Fiche résumé vidéo
Chat Control : quand l'Union européenne veut lire vos messages privés

Introduction

Depuis 2022, un projet européen en apparence vertueux enflamme les débats : la lutte contre les abus sexuels sur enfants en ligne.

Officiellement baptisé « *Règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants* » (CSAR), ce texte est plus connu sous un autre nom : « *Chat Control* ».

Derrière ce terme technique se cache une proposition controversée de la Commission européenne, accusée d'ouvrir la voie à une surveillance massive des communications privées.

C'est dire à quel point le sujet est à prendre au sérieux : même *BFM TV*[1] et *France Inter*[2] en parlent… sans évoquer le risque d'une théorie complotiste !

[1] https://x.com/BFMTV/status/1971117369368932457
[2] https://www.youtube.com/watch?v=jG7qEZC8V-I

Pour certains, il s'agit d'une mesure nécessaire pour lutter contre la pédocriminalité en ligne. Pour d'autres, une menace directe contre le chiffrement, la vie privée et, plus largement, les libertés démocratiques.

Juste Milieu fait le point pour vous avec tous les éléments-clés à connaître… pour éviter le pire !

1. Contexte et enjeux du projet

Le 11 mai 2022, la Commission européenne, sous l'impulsion de la commissaire suédoise Ylva Johansson, dépose la proposition COM/2022/209. Objectif affiché : « *prévenir et combattre les abus sexuels sur enfants* » dans l'espace numérique.

Selon le texte, il s'agit d'harmoniser les règles dans l'UE pour la détection, le signalement et la suppression des contenus d'abus sexuels sur mineurs (CSAM). Le projet veut également combler ce que Bruxelles considère comme un « vide juridique » laissé par deux évolutions :

1. le chiffrement de bout en bout (E2EE), qui empêche les autorités d'accéder aux messages ;

2. la responsabilité limitée des fournisseurs de messageries sécurisées.

La Commission a expliqué que le cadre juridique actuel, adopté en 2021, expirait en avril 2026. De fait, il devenait urgent de « le moderniser » pour éviter une impunité numérique totale.

Mais les conséquences du texte ont rapidement suscité une levée de boucliers à travers tous les pays de l'UE…

Selon *Euronews* dans un article du 5 septembre 2025[3], l'un des points les plus controversés est la possibilité d'imposer aux plateformes de messagerie de scanner les contenus échangés, y compris lorsqu'ils sont chiffrés, *via* une technologie dite de « *client-side scanning* ».

Ce procédé, qui consiste à analyser les messages directement sur l'appareil de l'utilisateur avant qu'ils ne soient chiffrés, reviendrait à surveiller en temps réel les conversations privées.

Les experts en cybersécurité alertent sur un risque paradoxal : en affaiblissant le chiffrement, on expose tous les citoyens à de nouvelles vulnérabilités — piratages, espionnage industriel, ou ingérences étrangères.

---

3 https://www.euronews.com/next/2025/09/05/time-is-running-out-for-eu-member-states-to-decide-on-chat-control?utm_source=chatgpt.com

2. Concrètement, comment fonctionne *Chat Control* ?

Le texte initial prévoyait que toutes les plateformes de communication — messageries, *emails*, hébergeurs de fichiers — soient contraintes de détecter, signaler et supprimer les contenus à caractère pédopornographique (CSAM), ainsi que les activités dites de « *grooming* » (tentatives de manipulation d'enfants en ligne).

Pour cela, la Commission proposait un outil central : le *client-side scanning*. Concrètement, chaque photo, vidéo ou message serait analysé par un algorithme avant envoi, pour identifier d'éventuels contenus illégaux. L'idée n'est pas nouvelle : *Apple* avait déjà tenté en 2021 d'introduire un système similaire, avant de l'abandonner face au tollé mondial sur la vie privée.

L'Union européenne souhaitait aller plus loin, en rendant ce scan obligatoire pour tous les services opérant dans l'espace européen. Autrement dit : chaque message, même entre deux particuliers qui n'ont rien à se reprocher, pourrait être inspecté.

En octobre 2025, sous la présidence tournante du Danemark, les négociations ont abouti à un compromis inattendu. *Le Parisien* rapporte le 30 octobre 2025[4] que Copenhague a décidé de « *retirer la mesure de scan des messages privés du texte* » pour débloquer son adoption, après des années de blocage.

