CHAT CONTROL

Escrito y editado por el colectivo tecnopolítico TeknoKasa
Diciembre de 2025. Madrid.

teknokasa@sindominio.net || teknokasa.csolarosa.net

Los estados y grandes monopolios digitales quieren saber qué se dice y quién lo dice excusándose en la lucha contra contra el abuso sexual en menores. Quieren tener el control total sobre las aplicaciones de mensajería, correo electrónico y contenido en la nube, saltándose el cifrado de extremo a extremo y sin tener en cuenta los riesgos asociados y la falta de proporcionalidad.

El pasado 15 de noviembre se dio el primer paso en la aprobación de ChatControl en la Unión Europea. Una regulación que, escudándose en la protección de les niñes online, pretende acabar con el anonimato en Internet y la privacidad en las comunicaciones.

Esta regulación no viene sola, se da en un contexto de ofensiva legal contra la privacidad y los derechos políticos en Internet (de expresión, asociación, confidencialidad de las comunicaciones...), en todo el bloque geopolítico occidental (que hasta ahora señalaba este tipo de medidas en sus adversarios como autoritarias). Esta ofensiva puede tener muchas excusas, desde la protección de la infancia, la lucha contra el terrorismo, las fake news, las amenazas híbridas o la criminalidad. Hoy está claro que el verdadero motivo es blindar los intereses económicos y geopolíticos de nuestras clases poseedoras controlando, silenciando y reprimiendo toda expresión, asociación y acción antagónica.

Esta ofensiva viene a sumarse a otras formas de control como la proliferación de cámaras en cada esquina de nuestros barrios, una presencia policial cada vez mayor con decenas de infiltraciones en movimientos sociales, el espionaje legal y alegal a través de grandes plataformas como Google y Meta, o el uso de software espía por parte de los Estados.

La excusa hoy es el abuso infantil, sin embargo, la verdadera motivación la podemos leer todos los días en la prensa y en los propios discursos de los representantes políticos de la UE y la OTAN: vivimos en un mundo en crísis donde ya suenan los tambores de guerra, donde debemos aceptar unas condiciones de vida cada vez mas miserables y, al mismo tiempo, ser poblaciones disciplinadas, dispuestas a luchar y morir por defender los intereses de nuestras oligarquías frente a sus antagonistas.

Sin embargo, producir estas poblaciones disciplinadas no es sólo una tarea ideológica, sino que requiere del endurecimiento de la represión y el control social sobre quienes defiendan intereses contrarios a los suyos. Por ello se atacan dos pilares de la organización y la acción política independiente de sus intereses: la privacidad, es decir, el control de un sujeto (individual o colectivo) sobre la información que produce y a quien llega; y la comunicación, es decir, la capacidad de llegar a la gente con un mensaje propio. En otras palabras, los estados quieren tener la máxima información o inteligencia sobre nosotres, pero que la población tenga el mínimo de información o comunicación por nuestra parte.

NEO-EUROPE IS ABOUT TO E.X.P.L.O.D.E

GUÍA PARA LA VIGILANCIA MASIVA

Esta ofensiva no es la primera, sino que sigue la estela de otras que siguen un patrón similar:

1. Azuzar a la población señalando o creando un problema en el que la amplia mayoría esté de acuerdo y decir que hay que luchar contra ello
2. Señalar a un grupo de culpables al que pocos defenderán
3. Construir herramientas de vigilancia y represión hacia este grupo, de tal forma que sean ampliables a cualquier otro objetivo.
4. Ampliar estos sistemas de vigilancia a otros grupos una vez que la infraestructura ya está construida y funcionando.

Además, una vez que estos sistemas se implementan y normalizan es muy dificil echarlos atrás. Por ejemplo, con el pretexto del terrorismo tras el 11S en Estados Unidos se aprobó la Patriot Act en 2001, que legalizaba las órdenes de registro sin notificación (Sneak and Peak warrants) o la búsqueda en registros privados por terceros: financieros, médicos, uso de internet, compras, viajes... Esta pérdida de privacidad y de derechos no sólo sigue vigente, sino que sirvió de paso previo para el despliegue del programa de espionaje masivo PRISM, amparado en la Protect America Act de 2007.

