

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

16 februari 2026

VOORSTEL VAN RESOLUTIE

**betreffende het verwerpen
van de Europese verordening inzake
Chat Control (CSAM-verordening)**

**Advies
van de Gegevensbeschermingsautoriteit**

Zie:

Doc 56 **1071/ (2024/2025):**

001: Voorstel van resolutie van de heer Van der Elst c.s.

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

16 février 2026

PROPOSITION DE RÉSOLUTION

**relative au rejet
du règlement européen
“Chat Control” (règlement CSAM)**

**Avis
de l'Autorité de protection des données**

Voir:

Doc 56 **1071/ (2024/2025):**

001: Proposition de résolution de M. Van der Elst et consorts.

02669

N-VA	: Nieuw-Vlaamse Alliantie
VB	: Vlaams Belang
MR	: Mouvement Réformateur
PS	: Parti Socialiste
PVDA-PTB	: Partij van de Arbeid van België – Parti du Travail de Belgique
Les Engagés	: Les Engagés
Vooruit	: Vooruit
cd&v	: Christen-Democratisch en Vlaams
Ecolo-Groen	: Ecologistes Confédérés pour l'organisation de luttes originales – Groen
Anders.	: Anders.
DéFI	: Démocrate Fédéraliste Indépendant
ONAFH/INDÉP	: Onafhankelijk-Indépendant

Afkorting bij de nummering van de publicaties:		Abréviations dans la numérotation des publications:	
DOC 56 0000/000	Parlementair document van de 56 ^e zittingsperiode + basisnummer en volgnummer	DOC 56 0000/000	Document de la 56 ^e législature, suivi du numéro de base et numéro de suivi
QRVA	Schriftelijke Vragen en Antwoorden	QRVA	Questions et Réponses écrites
CRIV	Voorlopige versie van het Integraal Verslag	CRIV	Version provisoire du Compte Rendu Intégral
CRABV	Beknopt Verslag	CRABV	Compte Rendu Analytique
CRIV	Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toezpraken (met de bijlagen)	CRIV	Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)
PLEN	Plenum	PLEN	Séance plénière
COM	Commissievergadering	COM	Réunion de commission
MOT	Moties tot besluit van interpellaties (beigekleurig papier)	MOT	Motions déposées en conclusion d'interpellations (papier beige)



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 134/2025 van 11 december 2025

Betreft: advies op eigen initiatief met betrekking tot een voorstel van resolutie *betreffende het verwerpen van de Europese verordening inzake "Chat Control" (CSAM-verordening)* (CO-A-2025-203)

Trefwoorden: monitoring van elektronische communicatie – technieken voor de opsporing van strafbare feiten – seksueel misbruik van kinderen – eind-tot-eindversleuteling

Vertaling

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name de artikelen 23 en 26 (hierna "WOG");

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op de adviesaanvraag van de heer Peter De Roover, voorzitter van de Kamer van volksvertegenwoordigers (hierna "de aanvrager"), ontvangen op 20 november 2025;

Brengt de Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit") op 11 december 2025 het volgende advies uit:

Enkel adviezen met betrekking tot ontwerpen en voorstellen met rang van wet, die uitgaan van de federale overheid, het Brussels Hoofdstedelijk Gewest en de Gemeenschappelijke Gemeenschapscommissie worden zowel in het Nederlands als in het Frans door de Autoriteit gepubliceerd. De 'Originele versie' is de versie die gevalideerd werd.

I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. Op 11 mei 2022 heeft de Europese Commissie een voorstel ingediend voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen, ook wel bekend als "Chat Control"¹ (2022/0155 (COD)) (hierna "het voorstel voor een CSAM-verordening"). Op 16 november 2023 heeft het Europees Parlement zijn onderhandelingsstandpunt² over het voorstel voor een CSAM-verordening vastgesteld (hierna "het standpunt van het Europees Parlement"), waarin verschillende amendementen zijn opgenomen.
2. Op 13 februari 2024 heeft het Europees Comité voor gegevensbescherming ("de EDPB") een verklaring afgegeven over de wetgevende ontwikkelingen met betrekking tot het voorstel voor een CSAM-verordening (hierna "de verklaring van de EDPB") naar aanleiding van het standpunt van het Europees Parlement.
3. Op 20 november 2025 heeft de heer Peter De Roover, voorzitter van de Kamer van volksvertegenwoordigers, het advies van de Autoriteit gevraagd over een voorstel van resolutie *betreffende het verwerpen van de Europese verordening inzake "Chat Control" (CSAM-verordening)*, waarin de federale regering wordt verzocht "zich in de Raad van de Europese Unie krachtig te verzetten tegen het voorstel van de Europese Commissie betreffende de CSAM-verordening".
4. Overeenkomstig artikel 46, § 1, eerste lid, van het Reglement van interne orde van de Autoriteit, artikel 36.4 van de AVG en artikel 57.1.a) van de AVG bestaat de opdracht van de Autorisatie- en Adviesdienst van de Autoriteit er in de eerste plaats in adviezen uit te brengen over ontwerpen van normatieve teksten met betrekking tot gegevensverwerkingen die uitgaan van bevoegde nationale instellingen. Een voorstel van resolutie kan niet als een dergelijk normatief ontwerp worden beschouwd. In het onderhavige geval creëert noch wijzigt het betrokken voorstel van resolutie enige verwerking van persoonsgegevens (en regelt het deze dus evenmin).
5. Gelet op het belang en het gevoelige karakter van het voorstel voor een CSAM-verordening, beslist de Autoriteit niettemin het volgende advies uit te brengen.

