Xnet

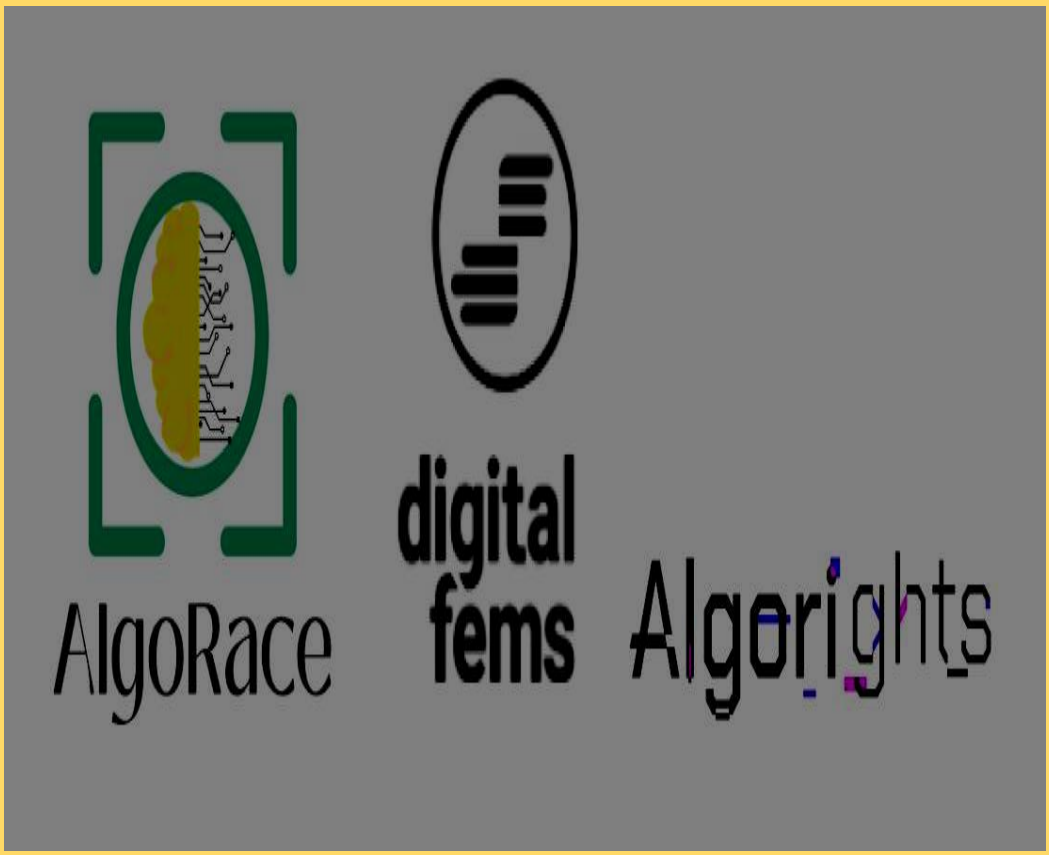
•Quiénes somos

•Blog – Nuestras acciones

- **Derechos digitales, datos, IA y neutralidad de la Red**
- **Libertad de expresión e información vs fake news, propaganda y desinformación**
- **Tecnopolítica y arte de la comunicación de incidencia. Democracia actualizada a la era digital. Método i+d político. Vigilancia ciudadana del poder**
- **Cultura Libre [vídeos y +]**
- **Alertadores – Whistleblowers. Filtraciones anticorrupción**
- **Luchas por las libertades civiles. Redes nacionales e internacionales**

23 mayo, 2023

#ChatControl – Lanzamos campaña contra la ley de monitorización automatizada de las conversaciones íntimas de la ciudadanía europea.



