# Is client side scanning proportioneel?

## Gespreksnotitie

**Prof. Dr. Mr. Frederik J. Zuiderveen Borgesius**

**Professor ICT & Recht**

iHub, interdisciplinary research hub on digitalization and society, Radboud Universiteit
frederikzb[at]cs.ru.nl

Voor: Commissie Digitale Zaken
Rondetafelgesprek - Client Side Scanning
Tweede Kamer, 11 oktober 2023, 18:30 – 20:05

Geachte leden van de Commissie Digitale Zaken,

Dank u voor de uitnodiging om hier te spreken. Misbruik van kinderen is een afschuwelijk misdrijf, en het is van enorm belang dat hiertegen opgetreden wordt. Het is dan ook begrijpelijk dat de Europese Commissie actie wil ondernemen. De Commissie heeft een voorstel gedaan voor een verordening 'tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen'.[1] Maar de voorgestelde verordening ('het voorstel') roept serieuze vragen op. Deze notitie focust op de volgende vraag, door u gesteld aan de sprekers vandaag: Wat is de effectiviteit en proportionaliteit van 'client side scanning' bij de bestrijding van 'child sexual abuse material' (CSAM-materiaal)?

Ik concludeer dat het voorstel, en de daarmee samenhangende client side scanning, leiden tot een disproportionele beperking op grondrechten, waaronder het recht op vertrouwelijkheid van communicatie, de moderne versie van het briefgeheim. Verder zou het scannen van de communicatie van honderden miljoenen onschuldige Europeanen leiden tot zo veel 'false positives' (onterechte beschuldigingen), dat autoriteiten overspoeld worden en de meldingen niet kunnen onderzoeken. De verordening zal daarom waarschijnlijk niet effectief zijn.

Hieronder noem ik eerst drie verplichtingen uit het voorstel die relevant zijn voor client side scanning. (Lezers die het voorstel kennen, kunnen dat deel van deze notitie overslaan.) Daarna bespreek ik of client side scanning effectief en proportioneel is.

[1] Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen, COM(2022) 209 final ('het Voorstel').

## Drie verplichtingen in de voorgestelde verordening

Het voorstel legt 'aanbieders [van communicatiediensten] verplichtingen op inzake het opsporen, melden, verwijderen en blokkeren van bekend en nieuw materiaal van seksueel misbruik van kinderen, alsook van het benaderen van kinderen' (oftewel grooming).[2] Volgens het voorstel kunnen nationale autoriteiten een bevel geven aan communicatiediensten, zoals Apple's iMessage, Facebook Messenger, Gmail, Signal, WhatsApp, de 'direct messaging' onderdelen van Slack of LinkedIn, en audio-diensten zoals Microsoft Teams en Zoom. Die autoriteiten kunnen onder meer drie soorten bevelen aan communicatiediensten geven: bevelen over (i) bekend CSAM-materiaal, (ii) onbekend CSAM-materiaal, en (iii) grooming.

Grofweg samengevat kunnen nationale autoriteiten de communicatiediensten opdragen zulk materiaal, of gevallen van grooming, op te sporen, te blokkeren, te verwijderen, en te melden aan een nieuw op te richten Europees centrum ter voorkoming en bestrijding van seksueel misbruik van kinderen ('EU-centrum').

Dat EU-centrum zou ondergebracht worden in het kantoor van Europol.[3] Het EU-centrum moet de meldingen 'controleren op duidelijk vals-positieve meldingen, en ze doorsturen naar Europol en de nationale rechtshandhavingsinstanties.'[4] Het EU-centrum moet Europol ook 'zo volledige mogelijke toegang' geven tot zijn informatiesystemen.[5]

*(i) Bekend CSAM-materiaal*

Nationale autoriteiten kunnen een communicatiedienst verplichten om CSAM-materiaal dat bekend is bij de autoriteiten op te sporen en te melden aan het EU-centrum.[6] Autoriteiten kunnen 'hashes' (een soort digitale vingerafdrukken) van bekend CSAM-materiaal aan de communicatiedienst sturen. Door alle communicatie van gebruikers te analyseren, kan de communicatiedienst checken of een gebruiker bekend CSAM-materiaal wil versturen. Als iemand CSAM-materiaal wil versturen, dan moet de communicatiedienst dat bericht blokkeren en het melden aan het EU-centrum.[7]

*(ii) Onbekend CSAM-materiaal*

Nationale autoriteiten kunnen een communicatiedienst ook bevelen om CSAM-materiaal dat *nog niet bekend is bij autoriteiten* op te sporen en te melden aan de het EU-centrum.[8] (Zie bladzijde 3 van deze notitie voor meer details.)

