Dossier Digital 5° Número - 16 Agosto, 2022

CSAM DE LA UNIÓN EUROPEA: ANÁLISIS DE LA PROPUESTA DE REGLAMENTO DE LA LUCHA CONTRA EL ABUSO SEXUAL DE MENORES

UN TRABAJO DEL IDD LAC

¡BIENVENIDOS!

Este análisis de Dossier Digital, iniciativa desarrollada por el Instituto de Desarrollo Digital para América Latina y el Caribe, se centra en analizar la Propuesta de Reglamento Del Parlamento Europeo y Del Consejo[1] del 11 de May de 2022, por el que se establecen normas para prevenir y combatir el abuso sexual infantil, reflejando su justificación, contenido y reacciones a la misma, principalmente en cuanto al nivel de obligaciones que la propuesta de norma implica.

ANÁLISIS DE LA PROPUESTA DE REGLAMENTO DE LA UNIÓN EUROPEA DE LA LUCHA CONTRA EL ABUSO SEXUAL DE MENORES: OBLIGACIONES DE ESCANEO PARA SERVICIOS DE ALOJAMIENTO Y DE MENSAJERÍA.

1. Justificación inicial para la elaboración de la Propuesta

La Comisión señaló que lucha contra el abuso sexual infantil en línea era una prioridad para la misma. Señalan que en ausencia de normas armonizadas a nivel de la UE, las plataformas de redes sociales, los servicios de juegos y otros proveedores de servicios de alojamiento y en línea en la actualidad se enfrentan a normas divergentes.

Señalan que si bien ciertos proveedores usan tecnología voluntariamente para detectar, informar y eliminar material de abuso sexual infantil en sus servicio, las medidas que desde estos sectores han sido adoptadas varían mucho y la acción voluntaria habría demostrado ser insuficiente para abordar el problema. La propuesta que realiza la comisión se basa en la Ley de Servicios Digitales (DSA)[2] y la complementa con disposiciones para abordar los desafíos específicos que plantea el abuso sexual infantil en línea.

2. Antecedentes

La propuesta presentada en Mayo, nace de la estrategia de la UE de julio de 2020 para tratar de afrontar una lucha más eficaz contra el abuso sexual infantil, ofreciendo una respuesta integral a la creciente amenaza del abuso sexual infantil tanto fuera de línea como en línea, con el propósitio de mejorar la prevención, la investigación y la asistencia a las víctimas. También se produce después de que la Comisión presentara su Estrategia de la UE sobre los Derechos del Niño de, que proponía medidas reforzadas para proteger a los niños contra todas las formas de violencia, incluido el abuso en línea.

El 21 de mayo de 2021 tras un acuerdo del Coreper,[3] el Consejo y el Parlamento Europeo alcanzaron un acuerdo provisional sobre una medida temporal para permitir que los

[1] Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0209

[2] Disponible en https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_es

[3] El Comité de Representantes Permanentes o Coreper se encarga de preparar los trabajos del Consejo de la Unión Europea.

proveedores de servicios de comunicaciones electrónicas, como el correo web y los servicios de mensajería, siguieran detectando, retirando y denunciando el abuso sexual de menores en línea, también por lo que respecta a la lucha contra la captación de menores, hasta que estuviera en vigor la legislación permanente anunciada por la Comisión Europea.

Dado que la Directiva sobre privacidad y las comunicaciones electrónicas de 2002,[4] que garantizaba la confidencialidad de las comunicaciones y los datos personales en el sector de las comunicaciones electrónicas, se basa en la definición de servicios de comunicaciones electrónicas, los servicios de comunicaciones interpersonales independientes de la numeración están también ahora sujetos a las normas de confidencialidad de la mencionada Directiva en lugar de a las del Reglamento General de Protección de Datos (RGPD). A diferencia del RGPD, la Directiva no contiene una base jurídica explícita con respecto al tratamiento voluntario de contenidos o datos de tráfico para fines de detección de abusos sexuales de menores. Por lo tanto, se introdujo una excepción específica para los servicios incluidos en el ámbito de aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas.

El acuerdo establecía una excepción al artículo 5, apartado 1, y al artículo 6, apartado 1, de la citada Directiva, a fin de permitir a los proveedores detecten, retiren y denuncien material de abuso sexual de menores y aplicando la tecnología contra la captación de menores.

Tras ese acuerdo, La Comisión anunción que propondría una normativa general para luchar contra el abuso sexual de menores en línea. Dicha normativa tendría por objeto ofrecer una solución duradera para sustituir esta medida temporal, así nace la propuesta actual.