Contenido

– Tecnología imposible, invasiva y que no resuelve el problema del abuso infantil

– Establece la vigilancia masiva. Anula la inviolabilidad de las comunicaciones

– Debilita la tutela judicial efectiva (demasiado extensos los ámbitos no sujetos a mandato judicial, como el registro de espacios privados)

– Tecnología invasiva que es en sí una brecha de seguridad

– Ataca los sistemas distribuidos y las startups y PyMEs tecnológicas en favor de los monopolios

– Falsos positivos que pueden acusar a cualquiera inundarán los investigadores

– Argumentos contra la verificación de edad en internet

– Lo contrario de una solución

Qué es Chat Control

Chat Control es el nombre con el que popularmente se conoce al *“Reglamento por el que se establecen normas para prevenir y combatir el abuso sexual de menores” (“Regulation to Prevent and Combat Child Sexual Abuse”, Child Sexual Abuse Regulation o CSAR)(1)*.

Una legislación que acabaría con el secreto de las comunicaciones en la Unión Europea. Se plantea aprobar durante la presidencia española de la UE y con un responsable del PP español.

Contrariamente a lo que su título indica, no hay ni una línea en esta legislación sobre cómo prevenir y combatir el abuso sexual a menores.

Propone una tecnología que es en sí una brecha de seguridad. Plantea tecnología imposible (tecnología encriptada y a la vez inspeccionable (¡!!)), invasiva y que no resuelve el problema del abuso infantil.

Establece la vigilancia masiva y anula la inviolabilidad de las comunicaciones.

Debilita la tutela judicial efectiva con extensos ámbitos no sujetos a mandato judicial, por ejemplo, el registro de espacios privados.

Ataca los sistemas distribuidos y las startups y PyMEs tecnológicas en favor de los monopolios.

Falsos positivos que pueden acusar a cualquiera inundarán los investigadores.

Es lo contrario de una solución.

La propuesta ha sido pormenorizada y duramente criticada por prensa especializada, activistas, empresas del sector y organizaciones de la sociedad civil, así como por la práctica totalidad de las asociaciones*(2)* y grupos europeos de defensa de los derechos digitales*(3)(4)(5)(6)(7)* además de por el Centro Europeo para la Democracia y la Tecnología.*(8)* También por académicos como Ross Anderson*(9)*, catedrático de Ingeniería de Seguridad del Departamento de Informática y Tecnología de la Universidad británica de Cambridge o Matthew D. Green*(10)* del Instituto de Seguridad de la Información Johns Hopkins; por empresas como Mullvad*(11)*, Tutanota*(12)* o la asociación de empresas tecnológicas alemanas Bitkom*(13)*; Servicio Científico del Parlamento Europeo*(14)*, el eurodiputado del Grupo de los Verdes y activista Patrick Breyer*(15)*, el Comité de Asuntos Digitales del Parlamento Alemán*(16)(17)(18)* o comité de la Unión Europea del Parlamento Austriaco*(19)(20)* (país donde el parlamento ha votado una resolución vinculante sobre la postura del gobierno austriaco que no aceptará la normativa si no se ajusta a los derechos fundamentales).

Principalmente por:

– Violar derechos fundamentales como el secreto de las comunicaciones o la privacidad.
– Ser técnicamente inviable.
– Ser contraproducente en la lucha contra el abuso infantil por el número de falsos.
– Por truncar la viabilidad de PyMEs tecnológicas de todo tipo y fomentar el monocultivo monopolístico digital de corporaciones tecnológicas muchas veces ni siquiera europeas.

Es una Regulación (no una directiva). Significa que es un texto que no hace falta transponer en cada país, sino que se aplica directamente en los países miembros de la Unión Europea. El 6 de julio de 2021, el Parlamento Europeo aprobó una excepción a ciertas disposiciones del Reglamento sobre privacidad y comunicaciones electrónicas (ePrivacy). Estas excepciones establecen que los proveedores de servicios de comunicaciones electrónicas sólo pueden procesar datos con el consentimiento del usuario o por motivos específicos, como la seguridad o la facturación. Esto permite a los proveedores escanear y denunciar los mensajes privados en línea que contengan material que muestre abusos sexuales a menores bajo señalamiento. Permite a las empresas aplicar tecnologías aprobadas para detectar técnicas de captación de menores*(21)(22)*. Esto fue Chat Control 1. Ahora viene Chat Control 2 que supondrá una nueva excepción en ePrivacy, estas con carácter de obligatoriedad.