*(iii) Grooming*

Nationale autoriteiten kunnen een communicatiedienst ook verplichten om gevallen van grooming op te sporen en te melden aan het EU-centrum.[9] Communicatiediensten moeten

---

[2] Het voorstel, p. 19.
[3] Het voorstel, p. 13.
[4] Het voorstel, p. 4. Zie ook artikel 48 van het voorstel.
[5] Het voorstel, artikel 53(2).
[6] Artikel 7 en 8 van het Voorstel. Zie ook p. 19. Bekend CSAM-materiaal wordt gedefinieerd in artikel 2(m) van het voorstel.
[7] Artikel 12 van het Voorstel. Zie ook p. 19.
[8] Artikel 7 en 8 van het Voorstel. Onbekend CSAM-materiaal wordt gedefinieerd in artikel 2(n) van het voorstel.
[9] Artikel 7 en 8 van het Voorstel. Grooming wordt in het voorstel 'het benaderen kan kinderen' genoemd, en wordt gedefinieerd in artikel 2(o) van het voorstel.

zelfs audio-gesprekken analyseren volgens het voorstel.[10] Bij de drie bovengenoemde bevelen moet de communicatiedienst het materiaal ook blokkeren of verwijderen.[11]

Als communicatiediensten end-to-end encryption gebruiken, is er slechts één theoretische mogelijkheid om aan zulke bevelen te voldoen: 'client side scanning'. Client side scanning betreft 'het scannen van de inhoud van berichten nog voordat deze verzonden worden en dus ook nog voordat er end-to-end-encryptie is toegepast'.[12]

## Client Side Scanning: proportioneel?

Zoals de Europese Commissie erkent,[13] vormt de verordening een beperking van verschillende grondrechten van gebruikers van communicatiediensten. Het gaat dan vooral om de rechten op vertrouwelijkheid van communicatie, op privacy, op de bescherming van persoonsgegevens, en op vrijheid van meningsuiting.[14]

Onder bepaalde voorwaarden mag de EU of een lidstaat deze rechten inperken. Maar daarvoor gelden wel strenge eisen, die onder meer volgen uit het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag voor de Rechten van de Mens, en de bijbehorende jurisprudentie.

Grondrechten beperken mag van het EU Handvest alleen om een 'algemeen belang' na te streven of om 'de rechten en vrijheden van anderen' te beschermen.[15] Het voorstel voldoet aan deze eis. Het tegengaan van kindermisbruik en het beschermen van de rechten van kinderen zijn uiteraard doelstellingen van algemeen belang.

Ook moet de een verordening 'duidelijke en precieze regels' bevatten die de beperking van een grondrecht omschrijven.[16] Maar zoals de European Data Protection Board en de European Data Protection Supervisor (EDPB & EDPS) opmerken, is het voorstel op veel punten onduidelijk.[17]

De volgende vraag is of het voorstel proportioneel is.[18] Om deze vraag te beantwoorden moeten de drie verplichtingen uit het voorstel apart behandeld worden. Eerst bespreek ik de proportionaliteit van bevelen over (ii) onbekend CSAM-materiaal, en (iii) grooming.

---

[10] EDPB & EDPS, p. 29.
[11] Artikel 12 van het Voorstel. Zie ook p. 19.
[12] Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen, 'Position paper – EU verordening ter bestrijding en voorkoming van seksueel misbruik, 19 september 2023, www.nationaalrapporteur.nl.
[13] Het voorstel, p. 14.
[14] Artikel 7, 8 en 11 van het EU Handvest.
[15] Artikel 52(1) EU Handvest.
[16] Artikel 52(1) EU Handvest. HvJEU, gevoegde zaken C-293/12 en C-594/12, 8 april 2014, ECLI:EU:C:2014:238 (Digital Rights Ireland), par 54. 'De betrokken Unieregeling moet dus duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten (…).
[17] EDPB & EDPS, 'Gezamenlijk advies 4/2022 over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen', 28 juli 2022, p. 5 en p. 16. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_nl
[18] Artikel 52(1) EU Handvest: 'Met inachtneming van het evenredigheidsbeginsel kunnen alleen beperkingen worden gesteld indien zij noodzakelijk zijn (…).' Verder moet de wezenlijke inhoud van rechten gerespecteerd worden. Dat punt komt later in deze notitie aan bod.

