Het opgeven van digitale grondrechten is een gevaar voor Europa.

Datum: 1 oktober 2024

Onderwerp: Positie van Nederland op de Europese CSAM-verordening

Aan de leden van het kabinet,

Online kindermisbruik en het verspreiden van beelden daarvan ruïneert levens. In Nederland bestrijden we dit effectief, op een manier die slachtoffers helpt en misbruikers hard aanpakt. We weten ook dat het probleem landsgrenzen overstijgt. Samenwerking in Europa is daarom noodzakelijk.

Op de JBZ-raad van 11 oktober, een overleg met de Europese Justitieministers, wordt gesproken over de verordening ter voorkoming en bestrijding van online kindermisbruik – oftewel de **Child Sexual Abuse Material (CSAM) verordening**.[1] Op 2 oktober wordt tussen lidstaten de positie al afgestemd.

Over deze verordening hebben wij ernstige zorgen, samen met alle autoriteiten, organisaties, bedrijven en experts die dit reeds kenbaar hebben gemaakt.[2][3][4][5][6][7][8] **We zijn eensgezind dat effectieve regels nodig zijn, maar deze verordening biedt die overduidelijk niet.** De plannen zijn volstrekt buiten proportie, onduidelijk, en maken de online wereld minder veilig. In deze brief zetten wij onze zorgen uiteen. Wij vragen u met klem om deze te betrekken bij het formuleren van uw standpunt, nu de positie van Nederland vlak voor de besluitvorming in Europa nog niet helder is.

Een effectieve aanpak is mogelijk en daar moet de Nederlandse inbreng zich op richten. Onze onafhankelijke autoriteiten, hun goede samenwerking, een systeem van laagdrempelig melden en brede preventie – dat helpt slachtoffers wél. **Het Hongaarse voorstel stort echter een verdachtmaking uit over alle Europeanen en bouwt een achterdeurtje in om mee te kunnen lezen met al onze privégesprekken.**

Volgens deze surveillancewet moeten alle grote communicatie-apps een scan inbouwen, gebaseerd op nog onbekende technologie, die alle foto's van gebruikers controleert. Op termijn moet een **nog onzekerdere kunstmatige intelligentie** meekijken op alle foto's en meelezen op alle berichtjes om zo te bepalen of er sprake is van online kindermisbruik. Bij detectie wordt een melding gedaan bij autoriteiten, de gevolgen zijn groot. Deze meldingen belanden vervolgens op de veel te hoge stapel van meldingen waar de politie, wegens personeelstekort, al niks mee kunnen.

► Het voorstel is buiten proportie

Er zijn situaties waar ingrijpen op privécommunicatie moet plaatsvinden om onveilige

---

[1] Gelekte tekst Hongaarse voorstel (9 september 2024)
[2] Brief Amnesty International, Bits of Freedom, Cyberveilig Nederland, NLdigital (18 september 2024)
[3] Brief Offlimits | Expertisecentrum Online Misbruik (18 september 2024)
[4] Brief prof. dr. Frederik Zuiderveen Borgesius (17 september 2024)
[5] Brief prof. dr. Jaap-Henk Hoepman (11 september 2024)
[6] Brief Bert Hubert (17 september 2024)
[7] Brief Internet Society (17 september 2024)
[8] Opinie European Data Protection Supervisor (24 januari 2024)

situaties te stoppen. Deze inbreuk op grondrechten moet altijd gericht zijn en zorgvuldig worden afgewogen, omdat het briefgeheim een groot goed is. In de digitale wereld beschermt **end-to-endencryptie** dat recht, zodat niemand kan meelezen met de berichtjes die je stuurt. Daardoor weten we zeker dat de overheid zich niet bemoeit met persoonlijke zaken; in de fysieke wereld scheur je zonder verdenking andermans post ook niet open.

De techniek van **client-side scanning** is volgens experts[9][10] een manier om encryptie te omzeilen. Een scan die meeleest vóórdat je iets verstuurt, betekent nog steeds dat er over je schouder wordt meegekeken. Hoewel het kabinet volhoudt dat dit écht je privacy niet schendt, heeft de Tweede Kamer u meermaals duidelijk gemaakt dat dit een brug te ver is. **Ook toen gaf uw voorganger op het Ministerie van Justitie en Veiligheid geen gehoor aan deze oproep.** De volksvertegenwoordiging hecht grote waarde aan het recht op vertrouwelijke communicatie, dat heeft u te respecteren, ook onder druk van het Hongaarse voorzitterschap.