La encargada del proyecto es la socialdemócrata sueca Ylva Johansson, Comisionada europea de Interior (Home Affairs) desde 2019.
El *rapporteur* es el español Javier Zarzalejos (EPP, Spain).*(23)(24)*

Recientemente se ha filtrado que el gobierno de España apoyará las posturas más extremas y conservadoras.

Extracto de la posición de España en el Consejo Europeo que presidirá a partir de junio. Documento filtrado publicado por The Wired:

(...) Idealmente, en nuestra opinión, sería deseable prevenir legislativamente que los proveedores de servicios con sede en la UE implementen cifrado de extremo a extremo (...).

(...) Estamos de acuerdo en incluir las comunicaciones de audio en el ámbito de la propuesta de CSA. Creemos que, como propuso la delegación húngara, la propuesta debería eliminar las referencias concretas a los diferentes tipos de materiales (imágenes, textos, videos o audios) y ser más general para abordar cualquier tipo de material (...).

(...) la detección automática de contenido en las comunicaciones interpersonales es clave (...)

Por qué debemos rechazar Chat Control

De qué NO habla el reglamento

En su propio título el reglamento dice establecer normas para prevenir y combatir los abusos sexuales a menores.

Pues bien, no hay ni una sola palabra sobre nada de esto en las 140 páginas de la regulación. De hecho no hay ni una sola palabra sobre nada que no sea Internet. El abuso sexual infantil aparece solo en el titulo, epígrafes o formulismos legales. La regulación va solo sobre el material de abuso sexual de menores y ni siquiera sobre su producción sino solo sobre su difusión, intercambio y almacenamiento. No es una

ley contra el abuso sexual de menores que perjudica a internet. Es solo una ley contra internet, que olvida el abuso sexual a menores salvo para justificar propagandísticamente ataques contra un Internet democrático.

La brutal influencia de lobbies conservadores, tecnófobos y con una visión de internet como un espacio que han de controlar y que tiene que ser monopolizado solo por grandes actores dominantes es evidente.

El Reglamento habla también de embaucamiento de menores (grooming en inglés) una práctica deplorable e ilegal. Sin embargo, abrazar el acercamiento al tema de los lobbies conservadores de Rusia y USA conduce, como ha conducido, a un uso indebido de legislaciones contra las minorías sexuales afectivas y de género.

Sobre los abusos sexuales a menores las estadísticas como las de la OMS*(25)* indican que la mayoría es cometida por personas conocidas por el niño o la niña, como familiares, amigos o vecinos. Una regulación que atacara de verdad los abusos sexuales a menores y el material generado con ello sería realmente urgente para dotar de medios, herramientas y marco legal a profesores, pediatras, psicopedagogos, trabajadores sociales, policías especializados y otros trabajadores en primera línea para identificar y actuar en este tipo de casos.

No hay nada sobre esto en el Reglamento.

Tampoco de otro grave problema de abuso sexual de menores en nuestra sociedad, el que se ha detectado en el ámbito de la Iglesia. La falta de una respuesta firme por parte de la UE y de sus estados miembros ha creado en las víctimas y opinión pública una considerable sensación de impunidad que este Reglamento intenta desviar.

De qué va el Reglamento

– Tecnología imposible, invasiva y que no resuelve el problema del abuso infantil

Es como si se planteara prohibir las carreteras para evitar los accidentes de coche.

Es una regulación eminentemente técnica hecha por personas sin el conocimiento necesario sobre la base de un imaginario tecnológico estereotipado, reaccionario y que no se corresponde con la realidad.