## False positives en onterechte verdachtmakingen

Hoe zou een communicatiedienst kunnen voldoen aan een bevel tot het opsporen en melden van (ii) onbekend CSAM-materiaal, en (iii) grooming? De Europese Commissie gaat ervan uit dat communicatiediensten AI-systemen (kunstmatige intelligentie-systemen) inzetten die automatisch herkennen welke beelden CSAM-materiaal bevatten, en welke communicatie grooming betreft.[19]

Maar soms zal een AI-systeem een onschuldige foto aanzien voor CSAM-materiaal. Stel dat een moeder een foto van een kind in bad stuurt aan oma. Een AI-systeem kan zo'n foto aanzien voor CSAM-materiaal. In de praktijk komt het nu al voor dat communicatiediensten zoals Microsoft en Google ten onrechte de account van een gebruiker afsluiten, omdat hun AI-systemen onschuldige beelden aanzien voor CSAM-materiaal.[20] Ook zullen AI-systemen soms CSAM-materiaal niet als zodanig herkennen.

De Europese Commissie noemt een AI-systeem dat zich weinig zou vergissen: 1 op de 1000 keer zou het systeem een onschuldige foto aanzien voor verboden CSAM-materiaal.[21] De claims over dat systeem zijn niet te verifiëren.[22] En zo'n kleine foutmarge zou een knappe prestatie zijn van de AI-ontwikkelaars.

Maar elke dag worden er miljoenen beelden uitgewisseld. Een foutmarge van 1 op 1000 zou tot duizenden false positives leiden: beelden en onterechte verdenkingen die gemeld worden aan het EU-centrum. Op zo'n manier wordt het EU-centrum overstelpt met onterechte meldingen. Het EU-centrum zal niet genoeg menskracht hebben om al die beelden te checken.[23]

Bovendien worden bij false positives mensen, ten onrechte, aan het EU-centrum gerapporteerd als iemand die waarschijnlijk verboden CSAM-materiaal uitwisselt.[24] Een verdenking van zo'n afschuwelijk misdrijf kan ingrijpend zijn.

Vergelijkbare bezwaren spelen bij AI-systemen die grooming zouden moeten opsporen in berichten en audio-gesprekken. Dit levert waarschijnlijk nog meer false positives, onterechte meldingen, op.[25] De EDPB & de EDPS concluderen dat in elk geval de verplichting om grooming op te sporen uit het voorstel geschrapt moet worden.[26] Niet alleen de EDPB & EDPS, maar ook veel anderen, waaronder veel informatici en AI-specialisten, waarschuwen voor het false positives-probleem. Zo hebben honderden academici in een open brief gewaarschuwd voor dit probleem.[27]

Zoals gezegd kunnen autoriteiten volgens het voorstel communicatiediensten ook bevelen om *bekend* CSAM te blokkeren en te melden. Grofweg samengevat stuurt het EU-centrum een soort digitale vingerafdrukken (*hashes*) van bekend CSAM-materiaal aan de

---

[19] Voorstel, p. 17.
[20] Zie Rechtbank Midden-Nederland, ECLI:NL:RBMNE:2020:5773, 30 december 2020; S. Hulsen, 'Microsoft zet honderden Nederlanders zonder uitleg uit account: "Dit is bizar"', RTL Nieuws, 11 december 2022. https://www.rtlnieuws.nl/tech/artikel/5351201/microsoft-zet-honderden-nederlanders-zonder-uitleg-uit-account K. Hill, 'A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal', New York Times, 21 augustus 2023 https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html
[21] Impact Assessment bij het voorstel, p. 282.
[22] EDPB & EDPS, p. 24.
[23] EDPB & EDPS, p. 18-19.
[24] EDPB & EDPS, p. 24.
[25] EDPB & EDPS, p. 19.
[26] EDPB & EDPS, p. 26.
[27] 'Joint statement of scientists and researchers on EU's proposed Child Sexual Abuse Regulation', https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y/edit

communicatiedienst. De communicatiedienst checkt dan of een gebruiker zulke bekend materiaal wil versturen.