Otro ejemplo lo tenemos en Reino Unido, donde se implementó un ID para regular la inmigración. Ahora necesitas un identificador para conseguir un trabajo y está vinculado a cualquier movimiento que hagas.

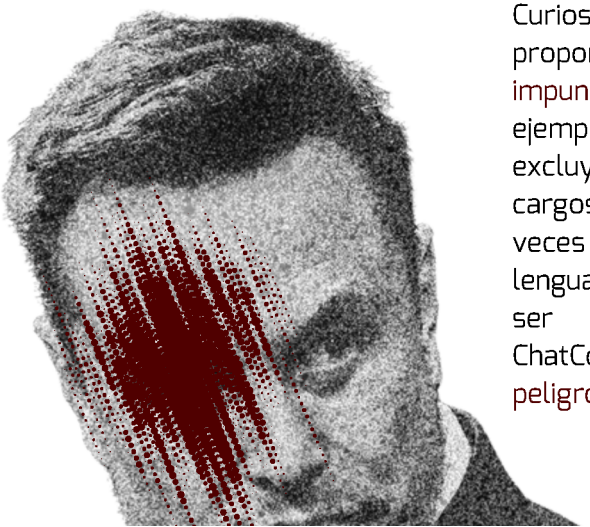
Siempre se empiezan con excusas de asuntos urgentes. Siempre terminan como sistemas de vigilancia y control permanentes. ChatControl no será una excepción, y allanará el camino de la estrategia ProtectEU, que busca que los sistemas de cifrado tengan una puerta trasera que permita a las autoridades europeas acceder a todo tipo de información privada.

QUÉ ERA CHATCONTROL

Desde su introducción en 2022, ChatControl iba a ser un sistema de vigilancia masiva con:

1. Escaneo local: sistemas de escaneo de todos los mensajes antes de ser enviados en comunicaciones encriptadas de punto a punto.
2. Hashes perceptuales en contenido multimedia: gracias a ciertos algoritmos se pueden establecer conexiones entre, por ejemplo, fotos censuradas y fotos sin censurar, o audios sin filtro y audios con filtros de voz.
3. Clasificadores IA: se usarían inteligencias artificiales para clasificar toda esta información escaneada.

Esto introduciría una "puerta trasera" enorme a todas nuestras comunicaciones privadas, creando de facto una forma para que los gobiernos y las empresas pudieran conocer todos nuestros mensajes instantáneamente. En seguridad informática es conocimiento común que las comunicaciones seguras y privadas no pueden tener una excepción. Una excepción conlleva la posibilidad de una brecha de seguridad siempre, y, por lo tanto, la introducción de actores maliciosos en nuestras comunicaciones (a parte de los gobiernos y las empresas).



Curiosamente, las oligarquías que proponen ChatControl seguirían impunes. Antes con Epstein, por ejemplo. Ahora, ChatControl excluye a políticos y otros "altos cargos". Nótese aquí muchas veces la falta de claridad en el lenguaje de esta propuesta. Parece ser que los que proponen ChatControl son conscientes del peligro que conlleva.

QUÉ ES CHATCONTROL

El 14 de octubre el gobierno Danés impulsó ChatControl en el Consejo de la Unión Europea. Por falta masiva de apoyo y ante la preocupación global, ChatControl no salió adelante.

Parece que se ha llegado al acuerdo de no introducir el escaneo local de mensajes encriptados. Esto es una victoria parcial, porque han cambiado de nuevo la propuesta de ley con los siguientes puntos:

1. Escaneo "voluntario" de mensajes que no están cifrados de punto a punto a gusto de las plataformas que ofrezcan sus servicios.
2. "Medidas de mitigación". Ahora ChatControl obligará a los proveedores a tomar "todas las medidas posibles para reducir el riesgo en sus servicios". Es tan vago como suena.

Estas medidas son contradictorias. Un escaneo voluntario no es compatible con llevar a cabo todas las medidas posibles de prevención de riesgos.