“3. Las tecnologías serán:

a) eficaces para detectar la difusión de material de abuso sexual de menores conocido o nuevo o el embaucamiento de menores, según proceda;

b) incapaces de extraer de las comunicaciones pertinentes ninguna otra información que no sea la estrictamente necesaria para detectar,

c) lo menos intrusivas posible en términos de repercusión en los derechos de los usuarios a la vida privada y familiar (incluida la confidencialidad de la comunicación), y a la protección de los datos personales;

d) lo suficientemente fiables, a fin de limitar en la mayor medida posible la tasa de errores en la detección.”

Se pide algo que no puede existir ya que violará los derechos a la vida privada y familiar. Es como decir que la policía puede entrar en casa de cualquiera sin mandato, pero prometiendo que no entrará.

Los promotores de la ley en Comisión de la UE no entienden su propia ley y los posibles efectos de la misma como han

demostrado en toda y cada una de las veces que han tenido que contestar a preguntas.*(26)*

– Establece la vigilancia masiva. Anula la inviolabilidad de las comunicaciones

Así lo indica incluso el Servicio Científico del Parlamento Europeo*(27)* en su informe sobre el reglamento de mayo del 2022. Viola los artículos 7 y 8 de la Carta de Derechos Fundamentales que prohíbe la vigilancia masiva de la población.

Tener una conversación privada es un derecho humano básico, un derecho que es especialmente vital para personas que puedan ser discriminadas o que quieran denunciar abusos.

En su redacción actual, el proyecto de ley obliga a todos los servicios de alojamiento y a los proveedores de comunicaciones interpersonales a escanear todos los contenidos y, a continuación, decidir qué entregar a las fuerzas de seguridad. Lo más probable es que pecarán de precavidos y sobreinformarán masivamente de las comunicaciones de la gente.

Lo que se plantea es que una inteligencia artificial escanee todas las comunicaciones, en particular material sexualmente explícito, incluso entre adultos, de forma general e indiscriminada para encontrar material de abusos sexuales infantiles (CSAM). Esto significa que las fotos personales y las conversaciones íntimas podrían ser recolectadas y almacenadas, lo que es una violación sin precedentes de la privacidad. Chat Control creará una enorme cantidad de información confidencial que estará en manos de empresas privadas y de la UE independientemente del estado de su

democracia, información potencialmente expuesta a filtraciones de datos, ataques cibernéticos o a ser utilizadas contra las personas.

Si un algoritmo informa de un caso sospechoso, todo el contenido del mensaje y los datos de contacto se envían automáticamente a un centro de distribución privado y, posiblemente después, a las autoridades policiales. Los usuarios afectados no reciben notificación alguna.

El sistema es fácilmente ampliable para buscar otros tipos de material, lo que podría ser utilizado por los diferentes gobiernos de la UE para espiar a sus ciudadanos.*(28)*

El Tribunal de Justicia de la Unión Europea aceptó un análisis automatizado permanente de las comunicaciones privadas sólo si se limita a los sospechosos (Caso C-511/18). Según el apartado 192 de su sentencia el análisis automático permanente y general de las comunicaciones privadas viola los derechos fundamentales. Es decir: la legislación de la UE prohíbe imponer obligaciones generales de supervisión a las plataformas por el riesgo de interferir en derechos fundamentales como la intimidad, pero la propuesta de la Comisión pretende eludir ese límite estableciendo «medidas específicas que sean proporcionadas al riesgo de uso indebido de un servicio determinado para el abuso sexual infantil en línea y estén sujetas a condiciones y salvaguardias sólidas». Aplican un requiebro que les funcionó con el copyright, pero aquí el ámbito es mucho más grave.

– Debilita la tutela judicial efectiva (demasiado extenso los ámbitos no sujetos a mandato judicial, como el registro de espacios privados)

No se requerirá una orden judicial o una sospecha inicial para buscar y recopilar los mensajes. Ocurrirá siempre y automáticamente.

Vulnera la presunción de inocencia, ya que obligan a los proveedores a tratar a todos las personas usuarias como sospechosas de distribución de imágenes de abusos sexuales a menores.

