluciones adquiridas por las instituciones educativas al sector de la tecnología educativa (EdTech), pero también los servicios y productos digitales en general que resultan útiles para los alumnos en cualquier contexto educativo y en todos los niveles (por ejemplo, la educación escolar, la formación profesional, la educación de adultos y el aprendizaje permanente).

Como parte del marco normativo digital más amplio de la UE, estos reglamentos contribuyen a un complejo marco regulador un entorno que, según el informe de Draghi (2024), podría limitar la innovación. Con el fin de simplificar el enfoque para la aplicación de la legislación digital de la UE, en noviembre de 2025 la Comisión propuso[3] un «paquete ómnibus digital» compuesto por dos reglamentos distintos que abarcan: 1) normas sobre datos, ciberseguridad y privacidad, y 2) modificaciones específicas de la Ley de IA[4] . La Comisión también está llevando a cabo una «revisión de la adecuación digital» para evaluar la interacción entre las diferentes normas y su impacto acumulativo en las empresas.

Este informe se basa en los textos legislativos originales y en las aportaciones de expertos para ofrecer una visión matizada de las oportunidades y los retos que estos reglamentos plantean a las partes interesadas del ámbito educativo, como los estudiantes, los educadores, los responsables institucionales, los responsables políticos y los proveedores de tecnología.

Tabla 1. Fechas clave

Reglamento	Aprobación	Entrada en vigor	Aplicación
Ley de Servicios Digitales	19 de octubre de 2022	16 de noviembre 2022	17 de febrero de 2024 (general); 25 de abril de 2024 (VLOP/VLOSE)
Ley de Mercados Digitales	14 de septiembre de 2022	1 de noviembre 2022	2 de mayo de 2023 (en general); fechas anteriores para artículos específicos.
Ley de gobernanza de datos	30 de mayo de 2022	23 de junio 2022	24 de septiembre de 2023
Ley de datos	13 de diciembre 2023	11 de enero 2025	11 de enero de 2026
Ley de ciberseguridad	17 de abril 2019	27 de junio 2019	27 de junio de 2019 (general); 28 de junio 2021 (artículos específicos)
Ley de Resiliencia Cibernética	23 de octubre de 2024	10 de diciembre 2024	11 de diciembre de 2027 (general); 11 de septiembre 2026 (notificación); 11 de junio de 2026 (notificaciones)

Fuente: Diario Oficial de la Unión Europea (https://eur-lex.europa.eu/oj/direct-access.html)

[1] Plan de Acción para la Educación Digital (https://education.ec.europa.eu/focus-topics/digital-education/actions).

[2] Unión de competencias: invertir en las personas para una Unión Europea competitiva (https://commission.europa.eu/topics/competitiveness/union-skills_en).

[3] Un «código normativo digital» ágil para la UE (https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook)

[4] La UE acuerda simplificar las normas sobre IA para impulsar la innovación y prohibir las aplicaciones de «nudificación» para proteger a los ciudadanos (https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1024)

Ley de Servicios Digitales (DSA)

La DSA[5] (Reglamento (UE) 2022/2065) tiene por objeto empoderar a los ciudadanos reforzando la protección de sus derechos fundamentales en Internet y otorgándoles un mayor control y más opciones a la hora de utilizar plataformas en línea y motores de búsqueda, haciendo hincapié en la transparencia, la moderación de contenidos y la protección de los menores. La DSA ofrece un marco unificado que proporciona a las empresas seguridad jurídica y la capacidad de expandirse por toda la UE.

Elementos clave de la DSA

- Establece normas armonizadas para los proveedores de servicios de intermediación y sus regímenes de responsabilidad, imponiendo obligaciones por niveles en función del tamaño y el tipo —desde los servicios de intermediación básicos hasta las plataformas en línea—.
- Las VLOP y las VLOSE están sujetas a los requisitos más estrictos, incluida la identificación y mitigación de cuatro categorías de riesgo: 1) contenidos ilícitos; 2) efectos negativos sobre el ejercicio de los derechos fundamentales; 3) efectos negativos sobre el discurso cívico, los procesos electorales y la seguridad pública; y 4) violencia de género, salud pública, protección de menores y bienestar físico y mental.

La DSA se aplica a una amplia gama de servicios de la sociedad de la información, en particular a aquellos clasificados como «proveedores de servicios de intermediación», que suelen operar a cambio de una remuneración, a distancia, por medios electrónicos y a petición del usuario. Este acervo introdujo un marco regulador por niveles con obligaciones básicas para todos los proveedores de servicios de intermediación, con responsabilidades adicionales para los «servicios de alojamiento», las «plataformas en línea» y los «mercados en línea».

Los requisitos más estrictos se reservan para las plataformas en línea de muy gran tamaño (VLOP) y los motores de búsqueda en línea de muy gran tamaño (VLOSE)[6] . Aunque las empresas «pequeñas»[7] y «micro»[8] puedan entrar en el ámbito de aplicación del Reglamento, pueden acogerse a determinadas exenciones de las obligaciones de información y resolución de litigios, con el fin de lograr un equilibrio entre la protección de los usuarios y el fomento de la innovación y la competencia en el mercado de la UE, evitando requisitos reglamentarios desproporcionados que podrían no suponer una carga excesiva para los pequeños proveedores de servicios (DSA, arts. 15, apartado 5, y 21, apartado 7).