VERIFICACIÓN DE EDAD

Las "medidas de mitigación" incluirían la verificación de edad de todas las personas usuarias antes de permitir el acceso a las plataformas. Los métodos aquí son invasivos de facto, e incluyen cosas como la verificación de documentos oficiales, escaneos biométricos o sistemas algorítmicos de "estimación de edad". La verificación de edad, presentada como una forma de proteger a la infancia, genera en la práctica nuevas formas de vigilancia, censura y exclusión digital.

Sin importar el método, todos tienen algo en común: exigen a las personas entregar información personal extremadamente sensible que vincula su identidad real con su actividad en internet. Una vez recogidos, estos datos pueden filtrarse, ser pirateados o reutilizarse con fines distintos a los originales.

No se trata de un riesgo teórico. Casos recientes demuestran que la verificación de edad es incompatible con la privacidad. Por ejemplo, una investigación periodística reveló que una importante empresa de verificación de identidad, AU10TIX, dejó información sensible expuesta durante más de un año, permitiendo acceder a datos sensibles de personas que habían subido documentos oficiales. Entre la información potencialmente accesible se incluían nombres, fechas de nacimiento, nacionalidad, números de identificación y copias de documentos como carnés de conducir. Plataformas muy conocidas han utilizado servicios de este tipo para verificar identidades. La experiencia demuestra que, una vez que se obliga a subir documentos oficiales para acceder a contenidos en línea, la exposición de esos datos no es una cuestión de "si ocurrirá", sino de "cuándo ocurrirá".

Además, la verificación de edad mediante escaneos faciales y tecnologías similares añade riesgos adicionales. Estas herramientas son inquietantes para empezar, pero también inexactas y discriminatorias, y normalizan el uso de sistemas biométricos que pueden reutilizarse para inferir identidad, género, etnia, emociones o supuestas intenciones. En manos de instituciones poderosas, estos sistemas pueden provocar exclusión injusta, vigilancia masiva y daños reales a personas inocentes.

Las filtraciones de datos derivados de estos sistemas pueden dar lugar a suplantación de identidad, estafas, chantaje o pérdida del anonimato. Obligar a las personas a subir documentos gubernamentales —algunos de los datos más sensibles que existen— perjudica a toda la población usuaria. Si estas leyes se generalizan, no sería extraño que, en poco tiempo, una misma persona se viera forzada a compartir su documento de identidad con múltiples empresas distintas sólo para poder participar en la vida digital.

Una cosa está clara: los sistemas de verificación de edad son, en esencia, sistemas de vigilancia. Una vez entregados tus datos, no puedes controlar qué hacen con ellos las empresas y los gobiernos.

LA EXCUSA

Pese a todo esto, podemos aún hacernos la pregunta: ¿responde al menos a un interés sincero en la lucha contra el abuso sexual infantil? Para responder a esta pregunta basta con observar la respuesta del Estado a este tipo de abusos.

En primer lugar, según Save The Children el 60% de la violencia sexual infantil se da en el ámbito familiar, siendo el agresor el padre en un 24% de los casos, el 18% la pareja de la madre, el 4,69 % a la expareja de la madre y el 12,2 % al abuelo. Sin embargo, en muchos de estos casos se utiliza el presunto Síndrome de Alienación Parental para desacreditar el testimonio de les niñes cuando la madre denuncia abusos hacia le menor por parte del padre en lugar de otorgar credibilidad a las pruebas físicas y declaraciones de las criaturas. Así, queremos destacar que el primer espacio social en el que se dan este tipo de abusos es la familia, y que en este ámbito existe una gran desprotección a les niñes frente a los sesgos machistas e ideológicos del aparato judicial.

Por otra parte, en casos tan notorios como el de los empresarios pederastas de Murcia o el de la red explotación sexual de Epstein encontramos una ausencia total de justica, demostrando cómo ser rico permite realizar este tipo de abusos, mientras que los abundantes casos de explotación sexual de menores tutelades muestran cómo la exclusión es uno de los mayores factores de riesgo para sufirlos.