– Tecnología invasiva que es en sí una brecha de seguridad*(29)*

Las llamadas "puertas traseras" que generan los proveedores de tecnología para romper el cifrado y monitorizar toda la comunicación en las aplicaciones y en los repositorios, pueden ser y serán usadas por criminales y servicios de inteligencia extranjeros para desestabilizar nuestra sociedad.*(30)*

Los artículos 7 a 11 del Reglamento prevén que puedan dictarse órdenes de detección que obliguen incluso a los proveedores de mensajes cifrados de extremo a extremo a escanear el contenido de los mensajes privados.

¿Confiaría a Europol las fotos de sus hijos? una agencia que ya ha sido criticada por el organismo de control de protección de datos de la UE por su mala gestión de grandes conjuntos de datos.*(31)* La inocente foto que haces a tu bebé en la bañera y envías a sus abuelos podría acabar en una base de datos de las fuerzas de seguridad o, incluso, en otras manos.

– Ataca los sistemas distribuidos y las startups y PyMEs tecnológicas en favor de los monopolios.

Las grandes empresas de redes sociales a menudo ni siquiera pueden cumplir las promesas de sus propias políticas de moderación de contenidos. Es increíble que los legisladores de la UE puedan ahora obligar a cualquier empresa proveedora de servicios a utilizar sus algoritmos de vigilancia para acusar a sus propios usuarios de los peores tipos de delitos.

¿Quién podrá permitirse este despliegue? ¿Y a quién beneficia? Muy pocas Big Tech podrán proveer la tecnología e incluso utilizarla. Por otra parte, la fantasía de un internet controlado por unas pocas empresas que le son amigas es lo que hay en las fantasías de quiénes han planteado esta ley: es un ataque a la propia estructura de internet, una herramienta no centralizada y colaborativa que no debe ser controlada por unas pocas empresas poderosas que vigilan capilarmente todos los usuarios.

– Falsos positivos que pueden acusar a cualquiera inundarán los investigadores.

El Reglamento yerra por completo el tiro, ya que los delincuentes rara vez utilizan mensajeros para compartir material: son demasiado lentos para compartir grandes colecciones de CSAM.

El sistema planteado ha demostrado errar incluso con las CSAM conocidas, es decir cuando ya se conocen los rasgos o elementos que se buscan. Cuando se escanea en busca de CSAM desconocidos, incluso admitiendo el argumento falaz que un porcentaje bajo de inocentes señalados sería admisible, hará que se notifiquen falsamente miles de millones de mensajes todos los días. O sea, se colapsaría a los investigadores con millones de informes automatizados de

escasa precisión, la mayoría de los cuales son criminalmente irrelevantes, al tiempo que perjudiciales para personas inocentes.

Ya sabemos que esta tecnología es propensa a errores porque algunos servicios de grandes plataformas como Facebook, Gmail y Outlook ya usan tecnología similar en sus servicios por ejemplo para identificar desnudos cuando no está permitido en sus plataformas. Todos tenemos experiencia de su falta de precisión. Imaginad esto aplicado a vuestras conversaciones privadas.

La comisionada utiliza metáforas como usar un imán para "buscar una aguja en un pajar". Introducir el escaneo obligatorio de nuestras fotos y mensajes no les ayudará a acotar el objetivo, sino que ampliará masivamente el «pajar» tal y como indica el Servicio Científico del Parlamento Europeo*(32)* en su informe sobre el reglamento de mayo del 2022.

No protegerán a los menores, sino que pueden exponerlos en línea cuando se envían imágenes sexuales. No ayudará a los niños y generará un internet menos seguro para todos.

Los falsos positivos causan un daño real. Un ejemplo reciente publicado por el New York Times destacó un escaneo CSAM errado por parte de Google: una persona envió fotos de su hijo a la enfermera para teleasistencia. El sistema automático de Google lo etiquetó como CSAM. La persona sufrió una década de investigaciones. Según la EFF no es un caso aislado, podría haber miles así.*(33)*

Del mismo modo, la policía nacional irlandesa verificó que actualmente conserva todos los datos personales que les ha remitido el Centro Nacional para Menores Desaparecidos y

Explotados (National Center for Missing and Exploited Children-NCMEC) el principal lobby conservador y pro censura de internet en nombre de la defensa de los derechos de los niños del mundo. Estos datos incluyen los nombres de usuario, las direcciones de correo electrónico y otros datos de usuarios inocentes verificados.

