

PROTÉGER L'INTÉGRITÉ DE L'INFORMATION SUR LES PLATEFORMES DE MESSAGERIE PRIVÉE

**RAPPORT FINAL DE L'AXE DE TRAVAIL
DU PARTENARIAT POUR L'INFORMATION
ET LA DÉMOCRATIE COPRÉSIDÉ
PAR LE LUXEMBOURG ET L'UKRAINE**

Knowledge Partner



Ceci est le résumé du rapport qui présente les résultats d'un an de travail de l'axe de travail sur l'intégrité de l'information sur les plateformes de messageries privées du Partenariat pour l'information et la démocratie (PID). L'axe travail est coprésidé par les gouvernements du Luxembourg et de l'Ukraine et s'est réuni pendant quatre fois en 2025.

RÉSUMÉ EXÉCUTIF

Les plateformes de messagerie privée sont devenues un élément central de l'écosystème mondial informationnel. Leur portée, leur conception en réseau et leur utilisation (variable) du cryptage en font à la fois des canaux essentiels pour la communication privée et des vecteurs importants de désinformation.

Ce rapport a été élaboré par le Forum sur l'information et la démocratie (FID) avec le soutien du Stern Center for Business and Human Rights de l'université de New York. Il s'appuie sur les pratiques, les recherches et les connaissances partagées par les États membres du Partenariat et les membres de la coalition de la société civile du Forum lors d'une série de réunions de l'axe de travail.

Il examine les approches actuelles en matière de gouvernance et formule des recommandations visant à préserver l'intégrité de l'information tout en protégeant la vie privée et la liberté d'expression. Il s'appuie sur les travaux antérieurs du FID, en particulier ses recommandations sur les espaces mixtes privés et publics sur les applications de messagerie privée ([Pour mettre fin aux infodémies](#), 2020).



PRINCIPALES CONCLUSIONS

- ➔ **La désinformation sur les plateformes de messagerie pose des défis particuliers.** Des études montrent que les groupes fermés, les listes de diffusion et les canaux de messagerie hybrides « semi-publics » amplifient la désinformation tout en échappant à la surveillance. Des études de cas menées au Brésil et au Liban illustrent comment des contenus manipulés circulent de manière virale au sein de groupes chiffrés pendant les périodes électorales et les crises politiques, souvent via des campagnes d'influence coordonnées qui imitent les codes de communication communautaires.
- ➔ **Les espaces de messagerie privée occupent une zone grise sur le plan réglementaire.** Dans toutes les juridictions, les définitions des communications « privées » et « publiques » restent ambiguës. De nombreux cadres réglementaires et d'autorégulation, tels que la loi européenne sur les services numériques (DSA) et le code de conduite volontaire australien sur la désinformation et la mésinformation, excluent explicitement ou ne couvrent que partiellement les fonctions de messagerie privée. La loi britannique sur la sécurité en ligne (Online Safety Act) constitue une exception notable, traitant la messagerie comme un service d'utilisateur à utilisateur soumis à des exigences de transparence et d'atténuation des risques.
- ➔ **L'éducation aux médias est la réponse de politique publique la plus cohérente.** La plupart des juridictions privilégient l'éducation plutôt que la répression. L'initiative « Filter » en Ukraine, la campagne « Be Media Smart » en Irlande et les investissements nationaux de l'Australie dans l'éducation des médias illustrent cette tendance. Ces programmes visent à sensibiliser les utilisateurs et à renforcer leur résilience, mais ils ne peuvent se substituer à des mesures structurelles visant à lutter contre la viralité et l'amplification.

PRINCIPALES CONCLUSIONS

- ➔ **L'équilibre entre chiffrement et redevabilité reste à trouver.** Les autorités reconnaissent largement que le chiffrement de bout en bout (E2EE) est essentiel au droit à la vie privée et à la liberté d'expression. Cependant, des tensions persistent entre le chiffrement et la modération des contenus. De nombreux gouvernements semblent aux prises avec ce dilemme, soulignant la nécessité de mesures proportionnées et transparentes.
- ➔ **L'introduction de l'intelligence artificielle et de la publicité brouille encore davantage la catégorisation des plateformes de messagerie privée et pose des défis en matière de chiffrement.** La nature évolutive des plateformes de messagerie privée modifie l'aspect « privé » de ces plateformes et démontre que la réglementation n'est pas encore adaptée.
- ➔ **La coordination internationale est limitée, mais elle se développe.** Plusieurs pays expriment le besoin de cadres de coopération afin de partager les meilleures pratiques et d'harmoniser les normes relatives à la réglementation des plateformes de messagerie privée.

