InDret
4.2026

Editorial

La Propuesta de EU KIDS ACT. Entre la autonomía digital de los menores y la seguridad de los servicios

-

El pasado 17 de septiembre la Comisión presentó una nueva propuesta de Reglamento europeo titulado *«EU KIDS ACT»* (COM(2026) 681 final). A pesar de lo que su nombre podría sugerir, la propuesta no ofrece un régimen de protección integral de los menores de edad en la Unión, sino un conjunto de medidas para la regulación del acceso y el uso por estos de servicios de redes sociales y otras tecnologías digitales. El nombre de la propuesta es, en realidad, el acrónimo de *«EU Keeping Internet Digital Spaces Accountable and Trustworthy»*. Se suma, así, la Comisión a cierta tendencia en otros ordenamientos de recurrir a acrónimos llamativos que esconden nombres muchas veces forzados, como la USA PATRIOT Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*) o la USA FREEDOM Act (*Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act*).

Planteada como uno de los compromisos personales de la Presidenta von der Leyen, la Propuesta de Reglamento por el que se establecen las condiciones para unos entornos digitales en internet fiables y responsables para los menores incluye esencialmente normas sobre la utilización por menores de redes sociales y otras tecnologías digitales, normas sobre diseño y seguridad de estas, y normas sobre gobernanza. La propuesta aparece en medio de cierto pánico moral sobre los riesgos y efectos perniciosos de las redes sociales y en medio de la ola de litigación, especialmente en EE.UU, contra sus operadores. Antes de la intervención europea, muchos ordenamientos ya habían presentado otras propuestas de limitación del acceso de menores a redes sociales y ahora el legislador europeo, así lo señala, persigue ofrecer unos estándares armonizados y un nivel de protección más homogéneo en la Unión (Considerando 3). Por ejemplo, en España, se presentó el año pasado el Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales (BOCG Nº 52-1, de 11.4.2025), que entre otras medidas, preveía la modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDYGDD) para elevar la edad para prestar el consentimiento a tratamientos de datos personales a los 16 años (DF 6ª). La modificación que se establecía afectaría de modo transversal al consentimiento para cualquier tratamiento de datos personales y no únicamente en entornos digitales o, específicamente, en redes sociales. Por otra parte, el Presi-

dente del Gobierno Pedro Sánchez anunció el pasado mes de febrero que impulsaría la prohibición de acceso a las redes sociales a menores de 16 años, pero todavía no se ha presentado ningún anteproyecto en este sentido, ni se lo espera después del avance electoral y, sobre todo, después de la publicación de la Propuesta de Reglamento EU KIDS ACT, que aquí comentamos.

No es el objetivo de este editorial ofrecer un examen de todas las medidas incluidas en la Propuesta. Me interesa únicamente apuntar algunas ideas sobre el impacto en el ámbito del derecho privado y, sobre todo, a partir de la combinación de medidas orientadas a la regulación de la autonomía personal de los menores de edad con otras orientadas a la seguridad desde el diseño de las tecnologías digitales.

Con arreglo a su artículo 1, la Propuesta de Reglamento EU KIDS ACT tiene por objeto establecer: a) una edad mínima armonizada para crear una cuenta en servicios de redes sociales en línea y servicios de plataformas de intercambio de vídeos; b) requisitos de seguridad armonizados para servicios de redes sociales en línea, servicios de plataformas de intercambio de vídeos, plataformas de videojuegos y tiendas de aplicaciones informáticas, y requisitos de seguridad armonizados para proteger a los menores en línea para los videojuegos, los compañeros de IA y los chatbots de propósito general; y c) normas armonizadas relativas a la garantía de la edad en línea.

Estas medidas se justifican con base en dos argumentos principales: (a) la falta de madurez suficiente de los menores o algunos de ellos para comprender las consecuencias derivadas del uso de las tecnologías digitales y, en particular, para advertir el impacto que pueden llegar a tener sobre su esfera personal y patrimonial (véase Considerando 38, por ejemplo); y (b) la mayor vulnerabilidad de los menores frente a los riesgos asociados con el uso de las tecnologías digitales (véanse, entre otros, Considerandos 1, 20 y 30).