Door in te stemmen met dit voorstel dreigt u het digitale briefgeheim onomkeerbaar geweld aan te doen. Het voorstel raakt de communicatie van alle Europeanen en verkiest zo'n ongeleid sleepnet boven een gerichte en effectieve aanpak. **Als je eenmaal de keuze maakt om een achterdeur in te bouwen in al onze chatapplicaties, kan je niet meer terug**. Een politieagent in elke slaapkamer om alle soorten misbruik te voorkomen zouden we niet accepteren, maar in het digitale domein maakt Nederland die afweging blijkbaar anders.

► Het voorstel is onduidelijk

Met misleidende spierballentaal doet de CSAM-verordening de ingewikkelde werkelijkheid af met wensdenken. **Het voorstel is gebouwd op juridisch en technisch drijfzand.** Het is volstrekt onduidelijk welke systemen worden gebruikt voor de scans op materiaal van kindermisbruik dat bekend is uit databanken – het is nog minder duidelijk hoe scans op onbekende foto's en appverkeer op termijn gaan werken. Terwijl de techniek er enorm toe doet in zo'n verstrekkend voorstel.

Techniek is namelijk feilbaar. Dagelijks worden miljarden berichtjes en foto's verstuurd in Europa**. De gevolgen van een minimale foutmarge kunnen al desastreus zijn, omdat zo'n fout onschuldige Europeanen verdacht kan maken van een walgelijk feit.** Ook jongeren, die met wederzijdse toestemming het volste recht hebben om met vertrouwde leeftijdsgenoten intiem contact te hebben, worden mogelijk bestempeld tot dader. Deze zorgen worden totaal niet afgedekt in de CSAM-verordening.

Het verplicht inbouwen van een scan aan de kant van de gebruiker kon eerder al rekenen op felle kritiek van de Juridische Dienst die de Raad van Europa adviseert.[11] Zij sprak van een **buitenproportionele beperking van grondrechten en grote juridische onzekerheid**. Het is aannemelijk dat een rechter dit voorstel zal afkeuren, waardoor de plannen nog verder zullen wankelen en alleen de bepalingen overblijven die op termijn de scans door onzekere kunstmatige intelligentie mogelijk maken.

► Het voorstel maakt Europa minder veilig

In dit tijdsgewricht weten we dondersgoed dat waterdichte systemen nodig zijn. Zij houden ons veilig van kwaadwillende partijen en overheidsbemoeienis. Door in te stemmen met een

---

[9] Waarom client side scanning wat anders is dan een virusscanner (26 september 2024)
[10] Bugs in our pockets: the risks of client-side scanning (27 januari 2024)
[11] Opinie van de Europese Juridische Dienst (26 april 2023)

algemene afzwakking van onze privécommunicatie door de encryptie die dat waarborgt te omzeilen, ontstaan er **grote veiligheidsrisico's**.[12] Autocraten die niks liever willen dan **massasurveillance** op hun burgers zijn hierbij geholpen, slachtoffers niet.

Boeven zijn slim. De aanname dat er geen waterbedeffect zal plaatsvinden, met als gevolg dat misbruikers verplaatsen naar andere kanalen zonder scans, is puur wensdenken. **Daders en mogelijke daders verdwijnen zo nog verder uit beeld.** Het betekent ook dat vooral onschuldige Europeanen worden gescand en mogelijk verdacht worden gemaakt door een technische fout. **Daar is geen kind bij geholpen.**

De keuze om veilige communicatie te ondermijnen kán en mág dus niet gemaakt worden met alleen repressie in het achterhoofd. Het is volstrekt zeker dat een generieke scan op iedere chatapplicatie de veiligheid van alle Europeanen die digitaal communiceren op het spel zet. Met het bestaan van o.a. Pegasus-software weten we al dat mogendheden in staat zijn om communicatie in te dringen.[13] We kunnen ons niet veroorloven om in deze tijd lichtzinnig om te gaan met keuzes die raken aan cyberveiligheid.