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, 11 november 2022, beschikbaar op <https://eur-lex.europa.eu/legal-content/nl/TXT/HTML/?uri=CELEX:52022PC0209>.

² Ontwerpwetgevingsresolutie van het Europees Parlement 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, 16 november 2023, beschikbaar op https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_NL.html.

II. ONDERZOEK VAN HET ONTWERP

6. Het advies van de Autoriteit sluit aan bij het standpunt dat de EDPB (waarvan zij lid en belanghebbende is) heeft ingenomen in zijn verklaring.
7. De belangrijkste elementen van de verklaring van de EDPB³ zijn de volgende.

II.1. Cruciaal belang van de bestrijding van seksueel misbruik en erkenning van de verbeteringen die zijn aangebracht door het standpunt van het Europees Parlement

8. De EDPB benadrukt het cruciale belang van de bestrijding van seksueel misbruik van kinderen. Hij neemt kennis van de talrijke verbeteringen die het standpunt van het Europees Parlement heeft aangebracht ten opzichte van het voorstel voor een CSAM-verordening van de Europese Commissie. Deze verbeteringen omvatten met name de uitsluiting van "communicatie met eind-tot-eindversleuteling" (i.e. een proces van beveiligde communicatie waarbij gegevens worden versleuteld voordat ze naar een ander eindpunt worden verzonden) van het toepassingsgebied van de bevelen tot opsporing⁴ van pedopornografisch materiaal die door de bevoegde autoriteiten kunnen worden uitgevaardigd aan de aanbieders van relevante diensten van de informatiemaatschappij⁵ (hierna "aanbieders van diensten"), alsook de afschaffing van de verplichting voor de aanbieders van diensten om technologieën te gebruiken voor de opsporing van pedopornografisch materiaal in audio- of schriftelijke communicatie (waardoor de opsporingsbevelen worden beperkt tot communicatie van beelden en visuele inhoud). De aanbieders van diensten zouden de mogelijkheid behouden om zelf te bepalen welke technologische oplossingen zij wensen in te voeren⁶, op voorwaarde dat deze voldoen aan de beschermingswaarborgen waarin de toekomstige CSAM-verordening voorziet.⁷

II.2. Aanhoudende risico's van algemene monitoring

³ EDPB, Verklaring 1/2024 over de wetgevende ontwikkelingen met betrekking tot het voorstel voor een verordening tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen (*Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse*), https://www.edpb.europa.eu/system/files/2024-02/edpb_statement_202401_proposal_regulation_prevent_combat_child_sexual_abuse_en.pdf.

⁴ Een opsporingsbevel is een bevel, geregeld door de artikelen 7 tot en met 11 van het voorstel voor een CSAM-verordening, dat door een bevoegde gerechtelijke of onafhankelijke administratieve autoriteit wordt uitgevaardigd aan een aanbieder van relevante diensten van de informatiemaatschappij, waarbij deze wordt gelast technische hulpmiddelen in te voeren om pedocrimineel materiaal op te sporen in de communicatie of bestanden van zijn gebruikers.

⁵ Artikel 2 (f) van het voorstel voor een CSAM-verordening definieert de "relevante diensten van de informatiemaatschappij" als "alle volgende diensten: i) een hostingdienst; ii) een interpersoonlijke communicatiedienst; iii) een appstore; iv) een internettoegangsdiens".

⁶ Overweging 4 van het voorstel voor een CSAM-verordening stelt het volgende: "Gelet op het snel veranderende karakter van de betrokken diensten en de technologieën die worden gebruikt om ze aan te bieden, moeten deze regels technologie-neutraal en toekomstbestendig zijn, zodat innovatie niet wordt belemmerd."

⁷ Overweging 26 van het voorstel voor een CSAM-verordening stelt het volgende: "Deze verordening laat de betrokken aanbieder derhalve de vrije keuze wat betreft de te gebruiken technologieën om op doeltreffende wijze aan opsporingsbevelen te voldoen, en mag niet worden opgevat als een aansporing of ontmoediging om een bepaalde technologie te gebruiken, mits de technologieën en begeleidende maatregelen voldoen aan de voorschriften van deze verordening."

9. Ondanks deze positieve ontwikkelingen ten opzichte van het voorstel voor een CSAM-verordening van de Europese Commissie, herinnert de EDPB er in zijn verklaring aan dat het standpunt van het Europees Parlement nog steeds een aanzienlijk risico inhoudt van **willekeurige en algemene monitoring van particuliere communicatie**.

10. De EDPB uit de volgende voornaamste bezorgdheden:

- **Criteria voor de uitvoering van opsporingsbevelen:**

Het standpunt van het Europees Parlement doet onzekerheid ontstaan over de wijze waarop opsporingsbevelen moeten worden uitgevaardigd en gericht. Er zijn geen relevante criteria vastgesteld om te waarborgen dat deze bevelen daadwerkelijk worden beperkt tot personen die mogelijk betrokken zijn bij de uitwisseling van pedopornografisch materiaal. In dit stadium houdt de tekst het risico in dat het beoogde opsporingsmechanisme van toepassing is op alle burgers, in plaats van uitsluitend gericht te zijn op gebruikers ten aanzien van wie de rechtshandhavingsautoriteiten beschikken over "redelijke gronden om te vermoeden" dat zij pedopornografisch materiaal uitwisselen. Bovendien omschrijft het standpunt van het Europees Parlement niet duidelijk de voorwaarden waaronder het bestaan van dergelijke redelijke gronden kan worden vastgesteld, die aanleiding geven tot het uitvoeren van opsporingsbevelen.