En relación con el primer argumento, se ha destacado de ordinario que muchos menores no pueden comprender suficientemente las consecuencias de exponer aspectos de su vida privada, de mostrar determinadas imágenes personales, o de consentir a que sus datos personales sean tratados por un prestador de servicios digitales. Por ello, el derecho recurre habitualmente a la fijación tanto de reglas como de estándares para mitigar los problemas asociados a su inmadurez cognitiva, emocional y moral. Así, atendiendo a la evolución esperable de las facultades de los menores, se puede fijar una edad mínima para llevar a cabo un determinado acto o negocio jurídico o la validez de este puede hacerse depender de un estándar como el de la madurez o capacidad natural.

Una de las innovaciones más importante en la Propuesta de Reglamento EU KIDS ACT es el enfoque empleado en la regulación de la capacidad de los menores para acceder a determinadas tecnologías. El sistema parte de una adquisición progresiva y gradual de capacidad en entornos digitales en atención a la madurez de aquellos. Así, según el régimen de acceso que establece, los menores de 15 años no podrían crear cuentas autónomas en servicios de redes sociales o de compartición de videos que presenten riesgos para la privacidad, seguridad o la protección de los menores (art. 6.1.). Para los menores de 13 a 15 años, se prevé la intervención parental mediante cuentas vinculadas a las de sus progenitores o tutores (art. 6.2). Estas cuentas permitirían el acceso a redes sociales y plataformas de intercambio de vídeos adaptadas a la edad de los menores, incorporando medidas de protección como la limitación de los contactos sociales y del tiempo de uso a un máximo de una hora diaria. Por su parte, los menores de entre 3 y 13 años no podrían acceder a las redes sociales, aunque sí a servicios de intercambio de vídeos específicamente diseñados para niños, mediante cuentas gestionadas por sus progenitores o

tutores (art. 7)[1]. La propuesta parte así de una adquisición gradual de la capacidad de obrar de los menores que tiene en cuenta el progreso cognitivo, moral y emocional de estos. Este sistema gradual ha sido calificado como de acceso aplazado a las redes sociales (*social media delay*) y no como una prohibición de acceso (*social media ban*).

La solución europea contrasta con otros enfoques más rígidos, como el adoptado por el legislador francés, que estableció, en relación con las redes sociales, la ineficacia del consentimiento prestado tanto por menores por debajo de 15 años como por sus representantes legales en su nombre. La prohibición de uso de las redes sociales fue incluida en el artículo 1 del proyecto que llevó a la *Loi n° 2026-813 du 24 août 2026 visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux* (JORF n°0197 du 25 août 2026). Antes de su aprobación definitiva, el artículo 1 fue declarado inconstitucional por sentencia del *Conseil constitutionnel* de 14 de agosto de 2026 (Cons. const., déc. n° 2026-911 DC du 14 août 2026). El *Conseil constitutionnel* entendió que la protección del interés superior del menor y del orden público justificarían que el legislador limitara la libertad de acceso de los menores a estos servicios; ahora bien, para el Tribunal, el precepto era desproporcionado, al incluir una prohibición generalizada, sin tener en cuenta las funcionalidades del servicio ni la situación del menor, y sobre todo, sin dejar margen de maniobra a los titulares de la potestad parental. La Propuesta de Reglamento EU KIDS ACT evita este extremo.