Repercusiones de la DSA en el ámbito educativo

Tanto si prestan servicios a instituciones educativas como si se dirigen directamente a educadores y alumnos, los proveedores de tecnología son el principal tipo de parte interesada del ámbito educativo afectada por la DSA en lo que respecta a los requisitos de

La tecnología en la educación en el marco de la DSA

Entre los ejemplos de *servicios de intermediación* relevantes para la educación y la formación se incluyen:

- Servicios de alojamiento diseñados para gestionar la impartición y la administración de programas y cursos educativos, que permiten la interacción y el intercambio de contenidos dentro de grupos definidos. A menudo se denominan «entornos de aprendizaje virtuales» o «sistemas de gestión del aprendizaje» (por ejemplo, Sakai, Moodle, Google Classroom, Microsoft Teams).
- Plataformas en línea que ofrecen cursos a gran escala accesibles para cualquier persona, como los cursos en línea masivos y abiertos (MOOC; por ejemplo, Coursera, Open edEX, Futurelearn).
- Plataformas en línea de gran envergadura utilizadas para buscar y compartir recursos educativos, como tutoriales, vídeos didácticos y contenidos académicos (p. ej., YouTube, Wikipedia).

Todo proveedor de tecnología que actúe como intermediario digital debe cumplir una serie de requisitos básicos, como designar un punto de contacto de acceso público para las autoridades y los denunciantes de confianza (art. 11 de la DSA) o publicar sus condiciones de uso en un lenguaje accesible, incluidas las políticas de moderación de contenidos y cualquier proceso de toma de decisiones algorítmica que se utilice (art. 14 de la DSA). En el caso de los servicios de intermediación dirigidos principalmente a los niños, o utilizados principalmente por ellos, el proveedor debe presentar los términos y condiciones de uso de forma que los niños puedan entenderlos.

Además, los proveedores de tecnología que ofrecen servicios que permiten a los usuarios almacenar y compartir contenidos en línea (por ejemplo, cualquier herramienta de tecnología educativa diseñada para facilitar la comunicación entre educadores y alumnos) deben implementar mecanismos fáciles de usar para recibir

[5] La Ley de Servicios Digitales (https://digital-strategy.ec.europa.eu/en/policies/digital-services-act)

[6] Aquellas que superen una media de 45 millones de destinatarios activos mensuales en la UE.

[7] Menos de 50 empleados y una cifra de negocios anual o un balance total que no supere los 10 millones de euros.

[8] Menos de 10 empleados y una cifra de negocios anual o un total del balance que no supere los 2 millones de euros.

notificaciones de contenidos ilícitos y actuar con celeridad para suprimirlos o inhabilitar el acceso a ellos (art. 16 de la DSA), así como proporcionar una explicación clara de los motivos a los destinatarios afectados cuando se supriman los contenidos o se inhabilite el acceso a ellos, incluyendo los fundamentos de la decisión (art. 17 de la DSA).

Los proveedores de servicios digitales que facilitan el intercambio de contenidos generados por los usuarios con el público en general y que, por lo tanto, se consideran «plataformas en línea» [9], están sujetos a requisitos de cumplimiento adicionales. Por ejemplo, las plataformas que permiten a los alumnos publicar contenidos de forma pública más allá de los límites de una comunidad determinada (por ejemplo, determinados MOOC o repositorios educativos abiertos) deben implementar mecanismos para que los destinatarios puedan presentar reclamaciones sobre las decisiones de la plataforma y responder en un plazo razonable (art. 20 de la DSA); combatir los usos indebidos suspendiendo, durante un período de tiempo razonable y tras una advertencia previa, la prestación de sus servicios a los usuarios que proporcionen con frecuencia contenidos manifiestamente ilegales (art. 23 de la DSA); ofrecer a los usuarios opciones de sistemas de recomendación que no se basen en la elaboración de perfiles e identificar los principales parámetros utilizados (art. 25 de la DSA). Del mismo modo, en virtud de la DSA, todas las plataformas en línea están obligadas a evitar el uso de «patrones oscuros», lo que significa que no pueden diseñar sus interfaces de forma que «engañen, manipulen o, de cualquier otra forma, distorsionen o menoscaben de manera sustancial la capacidad de los destinatarios del servicio para tomar decisiones libres e informadas» (art. 25, apartado 2, de la DSA).

La DSA impone restricciones más estrictas a las plataformas en línea a las que tienen acceso los menores, exigiendo que las interfaces se diseñen teniendo debidamente en cuenta el interés superior del menor (art. 28, apartado 3, de la DSA). Las disposiciones concebidas específicamente para reforzar la protección de los menores son de relevancia directa para el diseño de productos y servicios de tecnología educativa (EdTech). Tal y como se destaca en las *Directrices* de la DSA *sobre medidas para garantizar un alto nivel de privacidad, seguridad y protección de los menores en línea*:

> «Las plataformas en línea pueden proporcionar acceso a una gran variedad de recursos educativos, ayudando a los menores a adquirir nuevas habilidades y ampliar sus conocimientos. Las plataformas en línea también pueden ofrecer a los menores oportunidades para expresar sus opiniones y conectar con otras personas que comparten intereses similares, lo que les ayuda a desarrollar habilidades sociales, confianza y un sentido de comunidad. Al interactuar y explorar el entorno en línea, los menores también pueden fomentar su curiosidad natural, participando en actividades que estimulen la creatividad, la resolución de problemas, el , la autonomía y el entretenimiento». (C/2025/5519, 2025, 2025, p. 1)

En este sentido, la DSA incluye medidas proporcionadas y adecuadas para proteger a los menores de peligros en línea como la captación con fines sexuales, los contenidos nocivos, los comportamientos adictivos, el ciberacoso y las prácticas comerciales perjudiciales. Entre las obligaciones clave de los proveedores de tecnología de plataformas en línea accesibles a menores en la UE se incluyen la implementación de mecanismos precisos y proporcionados de verificación de la edad, así como ajustes de privacidad predeterminados o sistemas de recomendación modificados que reduzcan el riesgo de que los niños se encuentren con contenidos nocivos y se vean atrapados en «agujeros de conejo». Las plataformas en línea deben garantizar que su diseño no engañe, manipule ni induzca a los menores a facilitar datos personales; y deben evitar el uso de cualquier técnica que pueda afectar a la capacidad de toma de decisiones de los menores.