- **Opsporingsbevelen voor de opsporing van nieuw materiaal met betrekking tot seksueel misbruik van kinderen:**

De EDPB is van mening dat opsporingsbevelen moeten worden beperkt tot de opsporing van "bekend materiaal met betrekking tot seksueel misbruik van kinderen" (i.e. materiaal dat eerder is opgespoord en bevestigd als pedopornografisch materiaal). Opsporingsbevelen in verband met "nieuw materiaal met betrekking tot seksueel misbruik van kinderen" (i.e. materiaal dat niet eerder is opgespoord) zijn problematisch vanwege de aanzienlijke foutenpercentages van de technologieën die worden gebruikt om dit nieuwe materiaal op te sporen (met het risico op valse positieven). Het is van essentieel belang om het risico te beperken dat deze bevelen personen treffen die waarschijnlijk niet betrokken zijn bij misdrijven in verband met pedopornografisch materiaal.

- **Eind-tot-eindversleuteling:**

Versleuteling is een cruciaal instrument om de vertrouwelijkheid van elektronische communicatie te waarborgen. Elke maatregel die ertoe strekt het gebruik ervan te beperken, aanbieders van diensten te verplichten gegevens van elektronische communicatie te verwerken voor andere doeleinden dan de levering van hun dienst, of communicatie proactief door te geven

aan derden, dreigt het aanbod van dergelijke versleutelingsdiensten te doen afnemen, waardoor de rol van versleuteling wordt verzwakt, de grondrechten worden aangetast en het vertrouwen in digitale diensten afneemt.

11. Uit deze essentiële elementen blijkt dat de Autoriteit zich in wezen aansluit bij het standpunt dat de aanvrager in zijn voorstel van resolutie heeft ingenomen met betrekking tot de risico's van het voorstel voor een CSAM-verordening.

12. De bestrijding van seksueel misbruik van kinderen is een absolute prioriteit.

De Autoriteit is echter van mening dat **de in het voorstel voor een CSAM-verordening beoogde mechanismen in strijd zijn met het evenredigheidsbeginsel en een ernstige aantasting vormen van het grondrecht op privacy:**

- **Ondoeltreffendheid van de huidige technische oplossingen:**

Opsporingsbevelen kunnen, gelet op de huidige stand van de technische oplossingen, niet worden beschouwd als passende maatregelen om het nagestreefde doeleinde te bereiken, vooral niet voor het opsporen van nieuw materiaal met betrekking tot seksueel misbruik van kinderen.⁸ In de praktijk blijken ze ondoeltreffend te zijn, aangezien het bijvoorbeeld mogelijk is ze te omzeilen door een afbeelding zodanig te wijzigen dat deze aan de opsporingssystemen kan ontsnappen. Hierdoor zou slechts een beperkt aantal daders van misdrijven worden gesignaleerd (valse negatieven). Omgekeerd kunnen afbeeldingen ook worden aangepast om valse positieven te genereren, waardoor onschuldige gebruikers worden gesignaleerd voor misdrijven die zij niet hebben gepleegd.⁹ Deze fouten kunnen ertoe leiden dat onschuldige personen bij het EU-centrum¹⁰ worden gemeld zodra "potentieel" online seksueel misbruik van kinderen wordt opgespoord.¹¹ Het EU-centrum zou deze mogelijke valse meldingen in voorkomend geval doorgeven aan de bevoegde nationale autoriteiten, wat zou leiden tot een verlies aan betrouwbaarheid van het opsporingsproces en een verhoogd risico op een onevenredige aantasting van de grondrechten.

⁸ Zie overweging 10, § 2, van dit advies; gezamenlijk advies EDPB-EDPS 04/2022, beschikbaar op https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf, p. 21, § 60.

⁹ Zie de open brief van 29 augustus 2024 over het standpunt van wetenschappers en onderzoekers, beschikbaar op: https://homes.esat.kuleuven.be/~preneel/Open_letter_CSAR_aug24_still_unacceptable.pdf, p. 3.

¹⁰ EU-centrum ter voorkoming en bestrijding van seksueel misbruik van kinderen.

¹¹ Artikel 12 van het voorstel voor een CSAM-verordening: "1. Wanneer een aanbieder van hostingdiensten of een aanbieder van interpersoonlijke communicatiediensten op een andere wijze dan door middel van een overeenkomstig deze verordening uitgevaardigd verwijderingsbevel kennis neemt van informatie die duidt op potentieel online seksueel misbruik van kinderen via zijn diensten, dient hij hierover tijdig een melding in bij het EU-centrum overeenkomstig artikel 13. Hij doet dit aan de hand van het overeenkomstig artikel 39, lid 2, ingestelde systeem."

