EU stemt over controle privé-berichten chatapps

14 oktober 2025

Het is moeilijk voor te stellen, maar een nieuwe Brusselse wet doet precies wat de in de DDR gehate STASI ook deed: alle persoonlijke correspondentie openen. Wat toen nog in gesloten enveloppe zat, zit nu in encrypt berichtenverkeer. Met het volledige scannen van alle privé-communicatie is de Europese burger terug in de DDR.

Foto: Burgers van de DDR demonstreren voor meer vrijheid (EZAZ/STASI Museum Berlijn)

UPDATE 14 oktober 2025
Voorlopig geen chatcontrol EU. Te veel landen willen geen chat control. Om gezichtsverlies te vermijden werd de stemming in de EU geannuleerd. In december wil de EU-commissie het nog een keer proberen in de raad van ministers. Lees het artikel.

Terug naar de DDR

Bij rondleidingen door het STASI-Museum in Berlijn overheerst verbazing en verontwaardiging over de alles en iedereen bespionerende STASI, de staatsveiligheidsdienst van de toenmalige DDR (Oost-Duitsland). Beelden van tientallen taperecorders die vertrouwelijke gesprekken tussen burgers opnamen en machines die met stoom alle dichtgeplakte enveloppen openden, STASI-medewerkers die de geopende brieven kopiëren. Hoe kon dat hebben bestaan?

Met de voorgestelde EU-wet voor het scannen van privé-berichtenverkeer via diverse grotere chatplatforms wordt echter de werkwijze van de STASI in ere hersteld: alle correspondentie wordt op digitale wijze 'geopend' (van encryptie ontdaan) en gescand. Daarmee wordt op 'moderne' wijze het digitale briefgeheim beëindigd.

"Elke foto, elk bericht, elk bestand dat u verstuurt wordt automatisch gescand—zonder uw toestemming of verdenking. Dit gaat niet over het vangen van criminelen. Het is massasurveillance opgelegd aan alle 450 miljoen burgers van de Europese Unie", stelt de website Fight Chat Control. De scanning vindt bij iedereen plaats. Een heldere verdenking van een (voorgenomen) misdrijf is niet nodig, toch een van de fundamenten van een rechtsstaat.

Als reden wordt genoemd het bestrijden van kinderporno en andere vormen van criminaliteit. Maar wie even doordenkt realiseert zich dat de smerige wereld van de kinderhandel zich echt niet afspeelt bij de grote chatplatforms als Whatsapp, Signal of Telegram. Die zullen te vinden zijn op het Dark Web of hebben hun andere communicatiekanalen.

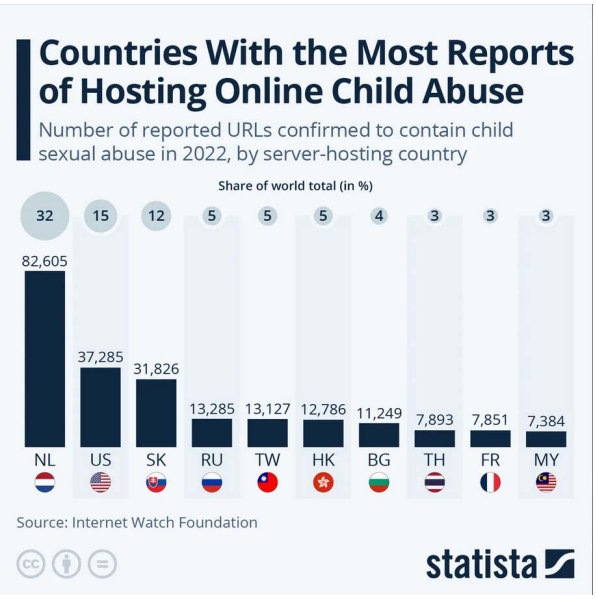
De reden is dan ook flauwekul en een voorwendsel om alles en iedereen te volgen, de data te verzamelen, af te leveren bij AI-bedrijven als Palentir en zo politieke of psychologische profielen op te stellen.

“Automatische scanners identificeren routinematig onschuldige inhoud, zoals vakantiefoto’s of privégrappen, als illegaal, waardoor gewone mensen het risico lopen van valse beschuldigingen en onderzoeken worden geschaad”, gaat Fight Chat Control verder.

Een medewerker van de STASi opent brieven van DDR-burgers en maakt een kopie.