Estos casos nos muestran que el interés de los Estados por la infancia es sólo una excusa, pues actúan de manera negligente allí donde tienen una responsabilidad de cuidado y de justicia, y, en lugar de invertir más recursos en las causas de esta lacra, los invierten en sistemas de vigilancia masiva ineficaces para combatirla.

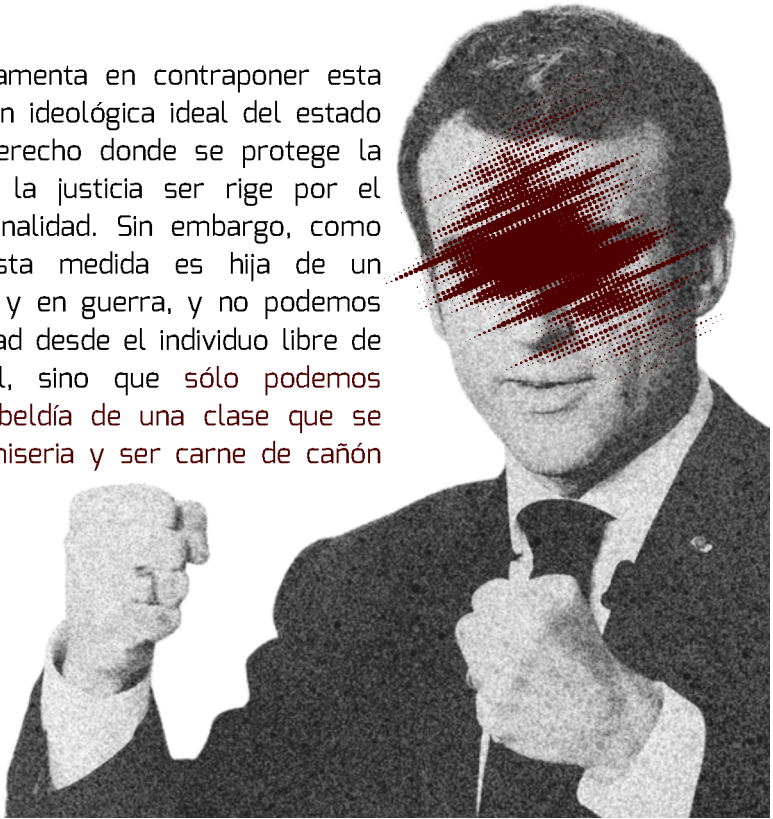
QUÉ HACER

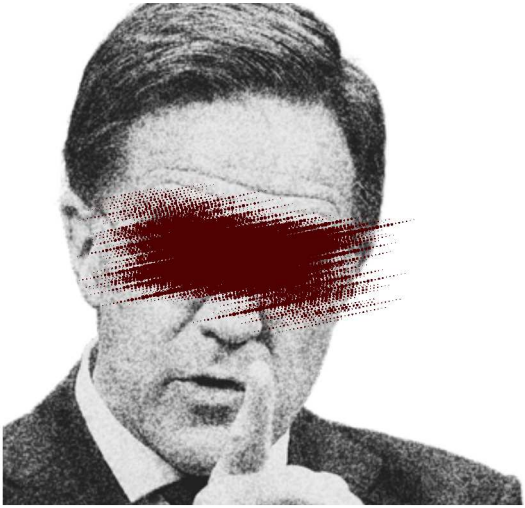
Ante todo esto no queremos quedarnos en el catastrofismo distópico o la denuncia impotente, sino preguntarnos qué se está haciendo al respecto, qué limites tiene y qué proponemos al respecto.

El primer recurso que encontramos respecto a ChatControl es la web fightchatcontrol.eu, impulsada por Patrick Breyer, exeurodiputado por el Partido Pirata Europeo. Esta web realiza un seguimiento de esta reforma, su avance burocrático y los estados y eurodputados que se posicionan a favor, en contra o indecisos.

A nivel práctico, esta plataforma propone una estrategia de lobby ciudadano, y nos invita a escribir mails a nuestros eurodiputados como medida de presión ciudadana. Además, propone un argumentario sobre la falta de proporcionalidad, los riesgos de seguridad, el socavamiento de la democracia, la ineficiencia técnica y frente al problema del abuso sexual infantil y el impacto en nuestra economía.