3. Propuesta

La Comisión propone una nueva legislación de la UE para prevenir y combatir el abuso sexual infantil en línea.

En su justifiación señalan que “Con 85 millones de imágenes y videos que muestran abuso sexual infantil reportados en todo el mundo solo en 2021, y muchos más sin denunciar, el abuso sexual infantil es generalizado. La pandemia de COVID-19 ha exacerbado el problema, y la fundación Internet Watch ha observado un aumento del 64 % en las denuncias de abuso sexual infantil confirmado en 2021 en comparación con el año anterior”

Señalan que el sistema actual basado en la detección y denuncia voluntaria por parte de las empresas ha demostrado ser insuficiente para proteger adecuadamente a los niños y,

[4] Disponible en https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=celex:32002L0058

en cualquier caso, dejará de ser posible una vez que expire la solución provisional que se mencionó antes. Según la propuesta hasta “el 95% de todos los informes de abuso sexual infantil recibidos en 2020 provinieron de una misma empresa”, a pesar de ello también reconocen que el problema no existe solo en una plataforma.

Para abordar de manera efectiva el uso indebido de los servicios en línea con fines de abuso sexual infantil, en opinión de la Comisión Europea se necesitan reglas claras, con condiciones y salvaguardas sólidas. Según lo establecido en la propuesta, la misma obligará a los proveedores a detectar, informar y eliminar material de abuso sexual infantil en sus servicios. Los proveedores deberán así, evaluar y mitigar el riesgo de uso indebido de sus servicios y las medidas que se tomen deben ser proporcionales a ese riesgo y sujetas a condiciones y salvaguardas sólidas.

La propuesta prevé la creación de un nuevo **Centro independiente de la UE sobre el abuso sexual infantil** que facilitaría los esfuerzos de los proveedores de servicios puesto que en su opinión actuaría como un centro de experiencia, proporcionando información confiable sobre el material identificado, recibiendo y analizando los informes de los proveedores para identificar informes erróneos y evitar que alcancen aplicación de la ley, reenviando rápidamente informes relevantes para la acción de aplicación de la ley y brindando apoyo a las víctimas.

Las nuevas reglas nacen con la voluntad de prevenir que nuevos menores sufran abusos y sacar a los que ya los están sufriendo, evitar que el material vuelva a aparecer en línea y llevar a los infractores ante la justicia.

Esas reglas incluirán:

- Evaluación de riesgos obligatoria y medidas de mitigación de riesgos: los proveedores de servicios de alojamiento o de comunicación interpersonal tendrán que evaluar el riesgo de que sus servicios se utilicen indebidamente para difundir material de abuso sexual infantil o para la captación de niños, lo que se conoce como preparación. Los proveedores también tendrán que proponer medidas de mitigación de riesgos.

- Obligaciones de detección específicas, basadas en una orden de detección: los Estados miembros deberán designar autoridades nacionales encargadas de revisar la evaluación de riesgos. Cuando dichas autoridades determinen que persiste un riesgo significativo, pueden solicitar a un tribunal o a una autoridad nacional independiente que emita una orden de detección de material de abuso sexual infantil o manipulación. Las órdenes de detección están limitadas en el tiempo y se dirigen a un tipo específico de contenido en un servicio específico.

- Sólidas garantías de detección: las empresas que hayan recibido una orden de detección solo podrán detectar contenido utilizando indicadores de abuso sexual infantil verificados y proporcionados por el nuevo Centro de la UE. Las tecnologías de detección solo deben utilizarse con el fin de detectar el abuso sexual infantil. Los proveedores deberán implementar tecnologías que sean lo menos intrusivas para la privacidad de acuerdo con el estado del arte en la industria, y que limiten la tasa de error de falsos positivos en la mayor medida posible.

- Obligaciones de denuncia claras: los proveedores que hayan detectado abuso sexual infantil en línea deberán denunciarlo al Centro de la UE.

- Eliminación efectiva: las autoridades nacionales pueden emitir órdenes de eliminación si el material de abuso sexual infantil no se elimina rápidamente. Los proveedores de acceso a Internet también deberán deshabilitar el acceso a imágenes y videos que no se pueden eliminar, por ejemplo, porque están alojados fuera de la UE en jurisdicciones no cooperativas.