Bij het opsporen van bekend CSAM-materiaal zullen er waarschijnlijk minder fouten gemaakt worden dan bij het opsporen van onbekend materiaal en grooming. Maar ook bij het opsporen van bekend CSAM-materiaal kunnen fouten optreden. Kwaadwillenden kunnen bijvoorbeeld bekend CSAM-materiaal zo manipuleren dat AI-systemen het materiaal niet meer herkennen.[28] Ook is het mogelijk om onschuldige beelden zo te manipuleren dat AI-systemen ze aanzien voor bekende CSAM-beelden, zonder dat een mens kan zien dat de beelden gemanipuleerd zijn.[29] Ook bij bekend CSAM-materiaal kunnen dus false positive optreden.

Samenvattend: de verplichting in het voorstel om groooming en bekend en onbekend CSAM-materiaal op te sporen is niet proportioneel. De risico's op false positives zijn te groot, vooral bij het opsporen van onbekend CSAM-materiaal en grooming. Zulke verplichtingen zijn niet effectief en maken onschuldige mensen verdacht.

## Disproportionele beperking van vertrouwelijkheid van communicatie en andere grondrechten

Het voorstel leidt ook tot een disproportionele beperking van het recht op vertrouwelijke communicatie. Volgens het voorstel moeten communicatiediensten, na een bevel daartoe, alle communicatie van hun gebruikers checken, voordat deze ge-encrypt (versleuteld) wordt. Zoals Ron Roozendaal opmerkt, is het alsof de communicatiediensten al uw brieven lezen voordat u die in de envelop stopt.[30] Als het voorstel wordt aangenomen, zou voor het eerst in Europa de communicatie van honderden miljoenen onschuldige mensen worden gemonitord en geanalyseerd voor de overheid.

Communicatiediensten zouden een soort achterdeur in hun apps moeten bouwen om client side scanning mogelijk te maken. Die infrastructuur maakt het mogelijk om ook andere beelden en tekst tegen te blokkeren en te melden. Autoriteiten hoeven daarvoor alleen een update met nieuwe *hashes* naar onze telefoons te sturen. Sommige EU-lidstaten nemen het minder nauw met de rechtsstaat. Zulke staten willen misschien ook andere communicatie laten opsporen, zoals gesprekken over demonstraties of spotprenten over de regering. Andere nationale autoriteiten willen misschien onze communicatie ook laten doorzoeken op gesprekken over drugs.

De EDPB & de EDPS betwijfelen dan ook of het voorstel proportioneel is. Ze 'benadrukken dat het voorstel aanleiding geeft tot ernstige bezorgdheid over de evenredigheid [ofwel proportionaliteit] van de beoogde inmenging en beperkingen op de bescherming van de grondrechten op privacy en de bescherming van persoonsgegevens.'[31]

---

[28] EDPB & EDPS, p. 20.

[29] M. Green, 'Remarks on "Chat Control"', 23 maart 2023, https://blog.cryptographyengineering.com/2023/03/23/remarks-on-chat-control/ ; J.H. Hoepman, 'DDoS-ing client-side scanning', 4 oktober 2023 https://blog.xot.nl/2023/10/04/ddos-ing-client-side-scanning/index.html

[30] R. Roozendaal, Buikpijn over client-side scanning, 7 oktober 2023, https://www.ronroozendaal.nl/blog/archive/2023-10

[31] EDPB & de EDPS, p. 5. Toevoeging tussen vierkante haakjes door de auteur.

Vergelijkbare zorgen zijn geuit door academici,[32] en de juridische diensten van het Europees Parlement[33] en de Raad van de Europese Unie.[34]

Ook in het licht van jurisprudentie van het Hof van Justitie van de EU (HvJEU) is het zeer de vraag of het voorstel proportioneel is. In het Dataretentie-arrest ('Digital Rights Ireland') besliste het HvJEU, samengevat, dat het opslaan van de metadata over de communicatie van honderden miljoenen Europeanen een disproportionele inbreuk maakt op het recht op privacy en vertrouwelijkheid van communicatie.[35] Metadata zijn, kort gezegd, data over communicatie, bijvoorbeeld met wie u chat, of wie u wanneer belt.