Las exenciones para las microempresas y las pequeñas empresas en virtud de la DSA son relevantes para el sector de la tecnología educativa (EdTech) de la UE, ya que las organizaciones europeas de este sector suelen tener menos de 10 empleados a tiempo completo (61 %) o entre 10 y 40 (28,9 %) (Alianza Europea de EdTech, 2025). Si bien estas exenciones pueden aliviar a los proveedores más pequeños de cargas principalmente administrativas (presentación de informes y resolución de litigios), no reducen las obligaciones sustantivas que rigen el funcionamiento de sus plataformas.

Los docentes, los estudiantes y, en general, las instituciones educativas son los beneficiarios directos de un entorno en línea más seguro en general, resultado de la aplicación de la DSA. Por ejemplo, los requisitos de transparencia de la DSA —incluida la obligación de publicar términos y condiciones claros— facilitan que los usuarios comprendan sus derechos y obligaciones al utilizar plataformas en línea, tanto si dichas plataformas son proporcionadas por sus instituciones como si se accede a ellas a título individual. Del mismo modo, se espera que la DSA reduzca la exposición de los menores a contenidos ilegales y nocivos cuando utilicen plataformas en entornos educativos.

Dado que los intermediarios digitales de gran tamaño suelen desempeñar un papel central en el entorno digital de educadores y alumnos —incluidos tanto los VLOP (por ejemplo, YouTube, Facebook, las tiendas de Amazon) como los VLOSE (por ejemplo, Google Search, Bing)—, pueden beneficiarse directamente del nivel más estricto de obligaciones previsto en la DSA. En particular, de la evaluación del riesgo sistémico (art. 34 de la DSA), que exige a los servicios designados que

[9] A menos que dicha actividad sea una característica menor y puramente accesoria de otro servicio (por ejemplo, los comentarios de los usuarios en un periódico en línea).

evaluar los perjuicios causados a los menores como elemento obligatorio, así como la prohibición de la publicidad basada en perfiles dirigida a menores (art. 28, apartado 4, de la DSA).

Cabe señalar que, si bien ningún servicio de tecnología educativa ha sido designado como VLOP o VLOSE, los grandes actores del sector —como Google Classroom, Microsoft Teams for Education o Duolingo— podrían llegar a alcanzar, con el tiempo, el número de usuarios activos en la UE que da lugar a dicha designación. Además, quedan incluidos los VLOP y VLOSE utilizados en entornos educativos (por ejemplo, Wikipedia, YouTube o la búsqueda de Google).

También es importante tener en cuenta que las instituciones educativas pueden estar sujetas a obligaciones de cumplimiento cuando actúan ellas mismas como prestadores de servicios de intermediación. Esto es especialmente relevante para las instituciones de educación superior, ya que las universidades suelen gestionar servicios de intermediación internos, como los entornos de aprendizaje virtuales, que pueden considerarse servicios de alojamiento. Los intermediarios que ponen a disposición del público contenidos generados por los usuarios —por ejemplo, servicios digitales autohospedados para la impartición de MOOC en los que cualquiera puede publicar y acceder a contenidos— se considerarían plataformas en línea, lo que conllevaría obligaciones adicionales. Es menos probable que los centros de educación primaria y secundaria, así como las instituciones de formación profesional, tengan que hacer frente a obligaciones de cumplimiento de la DSA, ya que suelen recurrir a proveedores externos de tecnología educativa (EdTech) o a las autoridades públicas, en lugar de gestionar plataformas propias.
interno.

Los organismos públicos que gestionan plataformas digitales al servicio de centros educativos —como un entorno de aprendizaje virtual de titularidad pública accesible a los centros escolares de una región determinada— también pueden considerarse proveedores de servicios de intermediación en virtud de la DSA y, por lo tanto, estarían sujetos a las obligaciones correspondientes.

Ley de Mercados Digitales (DMA)

La DMA[10] (Reglamento (UE) 2022/1925) tiene por objeto hacer que los mercados del sector digital sean más justos y competitivos.

La DMA se aplica a los «guardianes» que prestan servicios básicos de plataforma a empresas y usuarios de la UE, independientemente de su lugar de establecimiento, y que tienen un impacto significativo en el mercado y una posición consolidada (artículos 3 y 13 de la DMA). Estas empresas controlan infraestructuras y funciones críticas, como los motores de búsqueda, las tiendas de aplicaciones, los sistemas operativos y la computación en la nube. Los servicios básicos de plataforma incluyen las redes sociales (p. ej., Instagram, LinkedIn), las plataformas para compartir vídeos (p. ej., TikTok, YouTube), los sistemas operativos (p. ej., iOS, Windows) o las aplicaciones de mensajería (p. ej., WhatsApp) (art. 2 de la DMA). En total, actualmente están designados 23 servicios de plataforma fundamentales, prestados por siete «guardianes» (Alphabet, Amazon, Apple, Booking, ByteDance, Meta y Microsoft).

Elementos clave de la DMA

- Designa a los «guardianes» en función de umbrales cuantitativos (7 500 millones de euros de volumen de negocio en la UE o 75 000 millones de euros de capitalización bursátil, además de ≥45 millones de usuarios finales mensuales y ≥10 000 usuarios empresariales anuales).
- Impone a los «guardianes» una serie de obligaciones y prohibiciones: entre las obligaciones se incluyen garantizar la interoperabilidad, facilitar el acceso a los datos a anunciantes y editores, y evitar el favorecimiento propio; entre las prohibiciones se incluyen la combinación de datos entre servicios o el uso de datos de empresas terceras competidoras.

La DMA exige a los «gatekeepers» que abran sus plataformas a otros desarrolladores, garantizando *la interoperabilidad* con desarrolladores externos, fomentando la competencia y la libertad de elección de los usuarios. Esto también podría contribuir al desarrollo de una gama más amplia de herramientas y servicios educativos.

Además, la DMA permite *la portabilidad de datos*, al exigir a los «guardianes» que permitan a las empresas y a los usuarios de sus servicios transferir sus datos a diferentes plataformas. Esto debería facilitar una integración fluida, reforzar el control de los usuarios sobre sus datos y mejorar la experiencia general del usuario.

