1. Introducción y contexto

La Comisión Europea presentó en 2022 una propuesta de Reglamento para combatir el abuso sexual infantil en línea. Su elemento clave es el escaneo automatizado de todas las comunicaciones privadas, incluso en apps cifradas.

La UE considera que el volumen de material de abuso infantil ha crecido de forma explosiva (85 millones de imágenes reportadas en 2021). Para la Comisión, las medidas actuales voluntarias son insuficientes.

Sin embargo, esta propuesta entra en conflicto con décadas de protección de privacidad en Europa (RGPD, ePrivacy). Su aprobación implicaría un cambio profundo en la arquitectura de las comunicaciones digitales en la UE.

2. Historia legislativa

Antes de 2021: la legislación impedía a proveedores escanear mensajes privados.

2021 Chat Control 1.0: excepción temporal que permitió escaneo voluntario.

2022: nace la propuesta Chat Control 2.0, obligatoria y mucho más amplia.

El proceso legislativo se polarizó:

En contra

Servicio Jurídico del Consejo

Autoridad Europea de Protección de Datos (EDPS)

Comité Europeo de Protección de Datos (EDPB)

Los organismos alertaron de que el escaneo masivo vulnera derechos fundamentales y rompe el secreto de las comunicaciones.

Parlamento Europeo

Intentó limitar el escaneo solo a casos dirigidos, con sospecha individual.

Estados miembros divididos

Opositores: Alemania, Países Bajos, Austria, Finlandia, Polonia.

Partidarios: Francia, España, Italia, Irlanda y países del sur y este.

2025: El Consejo propone un compromiso:

el escaneo ya no sería obligatorio…

pero sí incentivado como requisito para demostrar que un proveedor mitiga riesgos, lo que en práctica lo vuelve casi obligatorio.

El trámite entró en trílogos, presionado por el vencimiento del régimen temporal en 2026.

3. Contenido técnico del Reglamento

a) Evaluación obligatoria de riesgos

Todas las plataformas deben evaluar riesgos de CSAM o grooming. Las de mayor riesgo deben aplicar medidas de mitigación, entre ellas escaneo voluntario.

b) Órdenes de detección

Permiten escanear todas las comunicaciones privadas de un servicio:

detección de imágenes conocidas mediante hashes

detección de imágenes nuevas mediante IA

detección de grooming mediante análisis semántico de chats

c) Escaneo del lado del cliente

En apps cifradas E2EE, el escaneo ocurre antes de cifrar el mensaje, instalando un módulo de monitoreo dentro del dispositivo del usuario. Expertos lo consideran equivalente a un software espía integrado.

d) Centro Europeo de lucha contra el Abuso Infantil

Recibe todos los reportes generados por empresas, filtra falsos positivos, transfiere casos a Europol y mantiene bases de datos.

e) Verificación obligatoria de edad

Plataformas deben identificar si un usuario es menor, eliminando el anonimato y obligando a recopilar datos sensibles.

f) Eliminación y bloqueo de contenido

Obligación de retirar archivos y bloquear URL.

g) Salvaguardas legales

Incluyen supervisión judicial y transparencia, aunque críticos dicen que no neutralizan el impacto.

4. Argumentos a favor

a) Protección de menores

La escala del problema justifica medidas extraordinarias; investigaciones han permitido rescates de menores.

b) Medidas voluntarias insuficientes

Muchas plataformas no actúan y Europa depende de reportes de EE.UU.

c) Seguridad jurídica

El escaneo actual opera en vacío legal.

d) Cooperación internacional más rápida

El nuevo Centro Europeo agiliza intercambios.

e) Actualización legal

Delincuentes migran a sistemas cifrados.

f) Salvaguardas

Se afirma que no se rompe el cifrado, aunque expertos lo cuestionan.

5. Argumentos en contra

a) Vigilancia masiva inconstitucional

Va contra privacidad y presunción de inocencia.

b) Rompe o debilita el cifrado

Escaneo en dispositivo equivale a puerta trasera, expone a hackers y gobiernos.

c) Falsos positivos

Hasta 80% pueden no ser ilegales; afecta a inocentes y consume recursos policiales.

d) Ineficacia

Delincuentes usan canales alternativos como dark web o cifrado propio.

e) Fin del anonimato

Afecta activistas, periodistas, víctimas y menores. Genera autocensura.

f) Precedente autoritario

Podría expandirse a terrorismo, delitos económicos o control político.

g) Desvía recursos

No mejora prevención ni apoyo a víctimas.

6. Comparación internacional

Estados Unidos: EARN IT incentiva escaneo indirecto.

China: identidad real obligatoria, vigilancia total, cifrado fuerte prohibido.

Ninguna democracia ha implementado un sistema tan amplio como el propuesto por la UE.

7. Impactos proyectados

Privacidad: desaparición del secreto de comunicaciones.

Seguridad digital: nuevas vulnerabilidades.

Economía: plataformas podrían abandonar la UE.

Libertad de expresión: autocensura generalizada.

8. Alternativas menos invasivas

Perseguir fuentes de alojamiento, cooperación internacional real, infiltración policial, prevención offline, herramientas opcionales y tecnologías criptográficas no intrusivas.

9. Conclusión general del informe

Chat Control 2.0 implica el mayor choque entre seguridad y derechos fundamentales en la historia digital europea. Es desproporcionado, inseguro y existen alternativas más eficaces sin instaurar vigilancia masiva.