► Het is nog niet te laat: stem tégen de surveillancewet!
Nederland staat – bij een vóórstem of onthouding – op het punt om de **blokkerende minderheid**, die eerdere versies van de verordening tot dusver heeft weten tegen te houden, te doorbreken. **Massasurveillance, juridische onzekerheid en een onveiligere digitale wereld worden daarmee een feit.**

Het is volstrekt onverantwoord als Nederland dat laat gebeuren door vóór te stemmen of zich stilletjes te onthouden van stemming. Géén standpunt innemen, geldt in de Europese verhoudingen als stille steun voor het voorstel. Terwijl we juist door de urgentie en het ongekende leed dat online kindermisbruik veroorzaakt, moeten komen tot zorgvuldige en effectieve regels. **De CSAM-verordening schiet daar in alle opzichten in tekort.**

Kabinet, in de meest harde bewoordingen roepen wij u op: **stem ondubbelzinnig tégen de surveillancewet**. Het Hongaarse voorstel en de eerdere versies gaven geen gehoor aan de analyse van het experts, politie, autoriteiten, waakhonden, het veiligheidsdomein en het bedrijfsleven die ook zien dat dit niks oplost, maar wel de grondrechten en cyberveiligheid van alle Europeanen op het spel zet.

Daarom moet de hele verordening **terug naar de tekentafel**. Zonder ingrijpende wijzigingen in het bereik en het doel van de verordening, zal deze slepende periode waarin telkens getornd wordt aan de veiligheid en fundamentele rechten met nieuwe ineffectieve voorstellen doorzetten. Intussen dringt de tijd en vragen wij u sterk om uw beslissende stem in Europa te heroverwegen.

Kinderen moeten beschermd worden en misbruikers moeten aangepakt, Nederland weet hoe dat moet. Het is dan ook onze verantwoordelijkheid om een grote rol te spelen in de gesprekken in Europa en te werken aan een geheel nieuw voorstel waarin onze veelbelovende aanpak verankerd wordt. **In huidige vorm van de surveillancewet wordt al dat werk ondermijnd.**

Dit voorstel voorkomt geen slachtoffers en het helpt geen slachtoffers; het maakt hooguit slachtoffers.

---

[12] Position paper client side scanning Cyberveilig Nederland (26 september 2024)
[13] Kamerbrief over Pegasus- of vergelijkbare software (23 december 2022)

Ondertekend,

GroenLinks-PvdA
Barbara Kathmann, Tweede Kamerlid
Kim van Sparrentak, Europarlementariër

D66
Hanneke van der Werf, Tweede Kamerlid
Raquel García Hermida-van der Walle, Europarlementariër

SP
Michiel van Nispen, Tweede Kamerlid

Offlimits
Robbert Hoving, directeur-bestuurder

Vereniging NLconnect
Mathieu Andriessen, directeur

Bits of Freedom
Rejo Zenger, beleidsadviseur

NLdigital

AMS-IX
Peter van Burgel, CEO

Stichting Digitale Infrastructuur Nederland
Michiel Steltman, directeur

Cyberveilig Nederland
Petra Oldengarm, directeur

ESET Nederland
Dave Maasland, CEO

Nationale Beheersorganisatie Internet Providers (NBIP)
Octavia de Weerdt, directeur

Branchevereniging ICT en Telecommunicatie Grootgebruikers (BTG)
Petra Claessen, voorzitter

Dutch Cloud Community
Simon Besteman, directeur

Internet Society Nederland

Diverse cybersecuritybedrijven
Vest
MITE3
Secureme2
Secwatch
Onyx Cybersecurity

Parell
Maurice Noordhof, CEO

Guardian360
Jan Martijn Broekhof, CEO

Secura
Dirk Jan van der Heuvel, CEO

Audittrail
Jorrit van der Walle, CEO

Computest
Dennis de Hoog, CEO

Privacy First
Vincent Böhre, directeur

Defend Digital Me (VK)
Jen Persson

Persoonlijke titel
Bert Hubert, expert cyberveiligheid
Danny Mekić, promovendus Universiteit Leiden
Prof. dr. Bibi van den Berg, hoogleraar Cybersecurity Governance (Universiteit Leiden)
Prof. dr. Michel van Eeten, hoogleraar Cybersecurity Governance (TU Delft)
Prof. dr. Herbert Bos, hoogleraar Systems Security (VU Amsterdam)