



International Panel on the Information Environment

Lutter contre l'exploitation numérique

Recommandations pour prévenir et lutter contre l'exploitation et les abus sexuels des enfants facilités par la technologie

Résumé 2026.1 à l'intention des décideurs politiques

DOI Number: 10.61452/HPBS9755

K. Pothong, S. Kaynak, S. Ghai, D. Fry, S. Livingstone, A. Phippen, C. R. Soriano, L. M. Given, P. N. Howard, S. Valenzuela



IPIE
International Panel on the
Information Environment

Lutter contre l'exploitation numérique

Recommandations pour prévenir et lutter
contre l'exploitation et les abus sexuels des
enfants facilités par la technologie

Résumé 2026.1 à l'intention des

Comment citer :

International Panel on the Information Environment [K. Pothong, S. Kaynak, D. Fry, S. Ghai, S. Livingstone, A. Phippen, C. R. Soriano, L. M. Given, P. N. Howard, M. Valente, S. Valenzuela (eds.)], « Lutter contre l'exploitation numérique : Recommandations pour prévenir et lutter contre l'exploitation et les abus sexuels des enfants facilités par la technologie », Zurich, Suisse : IPIE, 2026. Résumé à l'intention des décideurs politiques, SFP2026.1, doi: 10.61452/HPBS9755.

SYNOPSIS

L'exploitation et les abus sexuels des enfants facilités par la technologie (TF-CSEA pour « Technology-facilitated child sexual exploitation ») constituent une crise croissante. Les plateformes numériques, les réseaux sociaux, les services de diffusion en direct et les systèmes de paiement en ligne facilitent les abus sexuels sur les enfants à une échelle et à une vitesse considérables.

Les signalements de grooming (manipulation en vue de commettre des abus) en ligne, de sextorsion financière, d'abus diffusés en direct et de contenus pédopornographiques générés par l'IA continuent d'augmenter dans de nombreuses régions. Les interventions existantes peinent à suivre le rythme des évolutions technologiques, ce qui permet aux criminels d'opérer au-delà des frontières avec un risque limité d'être détectés ou perturbés.

Ce *Résumé à l'intention des décideurs politiques* présente les principales conclusions du *Rapport de synthèse* intitulé « Detecting, Deterring, Investigating, and Prosecuting Technology-Facilitated Child Sexual Exploitation and Abuse: A Systematic Review » - Détecter, dissuader, enquêter et poursuivre les actes d'exploitation et d'abus sexuels commis à l'encontre d'enfants à l'aide de technologies : une revue systématique ([SR2026.1](#)). À l'aide des protocoles PRISMA standard, cette revue fournit une synthèse méthodologique rigoureuse de plus de 100 études sur les interventions publiées au cours de la dernière décennie. Elle évalue les interventions techniques, juridiques, policières, comportementales et éducatives et présente quatre conclusions principales :

1. **La plupart des interventions se concentrent sur la détection des abus après les faits.** Beaucoup moins nombreuses sont celles qui s'attaquent aux systèmes qui permettent l'exploitation et les abus, tels que les mécanismes de paiement et les circuits de promotion et de recrutement, ou qui s'intéressent aux capacités judiciaires limitées qui ne permettent pas d'assurer la dissuasion ou l'application de la loi.
2. **Les outils techniques peuvent réduire les préjudices à grande échelle, mais ils dépendent de l'autorité légale, de l'accès sécurisé aux données, des garanties et de l'application efficace de la loi.** Sans ces éléments, ces outils automatisés et assistés par l'IA ont un impact limité.
3. **Les interventions comportementales et éducatives peuvent réduire les risques et sensibiliser le public, mais elles ne peuvent se substituer à la responsabilité des plateformes.** Les preuves d'un changement de comportement durable restent limitées sans financement, notamment

pour les études longitudinales.

4. **Les systèmes financiers sont le levier le plus sous-utilisé contre les TF-CSEA.** Peu d'interventions perturbent le financement des abus, se concentrant plutôt sur le traçage des transactions après que le préjudice a été causé.

La synthèse fournit l'évaluation la plus complète à ce jour des interventions contre les TF-CSEA et a été réalisée par le *Scientific Panel on Child Protection and Social Media* de l'IPIE. Les conclusions démontrent un consensus clair sur la nécessité d'une autorité juridique coordonnée, d'outils techniques évolutifs, d'une application soutenue et de mesures visant à interrompre les flux financiers.