- **Algemene en onevenredige monitoring:**

De voorwaarden voor het uitvaardigen van bevelen zoals voorzien in het voorstel voor een CSAM-verordening, die in algemene bewoordingen zijn geformuleerd¹² (bijvoorbeeld opsporingsbevelen die van toepassing zijn op een volledige communicatiedienst in plaats van op specifieke en verdachte gebruikers; de bewaring gedurende 24 maanden van al het opgespoorde pedopornografische materiaal (ongeacht of het om bekend of nieuw materiaal gaat), enz.)¹³, zouden leiden tot een bijzonder breed opsporingsgebied. In de praktijk zouden overheidsinstanties onbeperkte toegang hebben tot de digitale inhoud van alle gebruikers van interpersoonlijke communicatiediensten, waardoor een aanzienlijk aantal personen zou worden blootgesteld aan een inbreuk op hun grondrechten. Een dergelijke aanpak zou leiden tot een globale en onevenredige monitoring van alle elektronische uitwisseling binnen de Europese Unie en de EER¹⁴. De monitoring die hieruit zou voortvloeien, zou inherent algemeen en ongedifferentieerd zijn in verhouding tot het nagestreefde doeleinde. Bovendien zal het gebruik van algemene en onnauwkeurige termen om te bepalen of een opsporingsbevel noodzakelijk is, leiden tot rechtsonzekerheid en tot aanzienlijke verschillen¹⁵ in de concrete uitvoering van het voorstel voor een CSAM-verordening. Ten slotte kan het besef dat persoonlijke communicatie aan systematische monitoring kan worden onderworpen, ook de uitoefening van de vrijheid van meningsuiting beperken en individuen aanzetten tot zelfcensuur, uit vrees voor represailles.¹⁶

- **Risico op functieverschuiving ("function creep"):** Hoewel het voorstel voor een CSAM-verordening zich momenteel richt op het delen van pedopornografisch materiaal, roept de invoering van een algemeen systeem voor het scannen van de inhoud van apparaten van burgers van de Europese Unie en de EER grote bezorgdheid op. Een dergelijke technologie zou gemakkelijk kunnen worden uitgebreid naar alle inhoud die op die apparaten is opgeslagen, en zou kunnen worden gebruikt voor andere categorieën van inhoud (bijvoorbeeld om inhoud in verband met terroristische propaganda op te sporen), zonder dat een effectieve democratische controle gewaarborgd is.

Het voorstel voor een CSAM-verordening houdt aldus het risico in dat autoritaire regimes deze methode vervolgens zouden kunnen gebruiken om op grote schaal inhoud te identificeren die kritisch staat tegenover hun regering. Een dergelijk gebruik zou bijvoorbeeld kunnen leiden tot het opstellen van lijsten van journalisten, mensenrechtenverdedigers en oppositieleden die

¹² Zie overweging 10, § 1, van dit advies.

¹³ Gezamenlijk advies EDPB-EDPS 04/2022, *op. cit.*, p. 20, § 53.

¹⁴ De Europese Economische Ruimte, inclusief IJsland, Liechtenstein en Noorwegen.

¹⁵ Gezamenlijk advies EDPB-EDPS 04/2022, *op. cit.*, p. 16, § 37.

¹⁶ Gezamenlijk advies EDPB-EDPS 04/2022, *op. cit.*, p. 20, § 55.

dergelijke inhoud verspreiden. Het voorstel voor een CSAM-verordening zou zo niet-democratische regimes een operationeel instrument voor massamonitoring kunnen verschaffen.¹⁷

13. Gelet op de bovengenoemde elementen wordt het grondrecht op privacy dan ook ernstig aangetast door het **intrinsiek ingrijpende karakter** van de mechanismen waarin het voorstel voor een CSAM-verordening voorziet. Deze inmenging vloeit met name voort uit de mogelijkheid voor de autoriteiten om op algemene wijze toegang te krijgen tot de inhoud van de communicatie van alle gebruikers van aanbieders van diensten in de Europese Unie en de EER-landen, alsook uit de foutenpercentages die inherent zijn aan de gebruikte technologieën.
14. De Autoriteit is ook van mening dat **het voorstel voor een CSAM-verordening de voorkeur moet geven aan gerichte en evenredige maatregelen, waarbij eind-tot-eindversleuteling wordt gehandhaafd**, overeenkomstig de verklaring van de EDPB en de standpunten van de wetenschappelijke gemeenschap.¹⁸
15. Daarentegen voorziet het voorstel voor een CSAM-verordening in de opsporing van pedopornografisch materiaal rechtstreeks op het apparaat van de gebruiker ("*client-side scanning*"). Deze methode bestaat erin berichten of bestanden op het niveau van het apparaat te analyseren, hetzij vóór verzending (i.e. vóór de versleuteling), hetzij na ontvangst van het bericht (i.e. na de ontsleuteling). In de praktijk omzeilt een dergelijke methode de eind-tot-eindversleuteling, aangezien de inhoud wordt geïnspecteerd nog vóór zij wordt beschermd. Zo zou bijvoorbeeld opsporingssoftware worden geïntegreerd in een berichtenapplicatie om de inhoud van gesprekken te onderzoeken en automatisch elk als verboden aangemerkt element door te sturen naar de bevoegde autoriteiten. Zodra de inhoud toegankelijk wordt voor een andere partij dan de afzender of de ontvanger, verdwijnt de bescherming die door de versleuteling wordt geboden. Het behoud van eind-tot-eindversleuteling blijft echter essentieel om de vertrouwelijkheid van elektronische communicatie te waarborgen.¹⁹
16. De door het voorstel voor een CSAM-verordening voorgestelde maatregelen waarborgen geen vertrouwelijkheid van de communicatie en vormen derhalve een ernstige inbreuk op de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna "HGEU")²⁰ en op artikel 8 van

¹⁷ Gezamenlijk advies EDPB-EDPS 04/2022, *op. cit.*, p. 11, § 10.