Nederland koploper hosting van verboden kindermateriaal

Volgens het Duits statistisch bureau Statista host Nederland 32% van de mondiale kinderporno op haar servers. Het gaat daarbij om getelde URL’s die naar Nederland leiden, maar liefst 82.605. Het is niet verrassend dat Nederland ook hoog scoort bij de productie van dat materiaal.



Verklaring voor deze Nederlandse positie is de uitgebreide en internationaal goed verbonden internet-infrastructuur. Maar zeker ook de als liberaal bekendstaande Nederlandse cultuur. Toch verbaast het dat niemand, niet in Den Haag, noch in Brussel de behoefte voelt om in actie te komen. Statista weet klaarblijkelijk exact hoe het zit, maar deze kennis lijkt onbenut.

In plaats van de bron van deze smerige industrie aan te pakken, wordt het fenomeen aangrepen om ieders digitale privé post te openen. De wens tot totale controle over wat de burger denkt en uit lijkt eerder de reden.

Wat zegt AI lumo.proton.me?

Client-side scanning (CSS) is een techniek waarbij de software die op jouw apparaat draait – bijvoorbeeld een e-mail-client, cloud-opslagapp of chat-programma – automatisch de inhoud van bestanden, berichten of andere data analyseert voordat die naar een server wordt verzonden.

Het doel kan variëren:
– **Malware-detectie** – schadelijke code opsporen zodat deze niet wordt geüpload.
– **Content-moderatie** – expliciete of illegale materialen (bijvoorbeeld kindermisbruikmateriaal) detecteren om wettelijke verplichtingen na te komen.
– **Spam- en phishing-filtering** – verdachte patronen herkennen om ongewenste berichten te blokkeren.

De scan gebeurt lokaal, dus de ruwe data verlaten je apparaat niet eerst; alleen een **hash-waarde**, een **signatuur** of een **alert** wordt eventueel naar de server gestuurd. In sommige implementaties (bijv. bij bepaalde grote tech-bedrijven) kan

echter ook een **geëncrypteerde versie** van de data worden geüpload voor verdere analyse, wat de privacy-implicaties vergroot.

Hoe kun je client-side scanning voorkomen of beperken?

1. **Kies privacy-gerichte software**

Diensten die zero-knowledge encryptie bieden (zoals Proton Mail, Proton Drive, of andere end-to-end versleutelde oplossingen) voeren doorgaans geen client-side scans uit, omdat de provider de inhoud nooit kan lezen.

2. **Schakel optionele scans uit**

Veel programma's hebben een instelling voor "malware-scan" of "content-moderatie". Controleer de voorkeuren of instellingen-menu's en zet die functie uit als je er zeker van wilt zijn dat er geen lokale analyse plaatsvindt.

3. **Gebruik offline-tools**

Werk met applicaties die volledig offline blijven (bijv. een lokale teksteditor of een zelf-gehoste mailserver). Zonder netwerkverbinding kan er geen data naar een externe scanner worden gestuurd.

4. **Beperk rechten van de applicatie**

Op mobiele apparaten kun je vaak per app bepalen welke bestands- en netwerkmachtigingen ze hebben. Door een app alleen toegang te geven tot de bestanden die je echt nodig hebt, verklein je de kans dat er onbedoeld gescand wordt.

5. **Controleer de broncode of audit-rapporten**

Open-source projecten laten je toe de code te inspecteren. Als je technisch onderlegd bent, kun je zoeken naar bibliotheken die scannen (bijv. ClamAV-integraties) en deze verwijderen of vervangen.

6. **Gebruik een VPN of Tor**

Hoewel dit de scan zelf niet uitschakelt, verbergt het je IP-adres en maakt het lastiger om je verkeer te koppelen aan een specifieke gebruiker, waardoor eventuele server-side correlaties minder effectief zijn.

7. **Encryptie vóór de scan**

Sommige gebruikers passen een extra laag encryptie toe (bijv. met VeraCrypt-containers) *voordat* ze bestanden openen in een app die CSS gebruikt. De scanner ziet dan alleen willekeurige data en kan niets betekenisvol detecteren.