- Reducir la exposición: las reglas requieren que las tiendas de aplicaciones se aseguren de que los niños no puedan descargar aplicaciones que puedan exponerlos a un alto riesgo

- Sólidos mecanismos de supervisión y reparación judicial: Las órdenes de detección serán emitidas por tribunales o autoridades nacionales independientes. Para minimizar el riesgo de detección e informes erróneos, el Centro de la UE verificará los informes de posibles abusos sexuales infantiles en línea realizados por proveedores antes de compartirlos con las autoridades policiales y Europol. Tanto los proveedores como los usuarios tendrán derecho a impugnar ante los tribunales cualquier medida que les afecte.

El nuevo Centro de la UE apoyará a:

- Los Proveedores de servicios en línea, en particular para cumplir con sus nuevas obligaciones de realizar evaluaciones de riesgo, detectar, informar, eliminar y deshabilitar el acceso al abuso sexual infantil en línea, proporcionando indicadores para detectar el abuso sexual infantil y recibiendo los informes de los propios proveedores.

- Las fuerzas del orden nacionales y la Europol, revisando los informes de los proveedores y canalizándolos rápidamente a las fuerzas del orden.

- Los Estados miembros, sirviendo como un centro de conocimiento para las mejores prácticas en prevención y asistencia a las víctimas, fomentando un enfoque basado en evidencia.

- A las Víctimas, ayudándolas a retirar los materiales que representan su abuso.

La Comisión también presentó una estrategia europea para una Internet mejor para los niños[5] que acompaña esta propuesta. Dicha estrategia nace con la voluntad de mejorar los servicios digitales adaptados a la edad infantil y velar por que todos los niños estén protegidos y capacitados y sean respetados en línea.

Ahora corresponde al Parlamento Europeo y al Consejo acordar la propuesta definitiva. Una vez adoptado, el nuevo Reglamento sustituirá al actual Reglamento provisional. Actualmente se puede recibir comentarios a la actual propuesta.

[5] Disponible en https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2825

4. Reacciones a la propuesta

La propuesta de reglamento ha provocado reacciones encontradas, desde sus promotores y posteriores defensores que lo ven como un paso fundamental hacia prevenir los delitos de índole sexual en internet, hacia aquellos que reconociendo el problema y la necesidad de enfrentar esta clase de delitos señalan que la propuesta podría vulnerar derechos fundamentales de difícil reparación.

Reacciones a favor

- La Comisaria de Democracia y Demografía, la croata **Dubravka Šuica**, dijo: “Defender y proteger los derechos de los niños tanto en línea como fuera de línea es esencial para el bienestar de nuestras sociedades. El material de abuso sexual infantil en línea es un producto del abuso sexual físico manifestado de los niños. Es altamente criminal. El abuso sexual infantil en línea tiene amplias consecuencias a largo plazo para los niños y deja un profundo trauma. Algunos pueden, y lo hacen, nunca recuperarse. El abuso sexual infantil se puede prevenir si trabajamos juntos para proteger a los niños. No permitimos el abuso sexual infantil fuera de línea, por lo que no debemos permitirlo en línea”.

- El Comisario europeo “para la promoción de estilo de vida europeo”, el griego **Margaritis Schinas**, señaló: "La gran cantidad de material de abuso sexual infantil que circula en la web es asombrosa. Y vergonzosamente, Europa es el centro mundial para la mayor parte de este material. Así que es realmente en gran medida una cuestión de si no actuamos, ¿quién lo hará? Las reglas que estamos proponiendo establecen obligaciones claras, específicas y proporcionadas para que los proveedores de servicios detecten y eliminen contenido ilegal de abuso sexual infantil. Lo que los servicios podrán hacer será muy estricto. protegido con fuertes medidas de seguridad: solo estamos hablando de un programa que escanea en busca de marcadores de contenido ilegal de la misma manera que los programas de ciberseguridad ejecutan controles constantes en busca de violaciones de seguridad”.

- La Comisaria de Interior, la sueca **Ylva Johansson**, dijo: “Como adultos, es nuestro deber proteger a los niños. El abuso sexual infantil es un peligro real y creciente: no solo está aumentando el número de informes, sino que estos informes hoy en día se refieren a niños más pequeños. Estos informes son fundamentales para iniciar investigaciones y rescatar a los niños del abuso continuo en tiempo real. Por ejemplo, una investigación apoyada por Europol basada en un informe de un proveedor de servicios en línea permitió salvar a 146 niños en todo el mundo con más de 100 sospechosos identificados en toda la UE. También se necesita con urgencia la detección, denuncia y eliminación del abuso sexual infantil en línea para evitar que se compartan imágenes y videos del abuso sexual infantil, que vuelve a traumatizar a las

victimas, a menudo años después de que el abuso sexual ha terminado. La propuesta de hoy establece obligaciones claras para que las empresas detecten y denuncien el abuso de niños, con fuertes salvaguardas que garantizan la privacidad de todos, incluidos los niños".