¹⁸ Zie de open brief van 29 augustus 2024 over het standpunt van wetenschappers en onderzoekers, *op. cit.*

¹⁹ Zie de open brief van 29 augustus 2024 over het standpunt van wetenschappers en onderzoekers, *op. cit.*

²⁰ Artikel 7 van het Handvest van de grondrechten van de Europese Unie: "*Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.*"

Artikel 8 van het Handvest van de grondrechten van de Europese Unie: "*Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.*"

het Europees Verdrag voor de Rechten van de Mens²¹ (hierna "EVRM"). De bestaande veiligheidswaarborgen vormen essentiële elementen bij de beoordeling of sprake is van een fundamentele inbreuk op de artikelen 7 en 8 van het HGEU, alsook op artikel 8 van het EVRM.²² Wanneer een aantasting van een grondrecht aan de orde is, zoals hier het geval is, moeten dergelijke veiligheidsmaatregelen een compenserende rol vervullen teneinde de evenredigheid van de inmenging te waarborgen. In het voorliggende geval dragen de beoogde mechanismen er echter toe bij dat de bestaande veiligheidsmaatregelen worden verzwakt, waardoor zowel de bescherming van de versleuteling als de vertrouwelijkheid van de communicatie in het gedrang komen.²³

17. Bij wijze van conclusie is de Autoriteit van oordeel dat het voorstel voor een CSAM-verordening, gelet op zijn ingrijpende karakter en zijn onverenigbaarheid met het evenredigheidsbeginsel, in zijn huidige vorm niet kan worden aangenomen zonder een grondige herziening die ertoe strekt de vertrouwelijkheid van de communicatie en de effectieve bescherming van de grondrechten van de betrokkenen te waarborgen.



Voor de Autorisatie- en Adviesdienst,
Alexandra Jaspar, Directeur



²¹ Artikel 8 van het Europees Verdrag voor de Rechten van de Mens: "Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie."

²² Gezamenlijk advies EDPB-EDPS 04/2022, *op. cit.*, p. 11, § 13.

²³ Gezamenlijk advies EDPB-EDPS 04/2022, *op. cit.*, p. 11, § 10.



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 134/2025 du 11 décembre 2025

Objet : Avis d'initiative concernant une proposition de résolution *relative au rejet du règlement européen "Chat Control" (règlement CSAM)* (CO-A-2025-203).

Mots-clés : surveillance des communications électroniques – techniques de détection criminelle – abus sexuels sur des enfants – chiffrement de bout en bout

Version originale

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier ses articles 23 et 26 (ci-après « LCA »);

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis de Monsieur Peter De Rover, président de la Chambre des Représentants (ci-après « le demandeur »), reçue le 20 novembre 2025;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») décide d'émettre, le 11 décembre 2025, l'avis suivant :

L'Autorité ne publie en français et en néerlandais que les avis concernant les projets ou propositions de textes de rang de loi émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale ou de la Commission Communautaire Commune. La « Version originale » est la version qui a été validée.

I. OBJET ET CONTEXTE DE L'AVIS

1. Le 11 mai 2022, la Commission européenne a formulé une proposition de Règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants dite « Chat control »¹ (2022/0155 (COD)) (la « Proposition de Règlement CSAM »). Le 16 novembre 2023, le Parlement européen a adopté sa position de négociation² sur la Proposition de Règlement CSAM (la « Position du Parlement européen »), en y intégrant plusieurs amendements.
2. Le 13 février 2024, le Conseil européen de la Protection des Données (« EDPB ») a émis une Déclaration relative aux développements législatifs concernant la proposition de règlement CSAM (la « Déclaration de l'EDPB ») suite à la Position du Parlement européen.
3. Le 20 novembre 2025, Monsieur Peter De Roover, président de la Chambre des Représentants, adressait à l'Autorité une demande d'avis relative à une proposition de résolution *relative au rejet du règlement européen "Chat Control" (règlement CSAM)* enjoignant le gouvernement fédéral « *de s'opposer fermement, au sein du Conseil de l'Union européenne, à la proposition de la Commission européenne de règlement CSAM.* »
4. Conformément à l'article 46, §1, al. 1 du Règlement d'ordre intérieur de l'Autorité, à l'article 36.4 RGPD et à l'article 57.1.a) RGPD, la mission du Service d'Autorisation et d'Avis de l'Autorité consiste avant tout à émettre des avis sur les projets de textes normatifs encadrant des traitements de données émanant des institutions nationales compétentes. Une proposition de résolution ne peut être considérée comme un tel projet normatif. En l'occurrence, la proposition de résolution en question ne crée ni ne modifie (et donc n'encadre) aucun traitement de données à caractère personnel.
5. Compte tenu de l'importance et du caractère sensible de la proposition de règlement CSAM, l'Autorité décide néanmoins d'émettre l'avis suivant.

II. EXAMEN DU PROJET

6. L'avis de l'Autorité s'aligne sur la position exprimée par l'EDPB (dont elle est membre et partie prenante) dans la Déclaration de l'EDPB.

