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 :

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 négociation[2] 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'EDPB[3] 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 détection[4] de matériel pédopornographique pouvant être émises par les autorités compétentes à l'égard des fournisseurs de services pertinents de la société de l'information[5] (« 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 place[6], 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'UE[10] 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 généraux[12] (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 aout 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 EEE[14]. 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 divergences[15] 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 détections 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'homme[21] (« 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

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,
(sé) Alexandra Jaspar, Directrice