Para los menores de 15 años se confía en el control parental. Los responsables parentales –«tutores» en la terminología de la propuesta– podrán establecer un límite de tiempo máximo, preaprobar posibles nuevos contactos y fijar un límite máximo en el número de contactos. La responsabilidad parental comprende el deber de velar por los hijos (art. 154 CC). No se trata de un derecho de los progenitores, sino de un deber en atención a los intereses del menor. Estas facultades de intervención pueden, sin embargo, incidir en la esfera personal de los menores y restringir su autonomía digital. Entre otras, pueden plantearse situaciones en las cuales unos progenitores se opongan a algunos actos de ejercicio por los menores de derechos vinculados con su autonomía digital; situaciones en las cuales los progenitores deciden recurrir a sistemas técnicos de control parental para restringir el acceso a contenidos que, sin ser ilícitos o peligrosos, los progenitores aborrecen; o situaciones en las cuales aquellos deciden acceder, sin autorización de los menores, a contenidos que forman parte de la intimidad personal de estos. Por ejemplo, se ha criticado como el control parental puede comportar una limitación desproporcionada en el acceso a información relevante para el desarrollo de la personalidad de los menores, especialmente, contenidos sobre educación sexual, pluralismo ideológico, aborto, anticoncepción, activismo político o sobre colectivos LGTBIQ+[2]. Sea como fuera, incluso para los servicios utilizados por menores de 13 años, el art. 7.4 de la Propuesta prescribe que «*[e]l diseño y el funcionamiento del acceso controlado por el responsable parental [...] no deberán restringir de manera desproporcionada la privacidad del menor y deberán apoyar la autonomía y la capacidad de decisión del menor, de acuerdo con la evolución de sus capacidades*». Una nueva manifestación del enfoque gradual de la Propuesta.

En relación con el segundo argumento –la mayor vulnerabilidad de los menores de edad frente a los riesgos–, se han identificado muchos peligros derivados del uso de diferentes tecnologías digitales. En algunos casos, se trata de riesgos generales, que pueden afectar tanto a menores

[1] La Propuesta prevé que los EEMM puedan establecer una edad mínima más alta para categorías específicas de contenido, como el contenido pornográfico o los juegos de azar (véanse Considerandos 20 y 38; y artículos 7.2 y 16.3).
[2] Vid., p.e., TAKHSHID, Zahra, «Children's Digital Privacy and the Case Against Parental Consent», *Texas Law Review*, vol. 101, núm. 6, 2023, pp. 1417-1455.

como a mayores de edad, mientras que, en otros supuestos, los riesgos son idiosincráticos de los menores o, dada su mayor vulnerabilidad, pueden tener un impacto superior en estos. Entre los diferentes riesgos, pueden destacarse, entre otros, los siguientes: adicción, exposición a contenidos dañinos o inadecuados, tendencias suicidas y autolesivas, sobreexposición, *cyberbulling*, violencia sexual, o pérdidas patrimoniales[3]. El debate sobre estos riesgos se ha acentuado después de que se publicaran reportajes sobre el conocimiento por parte de responsables de algunas redes sociales como Instagram y TikTok de los riesgos de adicción en menores, derivados de algunas decisiones sobre el diseño de los servicios y de los sistemas de recomendación[4]. También, noticias sobre suicidios y comportamientos lesivos en el uso de chatbots de inteligencia artificial generativa llevan a cuestionar la adecuación de estos servicios digitales para menores y han motivado ya varios pleitos.

En relación con la protección frente a los riesgos en entornos digitales, la Propuesta de Reglamento EU KIDS ACT establece obligaciones vinculantes de seguridad desde el diseño, es decir, manda la incorporación de medidas de seguridad y protección de la infancia desde la fase de diseño y configuración de los servicios digitales. En este sentido, la Propuesta pretende concretar y reforzar las obligaciones de protección de los menores previstas en el marco normativo europeo, particularmente en el artículo 28.4 del Reglamento de Servicios Digitales, transformando en exigencias jurídicas vinculantes determinados criterios que hasta ahora se recogían en instrumentos de carácter orientativo, como las *Directrices de la Comisión sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea* (C/2025/5519). Estas reglas en la Propuesta se alinean con otras sobre requisitos de seguridad de tecnologías digitales como, en EE.UU., las incluidas en las propuestas de *Kids Online Safety Act* (KOSA) (2022) y la *Children and Teens' Online Privacy Protection Act* (COPPA 2.0) (2023); en Italia,en la propuesta de ley sobre *disposizioni per la tutela dei minori nella dimensione digitale*, presentada el 29 de mayo de 2024, actualmente en tramitación; o en el Reino Unido, la *Online Safety Act* de 2023.