¹ Proposition de règlement du Parlement européen et du Conseil établissant des règles visant à prévenir et à combattre les abus sexuels sur enfants, COM/2022/209 final, 11 novembre 2022, disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52022PC0209>.

² Projet de résolution législative du Parlement européen sur la proposition de règlement du Parlement européen et du Conseil établissant des règles visant à prévenir et à combattre les abus sexuels sur enfants, 16 novembre 2023, disponible sur https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_FR.html.

7. Les éléments essentiels de la Déclaration de l'EDPB³ sont les suivants.

II.1. Importance cruciale du combat contre les abus sexuels et reconnaissance des avancées apportées par la Position du Parlement européen

8. L'EDPB souligne l'importance cruciale du combat contre les abus sexuels sur des enfants. Il prend note des nombreuses améliorations apportées par la Position du Parlement européen par rapport à la proposition de Règlement CSAM de la Commission européenne. Ces améliorations incluent notamment l'exclusion des « communications chiffrées de bout en bout » (i.e. processus de communication sécurisée chiffrant les données avant de les transférer vers un autre point de terminaison) du champ d'application des injonctions de détection⁴ de matériel pédopornographique pouvant être émises par les autorités compétentes à l'égard des fournisseurs de services pertinents de la société de l'information⁵ (« fournisseurs de services »), ainsi que la suppression de l'obligation imposée aux fournisseurs de services d'utiliser des technologies pour détecter du contenu pédopornographique provenant de communications audios ou écrites (limitant ainsi les injonctions de détection aux communications d'images et de contenu visuel). Les fournisseurs de services conserveraient la faculté de déterminer eux-mêmes quelles solutions technologiques ils souhaiteraient mettre en place⁶, sous réserve que celles-ci respectent les garanties de protection prévues par le futur règlement CSAM.⁷

II.2. Risques persistants de surveillance généralisée

9. Malgré ces évolutions positives par rapport à la proposition de Règlement CSAM de la Commission européenne, l'EDPB rappelle dans sa Déclaration de l'EDPB que la Position du Parlement européen engendre toujours un risque substantiel de **surveillance indiscriminée et généralisée des communications privées**.

³ EDPB, Déclaration 1/2024 sur les développements législatifs concernant la proposition de règlement établissant des règles pour prévenir et combattre les abus sexuels commis sur des enfants (*Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse*), https://www.edpb.europa.eu/system/files/2024-02/edpb_statement_202401_proposal_regulation_prevent_combat_child_sexual_abuse_en.pdf

⁴ L'injonction de détection est un ordre, encadré par les articles 7 à 11 de la proposition de Règlement CSAM, émis par une autorité judiciaire ou administrative indépendante compétente à un fournisseur de services pertinents de la société de l'information, lui ordonnant de mettre en place des outils techniques pour détecter des contenus pédocriminels dans les communications ou fichiers de ses utilisateurs.

⁵ L'article 2 (f) de la proposition de règlement CSAM définit les « services de la société de l'information pertinents » comme « l'ensemble des services suivants : un service d'hébergement ; ii : un service de communications interpersonnelles ; iii) une boutique d'applications logicielles ; (iv) un service d'accès à internet ».

⁶ Le considérant 4 de la proposition de règlement CSAM indique que « Eu égard à la rapidité de l'évolution des services concernés et des technologies utilisées pour les fournir, ces règles devraient être formulées de manière technologiquement neutre et de sorte à pouvoir s'adapter aux évolutions futures, afin de ne pas freiner l'innovation ».

⁷ Le considérant 26 de la proposition de règlement CSAM indique que « Le présent règlement laisse donc au fournisseur concerné le choix des technologies à utiliser pour se conformer efficacement aux injonctions de détection et ne devrait pas être compris en ce sens qu'il encouragerait ou découragerait l'utilisation d'une technologie donnée, pour autant que les technologies et les mesures d'accompagnement satisfassent aux exigences du présent règlement. »

10. L'EDPB émet les préoccupations principales suivantes :

- **Critères pour l'émission des injonctions de détection :**

La Position du Parlement européen soulève une incertitude quant à la manière dont les injonctions de détection doivent être émises et ciblées. Aucun critère pertinent n'est prévu pour garantir que ces injonctions seront effectivement limitées aux personnes susceptibles d'être impliquées dans l'échange de matériel pédopornographique. À ce stade, le texte comporte le risque que le mécanisme de détection envisagé s'applique à l'ensemble des citoyens, plutôt que de viser exclusivement les utilisateurs pour lesquels les forces de l'ordre disposent de « motifs raisonnables de soupçonner » un échange de matériel pédopornographique. Par ailleurs, la Position du Parlement européen ne définit pas clairement les conditions permettant d'établir l'existence de « motifs raisonnables de soupçon » déclenchant les injonctions de détection.

- **Injonctions de détection pour la détection de matériels nouveaux relatifs à des abus sexuels sur enfants :**

L'EDPB estime que les injonctions de détection doivent être limitées à la détection de « matériel connu relatif à des abus sexuels sur enfants » (i.e. du matériel précédemment détecté et confirmé comme constituant du matériel pédopornographique). Les injonctions de détection concernant les « matériels nouveaux relatifs à des abus sexuels sur enfants » (i.e. du matériel n'ayant pas été détecté préalablement) posent problème en raison des taux d'erreurs importants des technologies utilisées pour détecter ces matériels nouveaux (impliquant des risques de faux positifs). Il est essentiel de limiter le risque que ces injonctions affectent des personnes peu susceptibles d'être impliquées dans des infractions liées aux matériels pédopornographiques.