Repercusiones de la DMA en el ámbito educativo

El sector de la tecnología educativa (EdTech) podría beneficiarse de una serie de nuevas oportunidades y derechos para las empresas de la UE en virtud de la DMA, lo que permitiría a las empresas emergentes y a las pequeñas empresas introducir en el mercado herramientas educativas innovadoras. Por ejemplo, los proveedores de tecnología pueden distribuir sus aplicaciones educativas a través de tiendas de aplicaciones alternativas, instalarlas directamente en todos los sistemas operativos designados (iOS, dispositivos móviles Android, PC con Windows) y comunicarse directa y libremente con sus clientes.

[10] La Ley de Mercados Digitales (https://digital-markets-act.ec.europa.eu)

La tecnología en la educación en el marco de la DMA

Ejemplos de servicios de plataformas fundamentales que tienen obligaciones en virtud de la DMA y que son relevantes para la educación:

- Sistemas operativos (p. ej., Google Android, iOS, Windows PC)
- Navegadores web (Chrome, Safari)
- Redes sociales (por ejemplo, TikTok, Instagram, LinkedIn)
- Compartir vídeos (YouTube)
- Búsquedas en línea (Búsqueda de Google)

Además, pueden beneficiarse de los requisitos que la DMA impone a los «guardianes» para que permitan la interoperabilidad de forma gratuita, así como de la prohibición de que las plataformas designadas promocionen de forma desleal sus productos y servicios por encima de otras alternativas a través de los resultados de búsqueda o los anuncios. La DMA también permite a los proveedores de tecnología educativa (EdTech) acceder a los datos generados por sus servicios y las interacciones de los usuarios (por ejemplo, métricas de rendimiento, comportamiento de los usuarios) en las plataformas de los «guardianes».

Sin embargo, al igual que ocurre con la DSA, existen herramientas educativas de uso generalizado que no han sido designadas como servicios básicos de la plataforma y que, por lo tanto, no están sujetas actualmente a las obligaciones de la DMA. Entre ellas se incluyen Google Classroom y Microsoft Teams, que se comercializan como herramientas educativas que permiten organizar clases, comunicarse y colaborar. Del mismo modo, los servicios de videoconferencia (por ejemplo, Google Meet), que pueden utilizarse para aulas virtuales, y los servicios de computación en la nube (por ejemplo, Google Workspace y Microsoft 365), que se utilizan ampliamente en entornos educativos, tampoco están designados actualmente.

Como usuarios de los servicios básicos de las plataformas, los estudiantes y los docentes pueden beneficiarse de una mayor variedad de opciones y flexibilidad a la hora de interactuar con el entorno digital. Por ejemplo, la DMA otorga a los usuarios el derecho a transferir sus datos de una plataforma a otra, al tiempo que les permite evitar que se les realice un seguimiento y se elaboren perfiles con fines publicitarios. Además, la DMA introduce medidas mejoradas de protección de datos que complementan el RGPD, garantizando la protección de la información personal de los estudiantes, especialmente en los casos en que se trate de datos de menores.

Los responsables de las políticas educativas interesados en promover la soberanía digital en la educación podrían encontrar en la DMA un instrumento valioso, ya que está llamada a limitar la dependencia de los «guardianes» dominantes al fomentar la competencia y facilitar el cambio entre plataformas.

Ley de Ciberseguridad (CSA)

La CSA[11] (Reglamento (UE) 2019/881) tiene por objeto reforzar la ciberseguridad en toda la UE mediante un mandato reforzado y una ampliación de los recursos destinados a la Agencia de la Unión Europea para la Ciberseguridad[12] (ENISA) y al Marco Europeo de Certificación de Ciberseguridad[13] (ECCF).

Elementos clave de la CSA

- Otorga a la ENISA un mandato permanente para aumentar la cooperación operativa a nivel de la UE, ayudando a los Estados miembros de la UE a gestionar sus incidentes de ciberseguridad y apoyando la coordinación de la UE en caso de ciberataques y crisis transfronterizas a gran escala y crisis transfronterizas a gran escala
- Establece un marco europeo de certificación en materia de ciberseguridad que permite la creación de sistemas de certificación armonizados a escala de la UE para productos, servicios y procesos de TIC. Establece tres niveles de garantía —básico, sustancial y alto—, cada uno de los cuales refleja el uso previsto y el perfil de riesgo del producto o servicio de TIC.

La CSA encomendó a la ENISA la tarea de prestar apoyo a los Estados miembros, las instituciones de la UE y las empresas en ámbitos clave como la aplicación de la Directiva sobre redes y sistemas de información (NIS), la Ley de ciberresiliencia y la Ley de cibersolidaridad. Asimismo, se encomendó a la Agencia la tarea de apoyar el proceso de certificación de la ciberseguridad de los productos, servicios y procesos digitales.

La certificación en el marco del ECCF es voluntaria y no impone obligaciones a los proveedores de tecnología que decidan no solicitarla. Se aplica a productos y servicios específicos, más que a las entidades jurídicas que los fabrican o prestan, y abarca una amplia gama de ámbitos, desde la computación en la nube hasta los dispositivos inteligentes.

[11] Ley de Ciberseguridad de la UE | Forjando el futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act)

[12] https://www.enisa.europa.eu/

[13] Ley de Ciberseguridad de la UE (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act)

En 2026, la Comisión propuso un nuevo paquete de medidas sobre ciberseguridad[14] para reforzar aún más la resiliencia y las capacidades de la UE en materia de ciberseguridad, que incluye modificaciones a la Directiva NIS2[15] y la propuesta de revisión de la CSA[16] . El paquete tiene por objeto simplificar el cumplimiento de las normas de ciberseguridad de la UE y los requisitos de gestión de riesgos para las empresas que operan en la UE, al tiempo que reduce los riesgos en la cadena de suministro de las TIC de la UE derivados de proveedores de terceros países que plantean problemas de ciberseguridad.