– Argumentos contra la verificación de edad en internet.

No hay ninguna forma de verificación de la edad en línea que no tenga efectos negativos sobre los derechos humanos de los usuarios adultos de internet. En general, obligar a la gente a identificarse con el DNI para poder usar internet podría considerarse una limitación del derecho a la privacidad y la libertad de expresión en línea. Además sería fácilmente evitable usando una VPN.

Si se requiere que los usuarios proporcionen su información personal para acceder a los servicios en línea, podría haber además riesgos en torno a la privacidad y la seguridad de los datos personales. En la siguiente brecha de seguridad no solo se filtrarán emails y passwords, si no nuestros DNI e identidades reales que al contrario que nuestras identidades digitales, no son desechables. Por el resto de tu vida podrás ser asociado por ejemplo con tu consumo de pornografía.

El anonimato además es una herramienta básica para garantizar la libertad de expresión de periodistas, activistas, alertadores y defensores de derechos humanos y sus labores de investigación y vigilancia de las instituciones.

En resumen, exigir la identificación con DNI en internet es costoso, arriesgado, complejo, poco efectivo, invasivo para la privacidad de los usuarios y dañino para la rendición de cuentas institucional y la libertad de expresión. También

puede ser perjudicial para los derechos de aquellos que no tienen acceso a un DNI o que no desean compartir su información personal.

– Lo contrario de una solución.

Los abusos a menores son horrendos. Por eso no debemos malgastar esfuerzos en acciones que son ineficaces e incluso perjudiciales.

La mayoría de las CSAM que se distribuyen no se alojan en espacios online europeos que estarían sujetos a estas normas.

Es increíble que el planteamiento de la UE respecto al CSAM se limite al mundo online.

La falta de inversión en la protección y el bienestar de la infancia es un reto constante en toda la UE, y no todos los países miembros han adoptado siquiera leyes nacionales de protección de la infancia. Miles de víctimas se han visto privadas de justicia debido a la prescripción de los delitos o a que instituciones como la Iglesia Católica han eludido su responsabilidad.

Hay mejores formas de salvar a los niños que someter a todos los ciudadanos de la UE a una vigilancia constante.

Entre el 70% y el 85% de los niños conoce a su agresor. La gran mayoría de los niños son víctimas de personas en las que confían.*(34)* ¿Cómo va a ayudar el escaneo de CSAM en cada mensaje de chat a prevenir los abusos sexuales a menores en la familia, el club deportivo o la iglesia?

Suponiendo que los delincuentes utilicen mensajería mainstream y no foros de nicho y que exista una tecnología mágica – genial, hemos reducido la distribución de CSAM en

una pequeña fracción. ¿Y ahora qué? Bueno, sólo porque se distribuya menos CSAM en línea, no significa que el CSA se detenga fuera de línea – tal vez se reduzca, definitivamente pero no se detiene. En 4/5 casos, los niños son abusados por alguien cercano a ellos.*(35)* Para atrapar realmente a los abusadores se necesita mecanismos de denuncia rápidos y sencillos, la capacidad de las fuerzas de seguridad en términos de personal y recursos financieros para localizar a los autores y productores, abordar la raíz del problema, no algoritmos.