INTRODUCTION

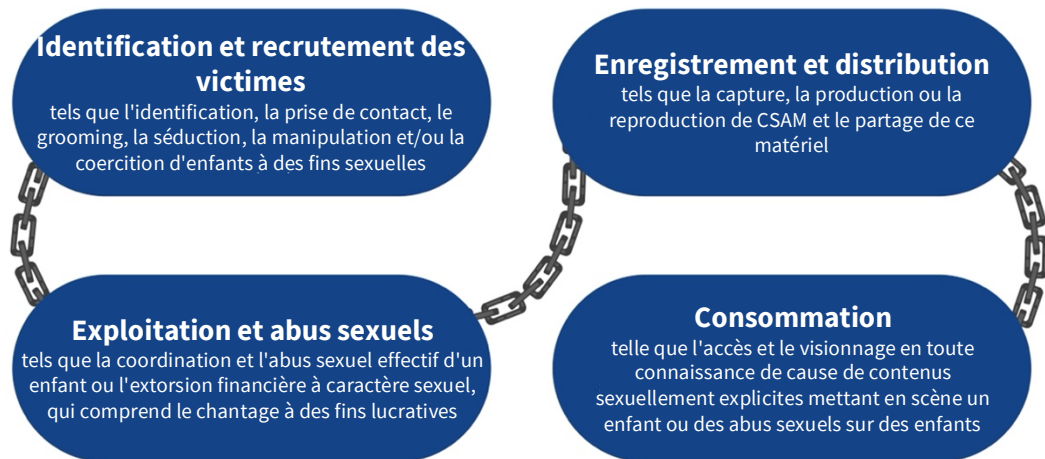
L'exploitation et les abus sexuels des enfants facilités par la technologie (TF-CSEA) sont devenus une crise mondiale persistante et croissante[1]. Les plateformes numériques, les réseaux sociaux, les services de diffusion en direct et les systèmes de paiement en ligne ont transformé la manière dont les abus sont produits, distribués et monétisés. Ces technologies permettent aux criminels d'atteindre un grand nombre d'enfants, d'opérer au-delà des frontières et d'échapper plus facilement à la détection que par le passé. Les signalements de grooming en ligne, de sextorsion financière, d'abus diffusés en direct et de matériel pédopornographique généré numériquement (CSAM pour « child sexual abuse material ») continuent d'augmenter dans le monde entier[2].

Les gouvernements, les entreprises technologiques et les organisations de la société civile ont réagi en mettant en place un large éventail de mesures visant à prévenir les TF-CSEA. Il s'agit notamment d'outils techniques permettant de détecter les contenus abusifs, de stratégies de maintien de l'ordre et d'enquête, de cadres juridiques et réglementaires, d'interventions comportementales et de campagnes d'éducation et de sensibilisation. Cependant, ces mesures varient considérablement en termes de portée, de maturité et d'efficacité. Les décideurs politiques de tous les pays sont soumis à une pression croissante pour comprendre quelles mesures permettent de réduire les préjudices, lesquelles peuvent être étendues à d'autres juridictions et où se trouvent les lacunes les plus graves.

La figure 1 illustre comment les TF-CSEA surviennent tout au long d'une chaîne d'activités connectées, du recrutement à l'exploitation, en mettant en évidence plusieurs points où des interventions politiques et répressives peuvent mettre fin aux abus.

Ce Résumé à l'intention des décideurs politiques présente les principales conclusions d'une synthèse des interventions TF-CSEA à travers le monde. L'évaluation s'appuie sur un examen systématique de plus de 100 études évaluées par des pairs et de rapports fondés sur des preuves publiés au cours de la dernière décennie.

Figure 1. Chaîne d'infractions TF-CSEA.



Source : IPIE. [2]

Le groupe d'experts a examiné les interventions utilisées dans les domaines technique, juridique, policier, comportemental et éducatif, et les a classées selon la chaîne d'infractions TF-CSEA. Conformément aux lignes directrices PRISMA, cette étude a systématiquement passé au crible des études évaluées par des pairs et des rapports fondés sur des preuves, rédigés par des centaines de chercheurs à travers le monde, afin d'évaluer les interventions TF-CSEA utilisées dans différentes disciplines à l'aide de critères d'inclusion prédéfinis. L'objectif était d'identifier les mesures politiques les plus susceptibles de lutter contre l'exploitation et les abus sexuels des enfants facilités par la technologie.

Nous mettons ici en évidence quatre conclusions principales tirées de l'évaluation plus large intitulée *Detecting, Deterring, Investigating, and Prosecuting Technology-Facilitated Child Sexual Exploitation and Abuse: A Systematic Review* [2]. Des informations supplémentaires sont disponibles dans le rapport principal.

RÉSULTAT 1. DETECTION PLUTOT QUE PREVENTION

CONCLUSION

La plupart des interventions se concentrent sur la détection des abus après les faits.

Les données montrent que la plupart des interventions TF-CSEA se concentrent sur la détection des abus après que le préjudice a déjà été causé. La littérature évaluée par des pairs et les rapports organisationnels montrent que la plupart des interventions visent la détection, l'enquête et l'identification du contenu. Ces interventions se concentrent sur l'identification du matériel pédopornographique, le suivi des activités des criminels et le soutien aux enquêtes des forces de l'ordre.

La plupart des interventions impliquent l'utilisation d'outils et de protocoles technologiques, suivis de mesures policières et d'enquêtes. Les interventions juridiques et réglementaires semblent moins fréquentes, tandis que les interventions comportementales et les campagnes d'éducation sont principalement abordées dans la littérature grise. Dans l'ensemble, les interventions visent notamment la détection, le stockage et la distribution de matériel pédopornographique, le grooming et les infractions sexuelles en général.