Praktische overwegingen

1. **Wettelijke verplichtingen** – In bepaalde rechtsgebieden (bijv. de EU-richtlijn voor digitale diensten) kunnen providers verplicht zijn om

kindermisbruikmateriaal of ander illegaal materiaal te detecteren. Zelfs als je de scan lokaal uitschakelt, kan de dienst alsnog een server-side controle uitvoeren zodra je iets uploadt.
2. **Balans tussen veiligheid en privacy** – Malware-scanners kunnen je beschermen tegen ransomware of andere bedreigingen. Het volledig uitschakelen ervan kan je blootstellen aan risico's, vooral als je regelmatig onbekende bestanden downloadt.
3. **Transparantie van de provider** – Controleer de privacy-policy en technische documentatie van de service die je gebruikt. Proton-diensten, bijvoorbeeld, benadrukken dat ze geen client-side scanning uitvoeren op hun gratis of betaalde plannen.

Samenvatting
Client-side scanning analyseert data lokaal om malware, illegale content of spam te detecteren. Je kunt het voorkomen door privacy-gerichte (zero-knowledge) tools te gebruiken, optionele scans uit te schakelen, offline te werken, app-rechten te beperken, open-source code te auditen, en extra encryptie toe te passen. Houd wel rekening met wettelijke eisen en de mogelijke veiligheidsimpact van het uitschakelen van dergelijke scans.