RECOMMANDATIONS EN BREF

Aux gouvernements :

1. Réglementer les fonctionnalités des plateformes plutôt que les catégories de plateformes. Les obligations légales devraient être liées à des fonctionnalités spécifiques (par exemple, les transferts de masse, les listes de diffusion, l'intégration de l'IA et de la publicité) plutôt qu'à de grandes catégories de plateformes, afin de refléter la nature hybride des services de communication modernes.

2. Clarifier les définitions des termes « public » et « privé ». Distinguer les obligations en fonction de la taille de l'audience, de la facilité de découverte, du chiffrement, des contrôles d'accès et de la possibilité de partage afin de garantir une supervision proportionnée.

3. Protéger le chiffrement. Éviter les obligations qui rendent le chiffrement de bout en bout techniquement inapplicable ; veiller à ce que toute obligation relative au contenu exclut les espaces chiffrés de bout en bout ou ne s'applique qu'aux fonctionnalités non chiffrées.

4. Imposer la transparence et l'autonomisation des utilisateurs. Cela inclut la transparence concernant la mise en œuvre des conditions d'utilisation et des services de la plateforme, les procédures de notification et d'action, ainsi que les informations fournies aux utilisateurs sur les nouvelles fonctionnalités et leurs implications.

5. Soutenir l'éducation aux médias. Élaborer des stratégies nationales visant à renforcer la résilience de la société face à la désinformation, mesurer leur efficacité et partager les enseignements tirés avec d'autres gouvernements.

6. Encourager les réponses internationales. Étendre les mécanismes de coordination en matière de désinformation aux plateformes de messagerie privée et élaborer des normes internationales.

RECOMMANDATIONS EN BREF

Aux plateformes :

1. Séparer les fonctions de messagerie, de diffusion et d'IA. Distinguer les communications privées chiffrées des fonctionnalités à grande échelle ou destinées au grand public ; envisager des produits ou des interfaces utilisateur distincts pour chacune d'entre elles. Veiller à ce que les fonctions d'IA dépendent d'un consensus opt-in et soient clairement distinguées des fonctionnalités chiffrées.

2. Appliquez le chiffrement de manière judicieuse. Limiter le chiffrement de bout en bout (E2EE) aux contextes où les utilisateurs ont des attentes raisonnables en matière de confidentialité ; introduire des freins au transfert massif afin de réduire la viralité.

3. Intégrer les droits humains dans la conception par défaut. Respecter les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits humains, établir des conditions d'utilisation claires et autonomiser les utilisateurs grâce à des fonctionnalités optionnelles, des procédures de notification et d'action et des mécanismes de révision.

4. Renforcer les systèmes d'authentification et de lutte contre les abus. Limiter la création de comptes multiples et réduire les manipulations liées aux « phone farms » grâce à des restrictions au niveau des appareils, des contrôles de fréquence et une autonomisation des utilisateurs.

5. Développer et promouvoir les « lignes d'information » vérifiées. Cela permet de vérifier les faits et de responsabiliser les utilisateurs.

6. Autonomiser les utilisateurs grâce à des outils de vérification intégrés à l'application. Soutenez et suivez les recherches sur les fonctionnalités intégrées à l'application qui permettent aux utilisateurs de vérifier les informations.

7. Participer à une coopération multiplateforme. Participez à des initiatives de partage d'informations afin de détecter les comportements inauthentiques coordonnés dans les écosystèmes de messagerie.

8. Promouvoir la transparence et la recherche indépendante. Partager de manière proactive les informations avec la société civile indépendante, les chercheurs et les régulateurs sur les caractéristiques, les fonctionnalités et les décisions de modération du contenu, tout en respectant la vie privée afin de permettre une évaluation indépendante.