Análisis crítico de la propuesta

En opinión de gabinetes jurídicos expertos como el español **Quatrecases**[6] Si este reglamento entrará en vigor en su actual propuesta, las obligaciones de detección que establece tendría que convivir con la actual prohibición de que los intermediarios establezcan medidas de supervisión sobre los contenidos que transmiten o albergan. La responsabilidad de intermediarios bajo el principio de no supervisión era hasta ahora un hecho incuestionable garantizado en las Directivas de Comercio Electrónico[7] como en la propia DSA

La propia DSA establece que establecer obligaciones de este tipo tendría como consecuencia una limitación desproporcionada de la libertad de expresión, la libertad de información, además de una carga excesiva para los proveedores de servicios. La DSA refleja en opinión de este reconocido buffete que "la prohibición general de monitorización tiene implicaciones positivas para la protección de los datos personales y la privacidad"

Muchas de las críticas a la actual propuesta se centran en el escaneo de CSAM, puesto que señalan que con la actual propuesta todas nuestras fotos y video compartidas en redes de mensajería instantánea o apps populares podrían ser escaneadas para verificar si hay imágenes y videos de abuso sexual infantil. Esta circunstancia, según expertos en la materia, puede socavar el cifrado de extremo a extremo que protege a los miles de millones de mensajes enviados todos los días y dificultar la privacidad en línea de las personas.

En esta misma línea, la **Global Encryption Coalition (GEC)** sacó un comunicado[8] que señalaba lo siguiente:

"La legislación de la Comisión permitiría a los Estados miembros obligar a las plataformas en línea, incluidas aquellas que ofrecen mensajes cifrados de extremo a extremo, a escanear el contenido y los metadatos de los usuarios en busca de imágenes CSA y conversaciones y comportamientos de "preparación" y, cuando corresponda, informarlos al público y autoridades y luego eliminarlos de sus plataformas. Dicho requisito es fundamentalmente incompatible con la mensajería cifrada de extremo a extremo porque las plataformas que ofrecen dicho servicio no pueden acceder al contenido de las comunicaciones. Esto ha sido confirmado por expertos de todo el mundo que produjeron un análisis de cómo cualquier forma de escaneo rompe los sistemas cifrados de extremo a

[6] https://www.cuatrecasas.com/es/spain/articulo/ue-el-interes-primordial-del-menor-la-excepcion-al-principio-general-de-no-supervision

[7] Disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=uriserv:OJ.L_.2000.178.01.0001.01.SPA

[8] Disponible en https://www.globalencryption.org/2022/05/joint-statement-on-the-dangers-of-the-eus-proposed-regulation-for-fighting-child-sexual-abuse-online/

extremo, además de un informe detallado sobre las múltiples formas en que el escaneo del lado del cliente, en particular, "puede fallar". , puede ser evadida y puede ser abusada".

La GEC señala que "En lugar de imponer medidas que sean inconsistentes con el cifrado de extremo a extremo y que disminuirían la seguridad de todos, los reguladores deberían incentivar medidas que aborden la CSA y protejan la seguridad de las comunicaciones. Entre estas medidas está facilitar la notificación de los usuarios de material CSA."

La propuesta europea de escanear los mensajes de las personas se ha encontrado con la crítica de numerosas organizaciones de la sociedad civil y de expertos en seguridad, quienes dicen que el cifrado de extremo a extremo, elemento que se ha convertido en una herramienta predeterminada en aplicaciones de mensajería como iMessage, WhatsApp y Signal.

El CEO de WhatsApp **Will Cathcart** señaló que: "Increíblemente decepcionante ver que una propuesta de regulación de la UE en Internet no protege el cifrado de extremo a extremo", y también que "Esta propuesta obligaría a las empresas a escanear los mensajes de cada persona y pondría en grave riesgo la privacidad y la seguridad de los ciudadanos de la UE".
Cualquier sistema que debilite el cifrado de extremo a extremo podría pese a la buena intención inicial ser aprovechado para buscar otros tipos de contenido, según señalan muchos expertos técnicos.