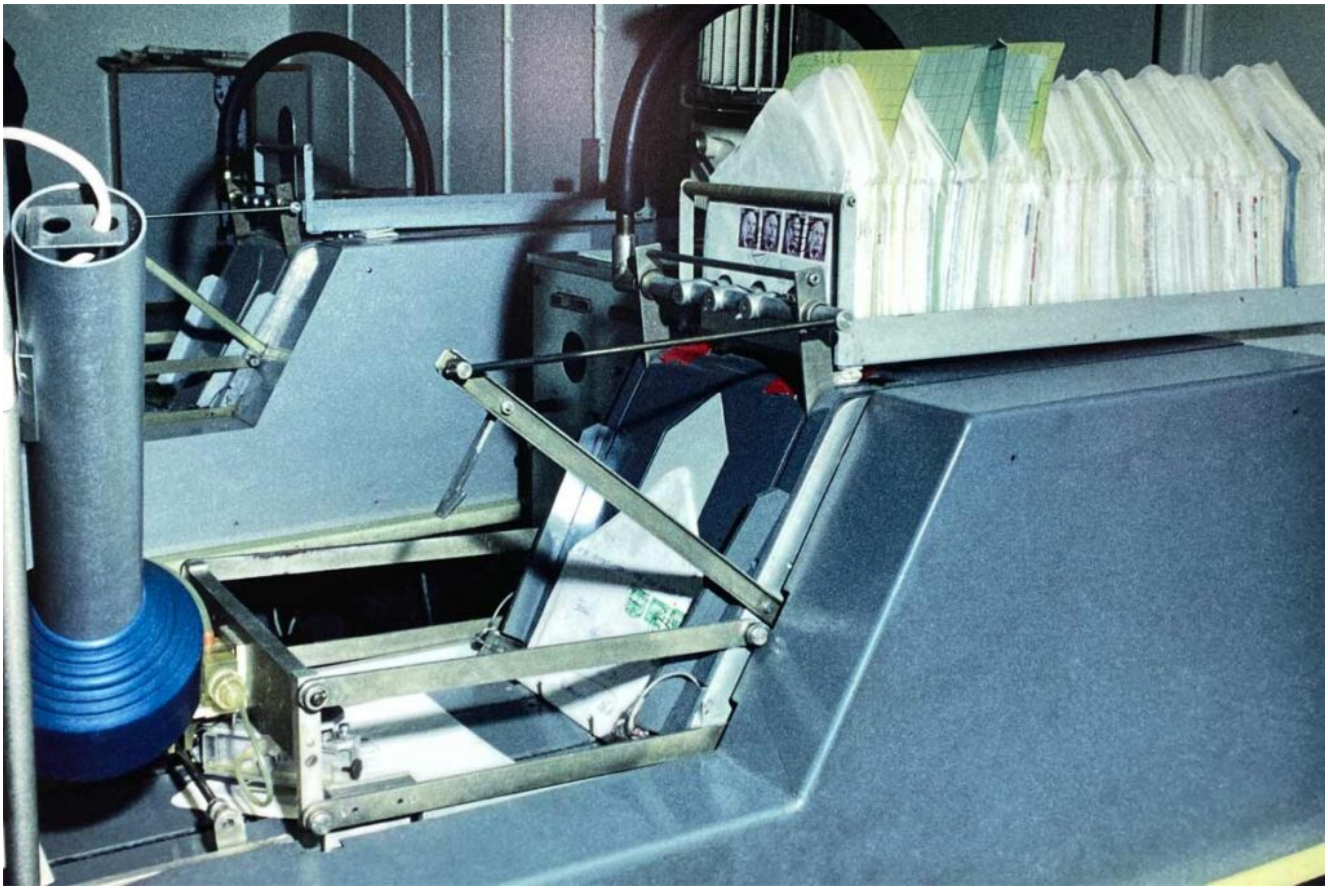
Europarlementariërs uitgezonderd

We kennen het uitzonderingsprincipe van de voorgestelde herziening van de Nederlandse pensioenwet: de risicovolle overgang geldt voor iedereen, behalve voor de leden van het parlement.
Met deze wet is het niet anders. Volgens Fight Chat Control blijven de chats van Europarlementariërs buiten de scan. Hun berichten blijven vertrouwelijk, die van bijna 500 miljoen Europese burgers niet. Het maakt het voor de parlementariërs een stuk eenvoudiger om met deze wet in te stemmen.

Landen die vóór deze wet zijn: Bulgarije, Kroatië, Cyprus, Denemarken, Frankrijk, Hongarije, Ierland, Italië, Letland, Litouwen, Malta, Portugal, Slowakije, Spanje en Zweden.
Opmerkelijk is hierbij dat een aantal landen die voor uit Nederland vertrekkenden als 'veilig' worden beschouwd voor de uitwassen van deze resettijd: denk aan Portugal, Kroatië of Zweden, dus vóór deze wet zullen stemmen.

Tegen zijn, naast Nederland, Oostenrijk, België, Tsjechië, Finland en Polen.

Nog twijfelend zijn: Estland, Duitsland, Griekenland, Luxemburg, Roemenië en Slovenië.



Automatische enveloppe-opener in gebruik bij de STASI (STASI-Museum Berlijn)

Scannen zonder verdenking ook gevaar voor bedrijfsleven

De toch al gaande uittocht van Europese bedrijven, kan met deze maatregel verder worden versneld. Immers ook geheimen rond innovaties of financiële situatie moeten binnen de Europese Unie 100% veilig gecommuniceerd kunnen worden. Als encryptie eenmaal wordt gebroken, staat de deur open voor criminelen om binnen te glippen. Helaas zijn ook overheden niet vies van bedrijfsspionage. Zo werd bekend dat de Amerikaanse overheid meekeek met interne communicatie binnen Airbus, de grote Europese concurrent van de Amerikaanse Boeing.

Met het zo onbeschaamd terzijde schuiven van het mensenrecht op privacy, is

alles geoorloofd. Denk aan de miljarden camerabeelden (met gezichtsherkenning) die overheden en bepaalde bedrijven beheren.

Tegenstanders vrezen dat de gegeven reden, bestrijding verspreiding kinderporno, als dat al de echte reden is, snel uitgebreid wordt met nieuwe redenen. Zo wordt de Digital-ID in het Verenigd Koninkrijk niet alleen tegen illegale immigratie ingezet, waarschijnlijk een vals voorwendsel, maar nu ook nodig om aan het werk te mogen in het land. De overheid zal snel nog vele andere redenen bij verzinnen om de 24/7 controle op privé-communicatie te legitimeren.

Signal en Telegram hebben al aangekondigd hun activiteiten binnen de EU te staken en hun platforms binnen de Unie te sluiten. Zover lijkt WhatsApp (van Facebook/Meta) nog niet te gaan, maar directeur Will Cathcart heeft wel aangegeven tegen deze wet te zijn.

Eigenaar Pavel Durov van Telegram heeft in een podcast van Lex Fridman laten weten er niet aan te denken om scanning toe te staan: *"Hoe meer druk ik ervaar, hoe weerbaarder en koppiger ik word."*

Protest tegen grootschalige privacyschending

De website fightchatcontrol.eu biedt de mogelijkheid om eenvoudig en direct protest aan te tekenen tegen deze ontwikkeling. Na een eenvoudig keuze van Nederlandse Europarlementariërs kan een bericht worden verzonden.

Een actuele timeline op de website toont de laatste ontwikkelingen.

Fight Chat Control is ook via Mastodon te volgen: mastodon.social/@chatcontrol