Repercusiones de la CSA en el ámbito educativo

Los proveedores de tecnología que operan en la UE pueden beneficiarse de la posibilidad de obtener certificados reconocidos en toda la UE en el marco del ECCF. Podrían obtener una ventaja competitiva en el mercado al contar con la certificación de sus productos, servicios y procesos.

La tecnología en la educación en el marco del CSA

Los sistemas de certificación implementados en el marco del ECCF pueden centrarse en certificar la ciberseguridad de una gama más amplia de productos y servicios de TIC relevantes para la educación y la formación, entre los que se incluyen:

- Cortafuegos (tanto de hardware como de software)
- Sistemas operativos (incluidos los de dispositivos móviles)
- Enrutadores
- Servicios de seguridad gestionados, como la respuesta ante incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría

Los responsables educativos podrían mejorar la ciberseguridad en sus instituciones mediante la implantación de productos y servicios digitales certificados, mientras que los responsables de las políticas de educación y formación podrían mejorar la ciberseguridad a nivel sectorial fomentando la adquisición de dichos productos y servicios.

En general, para los estudiantes, los educadores y las instituciones educativas, los sistemas de certificación puestos a disposición en el marco del ECCF pueden ofrecer un mayor nivel de seguridad y confianza en las complejas cadenas de suministro de las TIC.

Ley de Resiliencia Cibernética (CRA)

La CRA[17] (Reglamento (UE) 2024/2847) establece requisitos de ciberseguridad para todos *los productos con elementos digitales* (PDE) disponibles en el mercado de la UE.

Elementos clave de la CRA

- Establece requisitos horizontales de ciberseguridad para los PDE comercializados en el mercado de la UE, que abarcan el hardware y el software a lo largo de todo el ciclo de vida del producto (diseño, desarrollo, producción, mantenimiento y fin de vida útil).
- Exige a los fabricantes que apliquen los principios de «seguridad desde el diseño», gestionen las vulnerabilidades durante todo el periodo de soporte, realicen pruebas de seguridad y proporcionen actualizaciones de seguridad.
- Los productos llevarán el marcado CE para indicar que cumplen los requisitos de la CRA.

Los PDE se definen como un producto de software o hardware y sus soluciones de tratamiento de datos a distancia, incluidos los componentes que se comercializan por separado. Esta definición abarca una amplia gama de productos, entre los que se incluyen los dispositivos conectados al Internet de las cosas (IoT) (por ejemplo, las pizarras interactivas) y los productos que desempeñan funciones clave de seguridad (por ejemplo, los gestores de contraseñas).

La CRA promueve un enfoque de «seguridad desde el diseño», que exige a los fabricantes de PDE que garanticen que, al comercializar sus productos, se hayan cumplido los requisitos esenciales de ciberseguridad (artículos 13 y 32 de la CRA), así como que se subsanen las vulnerabilidades durante el período de soporte del producto.

Los fabricantes deben llevar a cabo una evaluación de los riesgos de ciberseguridad asociados a sus productos, con el objetivo de minimizar dichos riesgos y prevenir incidentes. Se debe seguir un procedimiento más estricto de «evaluación de la conformidad» en el caso de productos importantes y críticos, en los que un PDE desempeñe una función que conlleve un riesgo significativo de efectos adversos en cuanto a su intensidad y capacidad para perjudicar la salud, la seguridad o la protección de

[14] La Comisión refuerza la resiliencia y las capacidades de la UE en materia de ciberseguridad | Dando forma al futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/news/commission-strengthens-eu-cybersecurity-resilience-and-capabilities)

[15] Propuesta de Directiva relativa a medidas de simplificación y adaptación a la Ley de Ciberseguridad | Configurando el futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act)

[16] Propuesta de Reglamento para la Ley de Ciberseguridad de la UE | Configurando el futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act)

[17] Ley de ciberresiliencia | Forjando el futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act)

usuarios de dichos productos (por ejemplo, cerraduras inteligentes, sistemas de vigilancia para bebés, sistemas de alarma, juguetes conectados y tecnología sanitaria portátil).

Repercusiones de la CRA en el ámbito educativo

Al exigir el cifrado, las actualizaciones periódicas de software y la gestión de vulnerabilidades, la CRA pretende dar forma a un panorama educativo y formativo en el que la dependencia de los PDE para el aprendizaje y la evaluación está creciendo rápidamente, y en el que los datos personales de los alumnos se tratan, almacenan y transmiten de forma habitual en estos sistemas.

Las obligaciones de la CRA se aplican principalmente a los fabricantes y otros operadores económicos de la cadena de suministro. En el contexto de la tecnología educativa (EdTech), los proveedores de tecnología deben garantizar que sus PDE sean resistentes a las amenazas cibernéticas y capaces de proteger tanto los datos de los alumnos como los recursos educativos frente a actores malintencionados.

Las instituciones educativas que adquieren dispositivos conectados se ven directamente afectadas por la mejora de la seguridad, el soporte de parches más prolongado y las cadenas de notificación de vulnerabilidades que introduce la CRA. Como resultado, los alumnos y los docentes pueden beneficiarse de una menor exposición a las amenazas de ciberseguridad y a las vulnerabilidades al utilizar PDE, como sistemas operativos, navegadores y redes privadas virtuales (VPN).

La tecnología en la educación en el marco de la CRA

Las PDE cobran cada vez más relevancia en el ámbito de la educación y la formación, por ejemplo, en aplicaciones móviles, altavoces inteligentes, videojuegos, navegadores, gestores de contraseñas, sistemas operativos, software antivirus, dispositivos del Internet de las cosas (IoT) como la robótica, pizarras interactivas y dispositivos wearables personales, etc.