- **Chiffrement de bout en bout :**

Le chiffrement est un outil crucial pour garantir la confidentialité des communications électroniques. Toute mesure visant à en limiter l'usage, à contraindre les fournisseurs de services à traiter des données de communication électronique à des fins autres que la fourniture de leur service ou à transmettre proactivement des communications à des tiers risquerait de réduire l'offre de ces services de cryptage, affaiblissant ainsi le rôle du chiffrement, portant atteinte aux droits fondamentaux et réduisant ainsi la confiance dans les services numériques.

11. Il ressort de ces éléments essentiels que l'Autorité rejoint, en substance, la position exprimée par le demandeur dans sa proposition de résolution quant aux risques posés par la proposition de Règlement CSAM.

12. La lutte contre les abus sexuels commis sur des enfants constitue une priorité absolue.

L'Autorité considère toutefois que **les mécanismes envisagés par la proposition de Règlement CSAM violent le principe de proportionnalité et portent une atteinte grave au droit fondamental à la vie privée :**

- **Inefficacité des solutions techniques actuelles :**

Les injonctions de détection ne peuvent être considérées comme des mesures adéquates au regard de l'objectif poursuivi compte tenu de l'état actuel des solutions techniques, surtout pour détecter du matériel nouveau relatif à des abus sexuels sur enfants.⁸ En pratique, elles s'avèrent inefficaces puisqu'il est, par exemple, possible de les contourner en modifiant une image de manière à ce qu'elle puisse échapper aux systèmes de détection. Seul un nombre limité d'auteurs d'infractions seraient alors signalés (faux négatifs). À l'inverse, des images pourraient également être modifiées pour générer de faux positifs entraînant la dénonciation d'utilisateurs innocents pour des infractions qu'ils n'ont pas commis.⁹ Ces erreurs pourraient conduire des personnes innocentes à être signalées au Centre de l'UE¹⁰ dès lors qu'un « potentiel » abus sexuel sur enfants en ligne serait détecté.¹¹ Le Centre de l'UE transmettrait le cas échéant ces potentiels faux signalements aux autorités nationales compétentes, entraînant une perte de fiabilité dans le processus de détection et un risque accru d'atteinte disproportionnée aux droits fondamentaux.

- **Surveillance générale et disproportionnée :**

Les conditions d'émission d'injonction prévues par la proposition de règlement CSAM, formulées dans des termes généraux¹² (p. ex. les injonctions de détection applicables à l'ensemble d'un service de communication plutôt qu'à des utilisateurs spécifiques et suspects; la conservation pendant 24 mois de tout matériel pédopornographique détecté (qu'il soit connu ou nouveau), etc.)¹³ conduiraient à un champ de détection particulièrement vaste. En pratique, les autorités gouvernementales disposeraient d'un accès illimité aux contenus numériques de l'ensemble des utilisateurs de services de communications interpersonnelles, exposant ainsi un nombre considérable de personnes à une violation de leurs droits fondamentaux. Une telle

⁸ Voir considérant 10, §2 de ce présent avis ; Avis conjoint EDPB-EDPS 04/2022, disponible sur https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf, p. 21, §60

⁹ Voir la lettre ouverte du 29 août 2024 sur la position des scientifiques et chercheurs, disponible sur : https://homes.esat.kuleuven.be/~preneel/Open_letter_CSAR_aug24_still_unacceptable.pdf, p. 3

¹⁰ Centre de l'Union Européenne chargé de prévenir et de combattre les abus sexuels sur enfants

¹¹ L'article 12 de la proposition de Règlement CSAM : « 1. Lorsqu'un fournisseur de services d'hébergement ou un fournisseur de services de communications interpersonnelles a connaissance, par tout autre moyen que par une injonction de retrait émise conformément au présent règlement, de toute information indiquant un abus sexuel potentiel sur enfants en ligne sur ses services, il soumet rapidement un signalement à ce sujet au centre de l'UE conformément à l'article 13. Il le fait par l'intermédiaire du système établi conformément à l'article 39, paragraphe 2. »

¹² Voir considérant 10, §1 de ce présent avis

¹³ Avis conjoint EDPB-EDPS 04/2022, op. cit., p. 20, §53

approche instaurerait une surveillance globale et disproportionnée de l'ensemble des échanges électroniques au sein de l'Union Européenne et de l'Espace EEE¹⁴. La surveillance qui en résulterait serait, par nature, générale et indiscriminée par rapport à l'objectif poursuivi. De surcroît, l'utilisation de termes génériques et imprécis pour déterminer si une injonction de détection est nécessaire conduira à un manque de sécurité juridique et entraînera d'importantes divergences¹⁵ dans la mise en œuvre concrète de la proposition de Règlement CSAM. Enfin, la conscience que leurs communications personnelles peuvent être soumises à une surveillance systématique est également susceptible de restreindre l'exercice de la liberté d'expression et inciter les individus à adopter des comportements d'autocensure, sous l'effet de la crainte de représailles.¹⁶

- **Risque de glissement de fonction (« function creep »)** : Bien que la proposition de Règlement CSAM se concentre actuellement sur le partage de contenu pédopornographique, la mise en place d'un système de balayage généralisé sur les contenus des appareils de citoyens de l'Union européenne et aux pays de l'EEE soulève des préoccupations majeures. Une telle technologie pourrait aisément être étendue à l'ensemble des contenus conservés sur lesdits appareils et ceux-ci pourraient être utilisés pour d'autres catégories de contenus (p. ex. pour détecter tout contenu lié à la propagande terroriste) sans qu'un contrôle démocratique effectif ne soit garanti.