El profesor de ciberseguridad de la Universidad de Surrey, **Alan Woodward** señala: "O tienes E2EE o no" y que la voluntad de pedir puertas traseras en los mensajes cifrados E2E, sin entender que es una imposibilidad tecnológica es un error. Woodward señala que existe una posible solución alternativa: Escaneo en el dispositivo, después de que se haya descifrado el mensaje. Pero ese es precisamente el mismo enfoque que Apple propuso usar para el escaneo CSAM, y que generó tanto rechazo sobre el potencial de abuso por parte de gobiernos represivos.

En cuanto al escaneo del CSAM en dispositivos personales muchos plantean la pregunta de si ¿Está bien que la UE introduzca mecanismos de vigilancia masiva para todos los ciudadanos de la UE en un intento de atajar los abusos sexuales a menores?

Alexandra Koch-Skiba, de la Asociación alemana Eco, afirma: "En nuestra opinión, el proyecto tiene el potencial de crear un pase libre para la vigilancia del gobierno. Esto es ineficaz e ilegal. La protección sostenible de los niños y los jóvenes requeriría, en cambio, más personal para las investigaciones y una persecución exhaustiva".

Según la propuesta actual, el sector privado se vería obligado por ley a proporcionar a las autoridades europeas, todos los activos que les sean requeridos. En opinión de expertos como David Salcés[9] "A diferencia de lo que ocurre en la actualidad, con la iniciativa en este sentido en manos de las tecnológicas, estas pasarán a depender de las autoridades, con independencia de que decidan, o no, mantener de manera adicional sus propias iniciativas al respecto".

[9] Disponible en https://www.muycomputer.com/2022/05/12/europa-persigue-csam-privacidad/

“Por hablar más claro, si existe sospecha de que algún ciudadano europeo crea, posee, intercambia y/o comercializa contenido CSAM, las tecnológicas estarán obligadas, en Europa, a proporcionar a las autoridades todo los activos digitales de la persona sospechosa, sus conversaciones de WhatsApp, los archivos que almacena en la nube, etcétera. Incluido, como indicaba antes, también aquellos activos que actualmente se protegen con cifrado de extremo a extremo”

Es cierto también señala que se ofrece un marco bastante garantista de los derechos de la ciudadanía. No se trataría, según el texto legal, “de una barra libre de acceso a activos digitales de los ciudadanos, siempre con el aval de los reguladores y con los sistemas de protección necesarios para evitar la explotación inadecuada de este acceso preferente”

Pero “El simple establecimiento de este tipo de accesos, aunque sean tremendamente limitados, ya plantea un importante problema de seguridad, que podemos dar por seguro que se traducirá en muchos intentos de explotarlo. Desde ciberdelincuentes hasta gobiernos y empresas con servicios como el cada vez más polémico Pegasus, podemos apostar a que la implementación de puertas traseras, tal y como podría pedir Europa a las tecnológicas, iniciará una caza del zorro como nunca hemos visto hasta ahora.”.

El Center for democracy and technology (CDT)[10] publicó un análisis inicial en el que señalan que ell Reglamento CSA propuesto es fundamentalmente inconsistente con el cifrado de extremo a extremo porque requiere que los proveedores escaneen el contenido del usuario en busca de imágenes CSA conocidas y desconocidas, y conversaciones de "preparación" CSA. Para realizar tal actividad, el prestador debe tener acceso al texto de las comunicaciones que realiza en su servicio; los proveedores de servicios E2EE no tienen dicho acceso. Presentamos otras objeciones a la Propuesta de Reglamento CSA, incluida la forma en que prevé el acceso gubernamental sin orden judicial a las comunicaciones, así como el impacto negativo que tendrá en los derechos de libre expresión.

Además, European Digital Rights (EDRi) está haciendo circular una carta[11] en la que pide la retirada del Reglamento CSA propuesto debido a su impacto, entre otras cosas, en el cifrado. Como señala EDRi en la carta, el Reglamento CSA propuesto en realidad coacciona la misma conducta invasiva de la privacidad que las instituciones europeas han cuestionado: crea un régimen en el que se alienta a los proveedores de servicios de comunicación a escanear y controlar lo que dicen sus usuarios en línea, empoderando a los plataformas y debilitando los derechos de sus usuarios.

[10] https://cdt.org/insights/briefing-document-on-key-issues-in-european-commissions-csam-proposal/

[11] https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/