Ley de Gobernanza de Datos (DGA)

La DGA[18] (Reglamento (UE) 2022/868) introdujo un marco para fomentar la confianza en el intercambio de datos, reforzar los mecanismos destinados a aumentar la disponibilidad de los datos y superar los obstáculos técnicos para la reutilización de los datos, en beneficio de las empresas y los ciudadanos.

Elementos clave de la DGA

- Establece normas que facilitan la reutilización de determinadas categorías de datos protegidos en poder de organismos del sector público, incluidos los datos comerciales confidenciales, los datos de carácter personal o los datos sensibles a nivel nacional.
- Crea un marco para los servicios de intermediación de datos, estableciendo normas para los intermediarios neutrales que faciliten el intercambio de datos entre empresas, los interesados y las autoridades públicas.
- Introduce un marco de altruismo de datos que permite a las organizaciones facilitar que los interesados pongan voluntariamente sus datos a disposición del bien común (por ejemplo, investigación sanitaria, vigilancia medioambiental), siempre que se les reconozca la condición de «organización de altruismo de datos».

El sector público dispone de un volumen considerable de datos que no pueden ponerse a disposición como datos abiertos, como los datos personales y los datos comercialmente sensibles, ya que contienen información sensible sobre personas o información comercial confidencial. De dichos datos se puede obtener un valor significativo sin menoscabar su carácter protegido. La DGA establece normas y garantías para permitir dicha reutilización, en consonancia con el resto de la legislación aplicable.

Además, la DGA tiene por objeto aumentar el intercambio de datos de confianza entre sectores mediante la regulación de los nuevos «intermediarios de datos» y el establecimiento de un marco para promover el intercambio de datos con fines altruistas[19] . Abarca tanto los datos personales como los no personales, y en los casos en que intervengan datos personales, sigue siendo de aplicación el RGPD.

Implicaciones de la DGA en el ámbito educativo

El marco de la DGA para la reutilización de datos protegidos del sector público se aplica de forma paralela y sin perjuicio de la Directiva sobre datos abiertos (Directiva (UE) 2019/1024, de 2019), que es el instrumento principal que regula la reutilización de datos por parte de las instituciones culturales y educativas. Si bien las instituciones culturales, como bibliotecas, archivos y museos, están sujetas principalmente a la Directiva sobre datos abiertos, la DGA puede seguir siendo relevante para las entidades educativas y culturales

[18] Ley Europea de Gobernanza de Datos (https://digital-strategy.ec.europa.eu/en/policies/data-governance-act)

[19] Explicación de la Ley de Gobernanza de los Datos | Dando forma al futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained)

a través de sus disposiciones sobre el altruismo de datos (Título IV) y los servicios de intermediación de datos (Título III).

La tecnología en la educación en el marco de la DGA

Los datos de análisis del aprendizaje que se pongan a disposición de forma voluntaria con fines de interés general —incluida la investigación educativa, la evaluación de políticas o la mejora de la enseñanza y el aprendizaje— podrían hacerse accesibles a través del marco de altruismo de datos de la DGA.

Los servicios de intermediación de datos en el marco de la DGA pueden ayudar a los agentes del ámbito educativo a compartir y utilizar los datos de análisis del aprendizaje de forma más eficaz.

La reutilización de determinadas categorías de datos protegidos que obran en poder de los organismos del sector público, en virtud de la DGA, no se aplica ni a las instituciones educativas ni a las entidades culturales, como bibliotecas, archivos y museos.

Como reutilizadores de datos, las instituciones educativas —junto con las pymes, las empresas emergentes y la sociedad civil— pueden acceder a los datos protegidos que obran en poder de los organismos del sector público a un precio reducido o de forma gratuita (art. 6, apartado 4, de la DGA). En este sentido, el personal docente y el alumnado pueden beneficiarse de la reutilización de datos protegidos de titularidad pública como recursos educativos, puestos a su disposición a través de los mecanismos establecidos en virtud de la DGA, sobre una amplia variedad de temas (por ejemplo, salud, movilidad, industria manufacturera, servicios financieros, energía y agricultura).

Las organizaciones que operan como proveedores de servicios de intermediación de datos (por ejemplo, las cooperativas de datos) pueden poner en contacto a los titulares de datos con los usuarios de datos dentro del sector de la educación y la formación. Por ejemplo, podría crearse un fideicomiso de datos para agrupar los derechos que tienen los estudiantes y los padres sobre los datos personales en una plataforma educativa que realiza un seguimiento del progreso en el aprendizaje y registra las calificaciones de los exámenes (Consejo de IA del Reino Unido et al., 2021). Dicho fideicomiso de datos podría permitir a los miembros obtener un mayor valor de los datos al tiempo que ejercen sus derechos de portabilidad y acceso a los datos, reduciendo al mismo tiempo los riesgos que conlleva el intercambio de datos (Centro Común de Investigación, 2023).

Los responsables de las políticas educativas de los Estados miembros podrían adoptar medidas técnicas u organizativas para apoyar el «altruismo de datos» mediante el desarrollo de políticas nacionales que ayuden a los interesados a poner voluntariamente a disposición del interés general sus datos personales en poder de organismos del sector público (art. 16 de la DGA).

Ley de Datos

La Ley de Datos[20] (Reglamento (UE) 2023/2854, 2023) aprovecha el potencial de innovación y competitividad asociado al creciente volumen de datos del Internet de las cosas (IoT) disponibles para su reutilización en la UE, que se deriva de la creciente disponibilidad de productos conectados a Internet («productos conectados»)[21] en el mercado europeo[22] .

Elementos clave de la Ley de Datos

- Garantiza el acceso y el uso equitativos de los datos generados por los productos conectados al Internet de las cosas (IoT), abarcando las relaciones entre empresas (B2B) y permitiendo a los usuarios acceder a los datos y compartirlos con terceros.
- Otorga a los usuarios (tanto consumidores como empresas) el derecho a acceder a los datos generados por su uso de productos conectados y a que dichos datos se transmitan a un tercero de su elección.
- Incluye disposiciones sobre el cambio de proveedor de servicios en la nube para reducir los riesgos de bloqueo, exigiendo condiciones contractuales justas, garantías técnicas y herramientas de portabilidad para los usuarios que cambien de proveedor de servicios en la nube.