Pour autant, **attention à ne pas crier victoire trop vite** : un nouveau vote serait prévu en décembre 2025. Et que ce vote ait lieu ou non, l'horizon d'avril 2026 reste en ligne de mire : il s'agit de la date d'expiration du cadre juridique actuel…

3. Entre atteinte aux libertés et risques techniques

Dès 2023, la proposition de règlement a été attaquée sur le plan juridique.

Plusieurs ONG, associations de défense des droits numériques et experts en cybersécurité ont dénoncé une violation frontale de la Charte des droits fondamentaux de l'Union européenne, notamment ses articles 7 (droit à la vie privée) et 8 (protection des données personnelles).

Les critiques se concentrent sur quatre points majeurs.

1. **Atteinte à la vie privée** : le principe même du client-side scanning viole le secret des communications. Comme le résume l'ONG *European Digital Rights*, "*aucun algorithme ne devrait être le gardien de nos conversations*

[4] https://www.leparisien.fr/high-tech/vie-privee-lue-fait-marche-arriere-sur-le-chat-control-et-le-scan-des-messages-prives-30-10-2025-6I73FWKWKBCJ3ORNK2XO3NU6HU.php

intimes” (EDRi, communiqué du 20/04/2025).

2. **Risque de dérive sécuritaire** : en créant des portes dérobées (« *backdoors* ») dans le chiffrement, le système deviendrait une cible idéale pour les cybercriminels et les États autoritaires.

3. **Faux positifs et dérives administratives** : les systèmes automatisés de détection peuvent commettre des erreurs dramatiques. L’exemple irlandais cité par l’*Irish Council for Civil Liberties* en octobre 2022[5] est éloquent : plus de 11 % des signalements reçus par la Garda Síochána (police irlandaise) ne concernaient pas de contenu illégal, mais des photos d’enfants à la plage ou des vidéos familiales. Pire, ces données n’ont pas été supprimées malgré la mise hors de cause des personnes concernées.

4. Un précédent inquiétant : la surveillance au nom du bien

Les défenseurs de la vie privée rappellent qu’à chaque fois qu’une technologie de surveillance a été introduite « pour une bonne cause », elle a souvent fini par déborder de son cadre initial.

Aux États-Unis, l’entreprise *Palantir*, fondée avec le soutien de la CIA, avait été présentée comme un outil destiné à repérer les réseaux terroristes. Elle est aujourd’hui utilisée pour surveiller les migrants ou repérer les bénéficiaires de programmes sociaux suspects.

L’analogie avec *Chat Control* est frappante : une technologie née pour protéger peut rapidement devenir un instrument de contrôle politique.

De plus, la mesure intervient dans un contexte européen de tension croissante entre sécurité et vie privée. En 2024, plusieurs États-membres, dont la France, avaient déjà tenté d’introduire un filtrage systématique des contenus terroristes sur les réseaux sociaux. Les juristes rappellent que ces dispositifs, d’abord ciblés, finissent souvent par s’étendre à d’autres domaines : désinformation, piratage, ou encore contestation politique.

5. Le paradoxe du pouvoir numérique européen

La polémique *Chat Control* révèle une contradiction profonde au sein de l’Union européenne.

---

5 https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing-of-child-sex-abuse-material/

D’un côté, Bruxelles affirme vouloir garantir la souveraineté numérique du continent et protéger les citoyens des géants technologiques américains. De l’autre, elle multiplie les textes qui donnent aux États et aux institutions un accès sans précédent aux données privées.

Le contraste est d’autant plus ironique que l’Union européenne elle-même est loin d’être exemplaire en matière de transparence. Plusieurs enquêtes ont révélé la disparition de courriels et de messages échangés par la présidente de la Commission, Ursula von der Leyen, dans le cadre des négociations sur les vaccins anti-Covid. Ainsi, pendant que Bruxelles envisage de scanner les messages de 450 millions d’Européens, elle se montre incapable de retrouver ceux de sa propre direction…

6. Analyse finale : un cheval de Troie numérique

La lutte contre la pédocriminalité est une cause juste et nécessaire. Mais l’histoire *Chat Control* illustre une constante des politiques sécuritaires : l’instrumentalisation du choc moral pour imposer un contrôle technologique durable.

Derrière le vernis humanitaire, le projet CSAR représente une menace structurelle pour la liberté numérique. Il repose sur un postulat dangereux : que la surveillance généralisée pourrait rendre la société plus sûre. Or, chaque faille ouverte dans le chiffrement met en danger la sécurité collective : un outil créé pour protéger les enfants pourrait demain servir à espionner les citoyens.