Het HvJEU zei dat die dataretentie-verplichting te ver ging, ook al was die verplichting bedoeld om een algemeen belang na te streven zoals het tegengaan van terrorisme. In het licht van die jurisprudentie is de kans aanzienlijk dat het HvJEU ook de voorgestelde CSAM-verordening ongeldig zou verklaren. Kortom, het voorstel, en de daarmee samenhangende client side scanning, is niet proportioneel.[36]

Sterker nog: waarschijnlijk zou het HvJEU niet eens toe komen aan een proportionaliteitstoets. Het EU Handvest eist namelijk ook dat beperkingen op grondrechten de 'wezenlijke inhoud' van grondrechten eerbiedigen.[37] Het voorstel voldoet waarschijnlijk niet aan deze eis. Volgens het HvJEU 'moet een regeling op grond waarvan de autoriteiten veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie worden beschouwd als een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven zoals door artikel 7 van het Handvest gewaarborgd'.[38]

Het voorstel maakt zulke grootschalige analyse van de inhoud van communicatie mogelijk.[39] De Onderzoeksdienst van het Europees Parlement concludeert dan ook dat het voorstel de wezenlijke inhoud schendt van het recht op privacy en op de vertrouwelijkheid van communicatie.[40] Als het HvJEU vaststelt dat een verordening de wezenlijke inhoud van een grondrecht schendt, dan is die verordening per definitie ongeldig.

Daarom moeten de EU en de lidstaten – op zijn minst – de technische en juridische aspecten van het voorstel en client side scanning beter onderzoeken. Zoals de Nationaal

---

[32] O. van Daalen, 'Fundamental rights assessment of the framework for detection orders under the CSAM proposal', 22 April 2023, IViR, https://www.ivir.nl/publicaties/download/CSAMreport.pdf; T. Quintel, 'The Commission Proposal on Combatting Child Sexual Abuse - Confidentiality of Communications at Risk?' *European Data Protection Law Review* 8 (2022): 262.

[33] European Parliamentary Research Service, 'Proposal for a regulation laying down rules to prevent and combat child sexual abuse, Complementary Impact assessment', EPRS Study, April 2023, https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf, p. VII, p. 55 en p. 63.

[34] Council of the European Union, Opinion of the Legal Service, 'Proposal for a Regulation laying down rules to prevent and combat child sexual abuse', 26 April 2023, https://www.bitsoffreedom.nl/wp-content/uploads/2023/05/20230426-opinion-legal-services-on-csar-proposal.pdf, p. 27.

[35] HvJ-EU, gevoegde zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland en Seitlinger en anderen).

[36] Voor een vergelijkbare conclusie: O. van Daalen, 'Fundamental rights assessment of the framework for detection orders under the CSAM proposal', 22 April 2023, IViR, https://www.ivir.nl/publicaties/download/CSAMreport.pdf, p. 17.

[37] Artikel 52(1) EU Handvest.

[38] HvJEU, C-362/14, ECLI:EU:C:2015:650 (Schrems I), par 94. Zie ook EDPB & de EDPS, p. 11.

[39] EDPB & de EDPS, p. 11.

[40] European Parliamentary Research Service, 'Proposal for a regulation laying down rules to prevent and combat child sexual abuse, Complementary Impact assessment', EPRS Study, April 2023, https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf, p. 55.

Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen onlangs opmerkte, zou een vergaande verordening zoals deze niet overhaast aangenomen moeten worden.[41]

## Conclusie

Samenvattend: de voorgestelde verordening en de verplichting voor communicatiediensten om (i) bekend CSAM-materiaal, (ii) onbekend CSAM-materiaal, en (iii) gevallen van grooming op te sporen, te melden aan het EU-centrum, en te blokkeren is niet proportioneel. De verplichtingen beperken het recht op vertrouwelijke communicatie en andere grondrechten op een disproportionele manier.

Ten eerste is het voor deze verplichtingen nodig dat communicatiediensten afzien van end-to-end encryptie, of client side scanning toepassen. In beide scenario's gaat de beperking van grondrechten te ver. De communicatie van honderden miljoenen onschuldige Europeanen zou gemonitord worden voor de autoriteiten.

Bovendien leidt het opsporen van onbekend CSAM-materiaal en grooming-gevallen tot te veel false positives, en dus tot onterechte beschuldigingen. Autoriteiten zullen al die onterechte meldingen niet kunnen verwerken. Ook daarom is het voorstel disproportioneel. Het voorstel is geen effectieve manier om kindermisbruik en het uitwisselen van CSAM-materiaal tegen te gaan.

* * *

[41] Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen, 'Position paper - EU verordening ter bestrijding en voorkoming van seksueel misbruik', 19 september 2023, https://www.nationaalrapporteur.nl/publicaties/brieven/2023/09/19/position-paper-eu-verordening-seksueel-misbruik