

Avanza el nuevo Reglamento contra el abuso sexual de menores

El pasado mes de mayo la Comisión Europea presentó su propuesta de Reglamento por el que se establecen normas para prevenir y combatir el abuso sexual de menores¹, que contempla diversas iniciativas como la obligación de escanear mensajes privados por parte de los prestadores de servicios de internet para detectar material relacionado con ese abuso, como pornografía infantil o ciberacoso, incluso cuando esos mensajes puedan estar protegidos por cifrados de extremo a extremo como ocurre en el caso de WhatsApp.

Dichos prestadores estarían obligados a detectar el material abusivo, ya sea nuevo o antiguo, informando sobre el mismo, eliminándolo o, al menos, bloqueándolo para impedir el acceso al mismo, a partir de órdenes de detección dictadas por las autoridades nacionales.

Esta obligación de monitorización, es decir, de actuación *ex ante* y no sólo por propia iniciativa o a requerimiento de las entidades competentes para solicitar la retirada de contenidos o el cierre de páginas, supone un cambio de gran calado frente al estatuto mantenido hasta ahora por plataformas, buscadores, redes y prestadores de mensajería digital, que se consideraban exentos de "responsabilidad editorial" sobre los contenidos difundidos por terceros. Pero también afecta a otros aspectos, como la privacidad de los datos y las comunicaciones.

Va más allá, en este sentido, de la responsabilidad activa de las plataformas y redes recogida en la Directiva sobre propiedad intelectual y el Reglamento de Servicios Digitales.

La propuesta de nuevo reglamento también propone la creación de un centro a nivel de la UE a cuya base de datos los proveedores podrían acudir para contrastar si un determinado material está identificado como ilícito, únicamente en lo referido al abuso sexual y el acoso (*grooming*).

Algunos colectivos dedicados a la protección de la infancia consideran que la propuesta se queda corta, ya que no aborda la producción del material que contiene abusos sexuales a menores, sino solo su difusión, intercambio y almacenamiento. Otras organizaciones ven en ella un riesgo para la libertad de expresión en internet con la "excusa" de perseguir dicho abuso.

¹ Acceder al texto y a los anexos en:

https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0010.02/DOC_1&format=PDF
https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0010.02/DOC_1&format=PDF

Así, para la plataforma Xnet plantea el imposible de una tecnología encriptada y a la vez inspeccionable, generando brechas de seguridad, estableciendo la vigilancia masiva y anulando la inviolabilidad de las comunicaciones. Y además ataca a la variedad de ofertas como las que proporcionan startups y pymes tecnológicas a favor de los monopolios.

En agosto de 2021 entró en vigor un Reglamento temporal que derogaba algunas disposiciones de la directiva europea de privacidad electrónica (anterior al Reglamento General de Protección de Datos), estableciendo que los proveedores de servicios de comunicaciones electrónicas podían procesar datos sin el consentimiento del usuario por motivos específicos, como la seguridad o la facturación. Ello permite ya a estos proveedores escanear y denunciar los mensajes privados en línea que contengan material que muestre abusos sexuales a menores bajo señalamiento. El Reglamento, que expira en agosto de 2024, sería sustituido por el que constituye objeto de la actual propuesta, de modo que, como decíamos, lo que ahora se permite a las empresas (aplicar tecnologías aprobadas para detectar técnicas de captación de menores) de forma voluntaria se convertiría, como decíamos, en obligatorio.

El Parlamento Europeo ha anunciado su voluntad de llegar a un acuerdo antes de noviembre en relación con la propuesta. Este acuerdo daría paso a la negociación con el Consejo y la Comisión (trílogos) antes de acabar el año, en el periodo por tanto de la presidencia española.