Asimismo, la Ley de Datos contiene disposiciones sobre el cambio de proveedor de servicios en la nube que establecen la prohibición contractual de las cláusulas de bloqueo, los requisitos técnicos para la portabilidad de los datos y de las aplicaciones, y las garantías de nivel de servicio durante la transición.

Otorga a las empresas o particulares que posean, arrienden o alquilen productos conectados un mayor control sobre los datos que generan, al tiempo que mantiene los incentivos para quienes invierten en tecnologías de datos. Establece condiciones generales para las situaciones en las que una empresa tiene la obligación legal de compartir datos con otra empresa (B2B).

Introduce cambios significativos en la forma en que se accede a los datos, se comparten y se gestionan en diversos sectores, incluida la educación. Sus objetivos principales

[20] Ley de datos | Forjando el futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/policies/data-act)

[21] Se define «producto conectado» como «un artículo que obtiene, genera o recopila datos relativos a su uso o a su entorno y que es capaz de comunicar datos del producto a través de un servicio de comunicaciones electrónicas, conexión física o acceso en el propio dispositivo, y cuya función principal no sea el almacenamiento, el tratamiento o la transmisión de datos por cuenta de ninguna otra parte que no sea el usuario».

[22] Explicación de la Ley de Datos | Configurando el futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained)

son promover el uso justo de los datos, evitar desequilibrios en el mercado y fomentar la innovación.

Las revisiones del marco normativo digital de la UE propuestas como parte del «Omnibus digital» incluyen la integración de las disposiciones de la DGA, la Directiva sobre datos abiertos y el Reglamento sobre la libre circulación de datos no personales en una única Ley de Datos [23]reestructurada.

Repercusiones de la Ley de Datos en el ámbito educativo

Para el sector de la tecnología educativa (EdTech), la Ley de Datos implica que los proveedores de tecnología (es decir, los fabricantes de productos conectados, los proveedores de servicios vinculados a dichos productos y las empresas que tratan los datos generados por dichos productos) deben cumplir los requisitos de acceso a los datos. La Ley de Datos también exige a los proveedores de servicios en la nube que actúen de buena fe y faciliten información clara a lo largo de todo el proceso de cambio de proveedor (Ley de Datos, arts. 26-27), lo que refuerza la aplicabilidad práctica de los derechos de cambio de proveedor para las instituciones educativas.

La tecnología en la educación en el marco de la Ley de Datos

Los productos conectados y el Internet de las cosas (IoT) se han ido introduciendo progresivamente en el sector de la educación y la formación, por ejemplo, en forma de pizarras conectadas, tabletas, drones o computación en la nube. En virtud de la Ley de Datos, los datos generados por dichos productos deben ponerse a disposición de sus usuarios cuando estos lo soliciten.

Los servicios en la nube utilizados por los centros educativos —como los sistemas de gestión del aprendizaje alojados en infraestructuras en la nube, las plataformas de análisis de datos o los sistemas administrativos— entran dentro del ámbito de aplicación de la Ley de Datos, lo que otorga a los clientes el derecho a cambiar de proveedor de servicios en la nube e impone a los proveedores la obligación de facilitar dicho cambio de forma efectiva.

La Ley de Datos permite a las instituciones educativas beneficiarse del acceso a datos relevantes y de una mayor flexibilidad a la hora de seleccionar herramientas digitales más allá de las ofertas de los fabricantes, con la posibilidad de cambiar de proveedor de servicios más fácilmente y reducir el riesgo de quedar atrapadas en soluciones propietarias.

Además, las autoridades competentes de los Estados miembros deberían apoyar el desarrollo de la alfabetización en materia de datos y la sensibilización (sobre derechos y obligaciones) entre los usuarios y las entidades incluidas en el ámbito de aplicación de este reglamento, como los usuarios de productos conectados, las empresas que gestionan dispositivos del Internet de las cosas y los proveedores de servicios en la nube. Los responsables de las políticas educativas podrían desempeñar un papel importante al integrar la alfabetización en materia de datos —incluido el funcionamiento de la Ley de Datos— en los planes de estudios de las diferentes áreas del sector de la educación y la formación.

Análisis de las consideraciones políticas

Los seis reglamentos de la UE analizados en este informe configuran, de diferentes maneras y en diversos grados, la transformación digital de la educación y la formación. Estas normas contribuyen a crear un entorno digital globalmente más seguro y fiable para los educadores y los alumnos, especialmente los menores (gracias a las disposiciones específicas de la Ley de Datos).

Como adquirentes y usuarios de productos y servicios digitales, las instituciones educativas pueden beneficiarse de: servicios de alojamiento más seguros (DSA); una mayor interoperabilidad, portabilidad de datos y competencia en el mercado digital (DMA); la posibilidad de adquirir productos y servicios con certificación de ciberseguridad de proveedores de toda la UE (CSA); la obligación de los fabricantes de subsanar las vulnerabilidades a lo largo de todo el ciclo de vida de un producto y de notificar los incidentes significativos (CRA); el potencial de los proveedores de servicios de intermediación de datos y de los acuerdos de altruismo para sacar el máximo partido a los datos de análisis del aprendizaje (DGA); el derecho a cambiar de proveedor y a transferir datos, junto con unos derechos de acceso a los datos mejorados (Ley de Datos).