Las reglas de seguridad desde el diseño previstas en la Propuesta se aplican a un conjunto amplio de tecnologías digitales, que comprenden a los prestadores de servicios de redes sociales en línea, de servicios de plataformas de intercambio de vídeos, de juegos en línea, de compañeros de IA, de chatbots de propósito general y de tiendas de aplicaciones informáticas. Siguen algunos ejemplos.

El artículo 9 prohíbe los patrones de diseño adictivo para los prestadores de redes sociales y plataformas de intercambio de vídeos. Estos deberán evitar mecanismos que fomenten el uso compulsivo, como la reproducción automática sin interrupciones efectivas, las notificaciones que dificulten abandonar el servicio y los incentivos a la interacción frecuente. Asimismo, deberán establecer límites de uso y pausas que protejan el sueño y el horario escolar. El artículo 10 se refiere a los sistemas de recomendación: los prestadores de redes sociales y plataformas de intercambio de vídeos deberán priorizar las preferencias expresas de los menores, desactivar por

[3] Sonia LIVINGSTONE y Mariya STOILOVA han propuesto una taxonomía de riesgos para menores en entornos digitales denominada «4Cs», que clasifica los riesgos en cuatro categorías: *content, contact, conduct* y *contract*. Vid. LIVINGSTONE, Sonia/STOILOVA, Mariya, *The 4Cs: Classifying Online Risk to Children*, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut, 2021 (disponible en: https://doi.org/10.21241/ssoar.71817). La Comisión Europea ha añadido una quinta C: «*cross-cutting risks*» o riesgos transversales. Vid. *Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065* (C/2025/5519) (DO C 10.10.2025).

[4] En cualquier caso, la relación entre redes sociales y salud mental de niños y adolescentes es compleja. Vid. GALEA, Sandro/BUCKLEY, Gillian J. / et al., *Committee on the Impact of Social Media on Adolescent Health, Board on Population Health and Public Health Practice*, National Academies of Sciences, Engineering, and Medicine, 2023.

defecto las recomendaciones basadas en señales implícitas de comportamiento y evitar contenidos que pongan en riesgo su seguridad. También deberán ofrecer controles accesibles y opciones de recomendación no basadas en la elaboración de perfiles. Con arreglo al artículo 11, las redes sociales y plataformas de vídeo deberán aplicar ajustes que garanticen elevados niveles de privacidad y seguridad, desactivando por defecto la geolocalización, el acceso al micrófono y la cámara, las sugerencias de cuentas, la sincronización de contactos y las notificaciones push. Estas plataformas deberán impedir también los contactos directos no autorizados previamente por el menor, limitar la visibilidad de su información y establecer salvaguardias frente a interacciones potencialmente perjudiciales (artículo 12). Finalmente, según el artículo 13, los prestadores de redes sociales y plataformas de vídeo deberán garantizar la transparencia de las operaciones económicas dirigidas a menores, informar previamente de las transacciones y del valor monetario de las monedas virtuales, y prevenir prácticas que incentiven el gasto excesivo, incluidos los sistemas de recompensas aleatorias.

En relación con los compañeros de IA y chatbots conversacionales generales, el artículo 14 establece que sus proveedores deberán adoptar medidas proporcionadas para proteger la salud, la seguridad, los derechos fundamentales y el bienestar de los menores. En particular, deberán evitar diseños que generen dependencia emocional mediante la simulación de relaciones interpersonales y aplicar salvaguardias contra su uso compulsivo. Cuando estas herramientas estén integradas en otros servicios, deberán permanecer desactivadas por defecto y permitir, además, una desactivación sencilla. Con arreglo al artículo 15, los proveedores de juegos en línea deberán prevenir también el uso compulsivo, establecer configuraciones seguras por defecto, proteger las interacciones entre usuarios y facilitar herramientas de supervisión parental. También deberán impedir que los juegos induzcan a los menores a establecer contactos potencialmente peligrosos en otros servicios. Finalmente, según el artículo 16 de la Propuesta, los proveedores de tiendas de aplicaciones deberán implantar sistemas de clasificación por edades para todas las aplicaciones, impedir que los menores accedan o compren aplicaciones inadecuadas para su edad, verificar la edad de los usuarios y publicar los criterios y métodos de clasificación.