Firmado:

Xnet

Éticas

Interferencias

Guifi

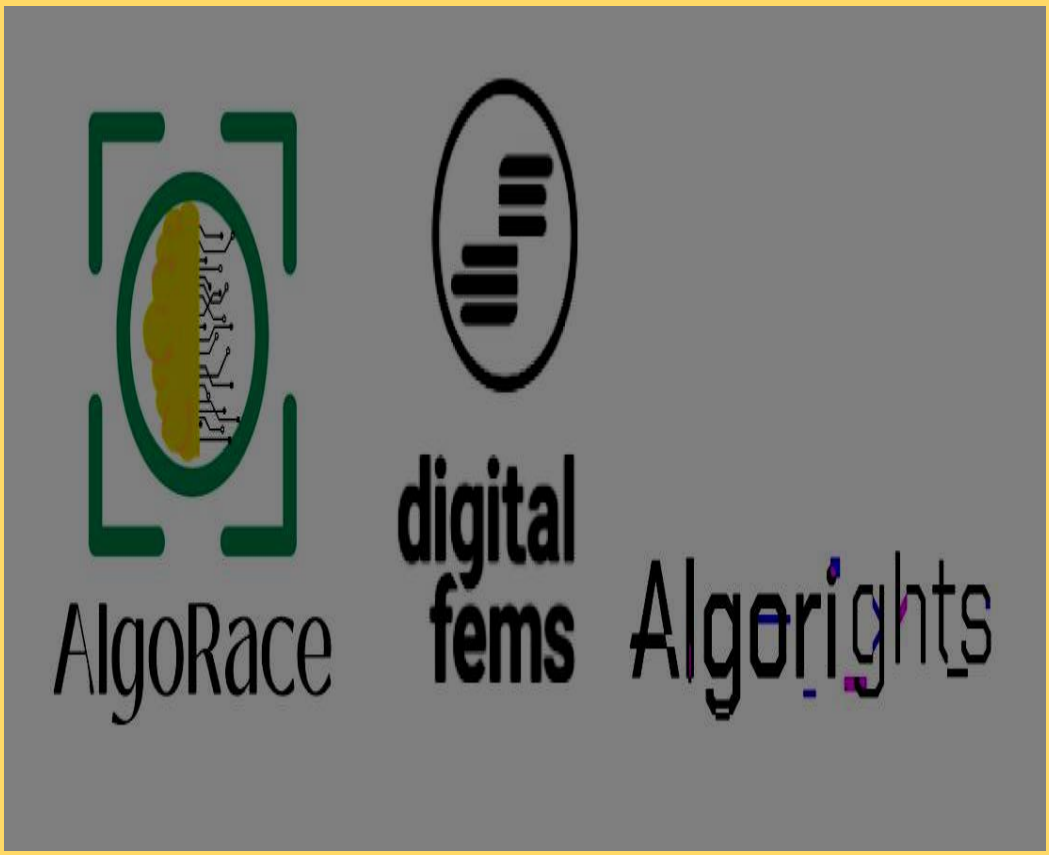
Political Watch

The Commoners

DigitalFems

AlgoRace

Algorights



Textos a tener en cuenta

– El reglamento

https://eur-lex.europa.eu/legal-content/ES/TXT/DOC/?uri=CELEX:52022PC0209&from=EN

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1232

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3 AFIN

– La consulta

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Child-sexual-abuse-online-detection-removal-and-reporting-/public-consultation_en

– La visión de la UE

https://home-affairs.ec.europa.eu/whats-new/campaigns/legislation-prevent-and-combat-child-sexual-

abuse_es

https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976

_____

(1)
https://en.wikipedia.org/wiki/Regulation_to_Prevent_and_Combat_Child_Sexual_Abuse
(2)
https://stopscanningme.eu/en/
(3)
https://netzpolitik.org/2021/eu-commission-why-chat-control-is-so-dangerous/
(4)
https://en.epicenter.works/content/chat-control-a-good-day-for-privacy
(5)
https://fsfe.org/news/2022/news-20221026-02.en.html
(6)
https://freiheitsrechte.org/en/themen/digitale-grundrechte/chatkontrolle
(7)
https://prostasia.org/blog/europes-chat-control-mandate-begins/
(8)
https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data
(9)
https://www.cl.cam.ac.uk/~rja14/Papers/chatcontrol.pdf
(10)
https://twitter.com/matthew_d_green/status/152420840205806