Las seis normativas se dirigen principalmente a los proveedores de tecnología y a los «guardianes», no a las instituciones educativas como tales. Por lo tanto, la carga que supone el cumplimiento directo para las instituciones educativas es relativamente limitada. No obstante, podrían enfrentarse a posibles obligaciones directas en virtud de la DSA si operan como proveedores de servicios de intermediación. Por ejemplo, una institución educativa que gestione una plataforma accesible al público en general (por ejemplo, los MOOC) podría considerarse un proveedor de plataformas en línea y estar sujeta a las obligaciones correspondientes, entre las que se incluyen las obligaciones de moderación de contenidos, los mecanismos de gestión de reclamaciones y los requisitos de transparencia en la presentación de informes. Las normativas tratadas en este informe añaden un nivel de complejidad a la gestión de las instituciones educativas que requiere atención en

[23] Un «código de normas digitales» ágil para la UE | Configurando el futuro digital de Europa (https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook)

en el contexto tanto de la formación inicial como de la formación continua del profesorado.

El sector de las tecnologías educativas (EdTech) de la UE podría beneficiarse de un sector digital más justo y competitivo, basado principalmente en las obligaciones que la DMA establece para los «guardianes». Al mismo tiempo, las obligaciones de cumplimiento acumulativas que se derivan de estas leyes pueden suponer un obstáculo para los proveedores de tecnología, ya que deben adaptar sus estrategias de cumplimiento a diferentes plazos y a un panorama normativo fragmentado.

Dado que el cumplimiento normativo requiere no solo una inversión inicial en sistemas y formación, sino también costes continuos de supervisión, presentación de informes y adaptación a medida que evoluciona el panorama normativo, las empresas más pequeñas del sector de la tecnología educativa podrían verse especialmente afectadas por las implicaciones financieras. La DSA ya incluye excepciones para evitar requisitos normativos desproporcionados que podrían suponer una carga excesiva para los proveedores de tecnología más pequeños, mientras que se espera que el «Digital Omnibus» simplifique el cumplimiento de las normas de ciberseguridad y la fusión de las normativas sobre datos.

Metodología

Este informe se basa en el trabajo analítico de un grupo interdisciplinar de expertos —entre los que se incluyen especialistas en estudios educativos, derecho, informática y sociología—, complementado con las aportaciones de más de 50 partes interesadas que participaron en dos talleres en línea del CCI y en una investigación documental. Para garantizar que el análisis fuera más allá de lo abstracto, se proporcionó a los expertos una lista estructurada de procesos y situaciones educativas concretas que podrían verse afectadas por esta legislación, lo que les ayudó a fundamentar sus reflexiones en contextos tangibles del mundo real.

Referencias

Comunicación de la Comisión: Directrices sobre medidas para garantizar un alto nivel de privacidad y seguridad para los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065, (2025), DO L, http://data.europa.eu/eli/C/2025/5519/oj.

Draghi, M. (colaborador) (2024), «El futuro de la competitividad europea: una estrategia de competitividad para Europa», El futuro de la competitividad europea, Oficina de Publicaciones de la Unión Europea, Luxemburgo, https://doi.org/10.2872/1823372.

Alianza Europea de Tecnología Educativa (2025), «La soberanía digital de Europa tiene un punto ciego en materia de educación», European Edtech News, boletín de Substack, 10 de noviembre, consultado el 5 de febrero de 2026, https://europeanedtechnews.substack.com/p/europes-digital-sovereignty-has-an.

Centro Común de Investigación (2023), *«Mapping the landscape of data intermediaries: emerging models for more inclusive data governance»*, Oficina de Publicaciones, LU, https://doi.org/10.2760/261724.

Consejo de IA del Reino Unido e Instituto Ada Lovelace (2021), «Exploring Legal Mechanisms for Data Stewardship», Data for the Public Good, https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Legal-mechanisms-for-data-stewardship_report_Ada_AI-Council-2.pdf.

Agradecimientos

La investigación presentada en este informe ha sido financiada por la Comisión Europea: Dirección General de Educación, Juventud, Deporte y Cultura (DG EAC), en el marco del acuerdo administrativo «Learning for Life in the Digital Age 6» (n.º JRC 37077 NFP / EAC-2025-0600). Se consultó a varias direcciones generales de la Comisión, que aportaron valiosas contribuciones: la DG EAC (Unidad B2), la DG CNECT (Unidades D1, D2, F3, G1, G2, H1) y el CCI (Unidades S4, T1, T3, T4).

Las opiniones expresadas son exclusivamente de los autores y no deben considerarse representativas de la posición oficial de la Comisión.

Autores: Villar Onrubia, D., Brown, I., Colonna, L., Cronin, C., De Martin, J.C., Fernández Enguita, M., Hacker, P., Holmes, W., Kralj, L., Wasson, B.

Editores: Cachia, R., López Cobo, M.

Cómo citar este informe: Villar Onrubia, D., Brown, I., Colonna, L., Cronin, C., De Martin, J.C. et al., *«Implicaciones de la legislación digital de la UE para la educación y la formación: análisis de la Ley de Servicios Digitales, la Ley de Mercados Digitales, la Ley de Ciberseguridad, la Ley de Ciberresiliencia, la Ley de Gobernanza de Datos y la Ley de Datos»*, Cachia, R. y López Cobo, M. (eds.), Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2026, https://data.europa.eu/doi/10.2760/1836591, JRC147584

Datos de contacto

Comisión Europea, Centro Común de Investigación (CCI) Persona de contacto: Daniel Villar-Onrubia
Correo electrónico: daniel.villar-onrubia@ec.europa.eu

La ciencia al servicio de las políticas

Escanea el código QR para visitar:

Centro Común de Investigación
https://joint-research-centre.ec.europa.eu

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2026

© Unión Europea, 2026
Se permite la reutilización de este documento, siempre que se cite la fuente adecuada y se indiquen los cambios realizados (licencia Creative Commons Attribution 4.0 International). Para cualquier uso o reproducción de elementos que no sean propiedad de la UE, puede ser necesario solicitar permiso directamente a los respectivos titulares de los derechos. Todas las imágenes © Unión Europea, salvo que se indique lo contrario

JRC147584
PDF ISBN 978-92-68-41285-5 doi:10.2760/1836591 KJ-01-26-290-EN-N