Esta crítica se fundamenta en contraponer esta medida con la imagen ideológica ideal del estado democrático y de derecho donde se protege la libertad individual y la justicia ser rige por el criterio de proporcionalidad. Sin embargo, como hemos señalado, esta medida es hija de un capitalismo en crisis y en guerra, y no podemos enfrentar su necesidad desde el individuo libre de un capitalismo ideal, sino que sólo podemos hacerlo desde la rebeldía de una clase que se niega a vivir en la miseria y ser carne de cañón disciplinada.





Por otra parte, encontramos planteamientos estratégicos tecnosolucionistas, bien desde el propio movimiento hacker defendiendo el uso de tecnologías federadas, P2P, de Software Libre, autohosteadas o simplemente más seguras que podrían permitir evadir este control, o bien desde entornos empresariales que te quieren vender su producto.

Aunque como colectivo consideramos fundamental promover buenas prácticas de seguridad, herramientas seguras y la construcción de infraestructuras propias, creemos que plantear esto como estrategia y no como táctica de resistencia es erróneo. Por un lado, porque es asumir la derrota y entrar en clandestinidad sin siquiera dar batalla y, por el otro, porque como movimiento no tenemos la capacidad de extender estas herramientas, no ya a la sociedad en general, sino ni siquiera a la militancia ya organizada.

Sobre esto queremos aclarar que no hacemos estas críticas desde fuera, sino que creemos que estos planteamientos estratégicos vienen de nuestros propios límites como movimiento hacker, que se derivan de nuestra escisión respecto a otros movimientos. En general, somos espacios de gente técnica para gente técnica, centrados en nuestras propias necesidades e intereses y por tanto desvinculados de los de otros espacios, pues aunque pensemos proyectos o herramientas útiles para otros, carecemos de la capacidad de socializarlos.

Por ello, plantear esta lucha para nosotres no tiene que ver sólo con plantear una lucha que nos parece importante, sino que tiene un sentido estratégico de ponernos frente al espejo de que mientras persista esta escisión seremos impotentes frente a la ofensiva actual contra la privacidad. Por tanto, queremos iniciar esta lucha desde el deber, pero también del deseo, de enfrentar este límite, de desarrollar vínculos y alianzas con otros movimientos que nos hagan más fuertes y de desarrollar capacidades políticas, de comunicación y de movilización de las que carecemos actualmente.

Así, las hipótesis que queremos plantear sobre Chat Control son las siguientes:

1. Que esta lucha no la debemos enfrentar desde el tecnosolucionismo ni desde el lobby ciudadano, sino desde la lucha política por que este reglamento no se pueda aprobar.

2. Que el sujeto de esta lucha deben ser los movimientos sociales y las organizaciones de clase. En primer lugar, por necesidad, pues sus libertades políticas están en cuestión con esta medida; en segundo, por capacidad, pues son quienes ya tienen capacidad de movilización, organización y comunicación.

3. Que en la medida en que este sujeto no existe debemos atravesar tres fases en esta lucha: una primera de coordinación de los colectivos, organizaciones y movimientos que quieran participar de esta lucha; una segunda de comunicación o de campaña, para hacer llegar este problema más allá de nuestros círculos inmediatos; y una tercera de movilización, que demuestre y movilice el rechazo a esta medida.

En estas tareas queremos destacar que no empezaríamos de cero, sino que ya hay trabajo realizado al respecto. Por una parte, desde la Coordinadora de Informática de la CGT se sacó la campaña nochatcontrol.org, con un manifiesto al que os invitamos a adheriros. Por otra, a nivel comunicativo dentro de nuestros círculos El Salto y Pantube han hecho cierto trabajo al respecto.

Sin embargo, creemos que a estas iniciativas aún les ha faltado cierta masa crítica y es a lo que queremos contribuir con este texto. Por ello os animamos a discutir nuestra propuesta y a construir con nosotres y quienes ya están en ello, un frente común contra Chat Control y en defensa de la privacidad.

LICENCIA PARA ESPIAR