La proposition de règlement CSAM présente alors un risque que des régimes autoritaires recourent ensuite à ce procédé afin d'identifier, à grande échelle, les contenus critiques à l'égard de leur gouvernement. Une telle utilisation pourrait conduire, par exemple, à la mise en place de listes de journalistes, de défenseurs des droits fondamentaux et de membres de l'opposition diffusant ces contenus. La proposition de Règlement CSAM contribuerait ainsi à fournir aux régimes non démocratiques un instrument opérationnel de surveillance de masse.¹⁷

13. En raison des éléments mentionnés ci-dessus, le droit fondamental à la vie privée subit dès lors une atteinte grave en raison du **caractère intrinsèquement intrusif** des mécanismes prévus par la proposition de Règlement CSAM. Cette intrusion découle notamment de la possibilité pour les autorités d'accéder de manière généralisée au contenu des communications de l'ensemble des utilisateurs des fournisseurs de services dans l'Union européenne et aux pays de l'EEE, ainsi que des taux d'erreur inhérents aux technologies utilisées.

¹⁴ L'Espace économique européen comprenant l'Islande, le Liechtenstein et la Norvège

¹⁵ Avis conjoint EDPB-EDPS 04/2022, op. cit, p. 16, §37

¹⁶ Avis conjoint EDPB-EDPS 04/2022, op. cit, p. 20, §55

¹⁷ Avis conjoint EDPB-EDPS 04/2022, op. cit, p. 11, §10

14. L'Autorité estime également que **la proposition de Règlement CSAM doit privilégier des mesures ciblées et proportionnées, qui préservent le chiffrement de bout en bout**, conformément à la Déclaration de l'EDPB et aux positions prises par la communauté scientifique.¹⁸
15. À l'inverse, la Proposition de Règlement CSAM prévoit les détectations de contenus pédopornographiques directement sur l'appareil de l'utilisateur (« *client-side scanning* »). Cette méthode consiste à analyser les messages ou fichiers au niveau de l'appareil, que ce soit avant l'envoi (i.e. avant le chiffrement) ou après réception du message (i.e. après leur déchiffrement). En pratique, un tel procédé contourne le chiffrement de bout en bout, étant donné que le contenu est inspecté même avant d'être protégé. Un logiciel de détection serait intégré à une application de messagerie par exemple, afin d'examiner le contenu des conversations et de transmettre automatiquement aux autorités compétentes tout élément signalé comme prohibé. Dès lors que le contenu devient accessible à une partie autre que l'expéditeur ou le destinataire, la protection assurée par le chiffrement disparaît. Or, la préservation du chiffrement de bout en bout demeure essentielle pour garantir la confidentialité des communications électroniques.¹⁹
16. Les mesures proposées par la proposition de Règlement, ne garantissant pas une confidentialité des communications, constituent ainsi une violation importante aux articles 7 et 8 de la Charte des Droits fondamentaux de l'Union européenne (« CDFUE »)²⁰ et l'article 8 de la Convention européenne des droits de l'homme²¹ (« CEDH »). Les garanties de sécurité existantes constituent des éléments essentiels pour apprécier l'existence d'une violation fondamentale des articles 7 et 8 de la CDFUE, ainsi que l'article 8 de la CEDH.²² Lorsqu'une atteinte à un droit fondamental est en cause, comme cela est le cas en l'espèce, de telles mesures de sécurité devraient jouer un rôle compensatoire afin de préserver la proportionnalité de l'ingérence. Or, dans le cas présent, les mécanismes envisagés contribuent à affaiblir les mesures de sécurité en place, compromettant ainsi la protection du chiffrement et la confidentialité des communications.²³

¹⁸ Voir la lettre ouverte du 29 août 2024 sur la position des scientifiques et chercheurs, op. cit.

¹⁹ Voir la lettre ouverte du 29 août 2024 sur la position des scientifiques et chercheurs, op. cit.

²⁰ Article 7 Charte des droits fondamentaux de l'Union européenne : « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »

Article 8 Charte des droits fondamentaux de l'Union européenne : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. »

²¹ Article 8 de la Convention européenne des droits de l'homme : « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »

²² Avis conjoint EDPB-EDPS 04/2022, op. cit, p. 11, §13

²³ Avis conjoint EDPB-EDPS 04/2022, op. cit, p. 11, §10

Avis 134/2025 - 8/8

17. En conclusion, l'Autorité considère que la proposition de Règlement CSAM, en raison de son caractère intrusif et son incompatibilité avec le principe de proportionnalité, ne saurait, en l'état, être adoptée sans une révision substantielle visant à préserver la confidentialité des communications et la protection effective des droits fondamentaux des personnes concernées.



Pour le Service d'Autorisation et d'Avis,
Alexandra Jaspar, Directrice