En buena medida, la Propuesta contribuye a delimitar con mayor precisión el estándar de diligencia exigible a varios proveedores de servicios digitales orientado a la protección de los derechos e intereses de los menores de edad. En lugar de limitarse a recomendar buenas prácticas, el establecimiento de obligaciones normativas específicas permitiría evaluar la conducta de las plataformas a partir de parámetros jurídicos previamente definidos, que serán especialmente muy relevantes para la aplicación pública de la norma (artículo 34). Pero, además, esta evolución podría tener consecuencias relevantes en el ámbito de la responsabilidad civil extracontractual. En particular, la existencia de un estándar legal de diligencia explícito podría facilitar que los menores perjudicados, a través de sus representantes legales cuando corresponda, fundamentasen reclamaciones indemnizatorias ante los tribunales nacionales por los daños psicológicos o emocionales derivados de determinadas prácticas de diseño digital. Si, por ejemplo, una plataforma incumpliera obligaciones específicas destinadas a prevenir patrones de utilización compulsiva y dicho incumplimiento pudiera vincularse causalmente con un perjuicio psicológico acreditado, las disposiciones de la Propuesta de Reglamento EU KIDS ACT podrían servir como parámetro normativo para valorar si el proveedor actuó o no con la diligencia jurídicamente exigible.

En este contexto, estos deberes de seguridad desde el diseño podrían reducir las dificultades interpretativas asociadas a la identificación del deber de cuidado aplicable a las empresas

tecnológicas en sus relaciones con niños y adolescentes. La cuestión ya no consistiría únicamente en determinar si una plataforma actuó de forma razonable conforme a criterios generales de buena práctica, sino también en examinar si observó las obligaciones concretas establecidas por el legislador europeo. Por supuesto, el incumplimiento de una obligación de seguridad no presume *per se* la negligencia, ni genera automáticamente responsabilidad civil, pero puede facilitar mucho la prueba de la imputación subjetiva y objetiva. De forma muy clara, la Propuesta de Reglamento EU KIDS ACT delimita muy bien los riesgos de daño que persigue evitar e identifica a los menores como los sujetos destinatarios de la protección ofrecida por sus normas. En cualquier caso, la viabilidad de estas acciones dependerá del contenido definitivo de la norma, de su relación con las reglas nacionales de responsabilidad civil y de la posibilidad de acreditar los restantes elementos exigidos por el ordenamiento aplicable, entre ellos la existencia de un daño indemnizable y la relación de causalidad entre la conducta del proveedor y el perjuicio sufrido. Las incertidumbres sobre los dos últimos requisitos son muchas y de calado.

En estos momentos, es muy difícil predecir si esta iniciativa va a cristalizar en un nuevo Reglamento y, en su caso, si las normas propuestas van a sufrir muchos o pocos cambios. Hay, al menos, dos cuestiones que no invitan al optimismo. Primero, las diferencias entre varios ordenamientos europeos que yan han aprobado normas sobre el acceso de menores a redes sociales y sobre la capacidad de estos en entornos digitales pueden hacer descarrilar la Propuesta en el marco del Consejo: de hecho, no queda claro hasta qué punto la competencia basada en el mercado interior (artículo 114 TFUE) ha de desplazar la competencia de los EEMM sobre decisiones tradicionales de derecho privado, como las referidas a la autonomía y a la capacidad de obrar de sus menores de edad[5]. Y segundo, dada la situación geopolítica de la Unión, otros asuntos más prioritarios pueden retrasar los debates sobre la Propuesta de Reglamento EU KIDS ACT y relegarla a un plano secundario.

Antoni Rubí Puig

[5] Véase Esther FORSON, «From Tobacco to TikTok: The KIDS Act and the Expansion of EU Harmonisation Powers», *European Law Blog*, 9 October 2026.