7974
(11)
https://mullvad.net/en/chatcontrol
(12)
https://tutanota.com/blog/posts/chat-control
(13)
https://www.bitkom.org/EN/List-and-detailpages/Publications/Statement-on-Chat-Control-and-the-Right-to-Encryption
(14)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0209
(15)
https://www.patrick-breyer.de/en/posts/chat-control/
(16)
https://prostasia.org/blog/europes-chat-control-mandate-begins/
(17)
https://www.bundestag.de/dokumente/textarchiv/2023/kw09-pa-digitales-928540
(18)
«los planes, que incluyen el uso de tecnologías como el escaneado del lado del cliente (CSS), fueron recibidos con críticas desde muchos sectores, lo que también se reflejó en las evaluaciones de los expertos: la mayoría de los expertos invitados subrayaron que el proyecto [iba] demasiado lejos en puntos cruciales.»
(19)
https://www.parlament.gv.at/dokument/XXVII/SA-EU/1/00870/TO_14694232.html
(20)
https://epicenter.works/document/4393

(21)
https://www.euractiv.com/section/data-protection/news/new-eu-law-allows-screening-of-online-messages-to-detect-child-abuse/
(22)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0568
(23)
https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-combating-child-sexual-abuse-online
(24)
https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf
(25)
https://www.who.int/es/news-room/fact-sheets/detail/child-maltreatment
(26)
https://mullvad.net/en/blog/2023/3/28/the-european-commission-does-not-understand-what-is-written-in-its-own-chat-control-bill/
(27)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0209
(28)
https://mullvad.net/en/chatcontrol/stop-chatcontrol
(29)
https://maxim.tips/chatcontrol/#todo
(30)
https://www.patrick-breyer.de/en/world-encryption-day-lawmakers-warn-against-eu-attack-on-secure-encryption-and-confidential-digital-correspondence/

(31)
https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data
(32)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0209
(33)
https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html
(34)
https://data.consilium.europa.eu/doc/document/ST-9068-2022-ADD-1/en/pdf#page=253
(35)
https://data.consilium.europa.eu/doc/document/ST-9068-2022-ADD-1/en/pdf#page=253

Últimos posts sobre:

Derechos digitales, datos, IA y neutralidad de la Red

- **Nuestro Plan de #DigitalizaciónDemocrática se une a Open Future y Commons Network para infraestructura democrática en la UE**
- **5º aniversario del RGPD**
- **#ChatControl – Lanzamos campaña contra la ley de monitorización automatizada de las conversaciones íntimas de la ciudadanía europea**
- **Xnet organiza evento en el Parlamento Europeo: Propuesta para una Digitalización Soberana y Democrática de Europa**

- **Acto de reconocimiento en el Ayuntamiento de Barcelona a los centros educativos co-creadores de nuestra plataforma DD**

Luchas por las libertades civiles. Redes nacionales e internacionales

- **#ChatControl – Lanzamos campaña contra la ley de monitorización automatizada de las conversaciones íntimas de la ciudadanía europea**
- **230 entidades nos posicionamos contra la propuesta de legislación UE sobre registro de financiación extranjera**
- **Presentamos una declaración promovida por @amnesty al #GlobalDigitalCompact junto con otras 54 orgs de la sociedad civil**
- **Celebramos una victoria anti-SLAPPs en UK**
- **Nada que**

#ChatControl - Monitorización automatizada de las conversaciones íntimas de la ciudadanía europea. Muy pronto en sus dispositivos.

Seremos claros: Chat Control, nombre con el que popularmente se conoce al 'Reglamento europeo para prevenir y combatir el abuso sexual de menores', NO es una regulación contra el abuso sexual de menores que perjudica a Internet. Es solo una regulación contra Internet, que olvida el abuso sexual de menores, excepto para usar propagandísticamente para justificar sus desvaríos.

Los otros miembros de la coalición son:
Éticas, Interferencias, Guifi, Political Watch y The Commoners