En revanche, plusieurs systèmes essentiels n'ont pas encore fait l'objet d'une évaluation systématique. Très peu d'interventions portent sur les voies de recrutement, la promotion des abus, la capacité judiciaire ou les mécanismes de paiement. Aucune publication évaluée par des pairs n'a examiné les interventions ciblant la promotion des TF-CSEA, et une seule a documenté une intervention ayant un effet indirect sur l'interruption des paiements. Aucune intervention visant à améliorer l'efficacité des tribunaux ou des processus judiciaires n'a été trouvée dans les publications évaluées par des pairs.

La figure 2 révèle que la plupart des interventions visant à détecter, dissuader, enquêter et poursuivre les auteurs de TF-CSEA au cours de la dernière décennie n'ont pas suffisamment abordé les domaines critiques en amont que sont le recrutement et les paiements.

Ce déséquilibre limite la prévention et la dissuasion. Les mesures axées sur la détection améliorent l'identification, mais ne perturbent pas les systèmes qui permettent aux abus de se multiplier et de persister. En conséquence, les réponses politiques restent réactives. Les données disponibles indiquent que la lutte contre les TF-CSEA peut nécessiter de se concentrer en amont, sur les systèmes qui permettent aux abus d'être organisés, financés et répétés.

Figure 2. Fréquence des interventions au sein de l'écosystème des TF-CSEA.



Source : Données basées sur des articles codés manuellement et collectés le 17 juillet 2025 dans des bases de données (SR2026.1).

Remarque : $n = 114$ (100 %) mécanismes d'intervention et leurs impacts sur la chaîne d'intervention. Les

RÉSULTAT 2. LES OUTILS DOIVENT ÊTRE SOUTENUS PAR LES

AUTORITES

CONCLUSION

Les outils techniques réduisent les préjudices à grande échelle, mais dépendent des autorités, des données, des mesures de protection et de l'application de la

Les outils et protocoles techniques représentent les interventions les plus développées et les plus évolutives contre les TF-CSEA. L'évaluation documente l'utilisation généralisée de l'analyse automatisée de contenu, des listes d'URL et de hachages, du crawling web et des outils d'investigation numérique. Ces technologies facilitent l'identification transfrontalière du matériel pédopornographique et améliorent les activités de police et d'enquête.

Plusieurs outils ont directement contribué aux enquêtes, aux poursuites et à l'identification des victimes, en particulier lorsqu'ils ont été intégrés dans les processus des forces de l'ordre. L'utilisation de l'intelligence artificielle s'est rapidement développée, notamment pour détecter les contenus pédopornographiques et identifier les comportements prédateurs, y compris le grooming. Certains outils basés sur l'IA font preuve d'une précision prometteuse, en particulier dans des environnements contrôlés ou en

laboratoire, bien que leurs performances dans le monde réel varient selon les contextes de déploiement (voir le rapport principal, [2]).

Cependant, les preuves font également état de limites évidentes. L'efficacité des outils techniques dépend de l'accès à des données d'entraînement représentatives et de haute qualité. Les contraintes juridiques, éthiques et liées à la confidentialité limitent l'accès aux CSAM vérifiés, ce qui restreint le développement et les tests des modèles. De nombreuses organisations qui déploient des outils technologiques ne disposent pas de l'autorité juridique ou du pouvoir d'exécution nécessaires, ce qui réduit leur capacité à perturber ou à supprimer les contenus et activités illégaux.

Parmi les autres défis figurent l'évolutivité, les dépendances aux plateformes et l'absence de mécanismes permettant de traiter les faux positifs et les erreurs. Aucune des études examinées n'a abordé les processus permettant aux personnes qui ont été identifiées à tort comme auteurs d'infractions de blanchir leur nom et d'obtenir réparation.

Les données disponibles montrent que les outils techniques réduisent le préjudice de manière plus efficace lorsqu'ils sont associés à des mandats juridiques clairs, à des accords de partage de données sécurisés, à des garanties et à des capacités d'application de la loi bien formées. Sans ces conditions, leur impact reste limité.

RÉSULTAT 3. MESURES DE PROTECTION ET RESPONSABILITÉ DES

PLATEFORMES

CONCLUSION

Les interventions comportementales et éducatives réduisent les risques, mais ne peuvent remplacer la responsabilité.

Les interventions comportementales et les campagnes d'éducation, d'alphabétisation et de sensibilisation jouent un rôle de soutien dans la lutte contre les TF-CSEA. L'étude identifie plusieurs interventions comportementales visant principalement les auteurs potentiels ou avérés. Il s'agit notamment de messages d'avertissement, de communications thérapeutiques et dissuasives, de lignes d'assistance anonymes et de programmes structurés de thérapie cognitive-comportementale en ligne.

Les résultats de plusieurs études indiquent que ces interventions peuvent réduire les tentatives d'accès à du matériel pédopornographique et encourager la recherche d'aide. Les approches non moralisatrices et confidentielles semblent particulièrement efficaces pour réduire les obstacles à l'engagement. Certaines interventions ont également ciblé les professionnels, tels que les agents des forces de l'ordre, en utilisant des outils de formation pour améliorer leurs compétences en matière d'enquête.

Les campagnes d'éducation et de sensibilisation ciblent principalement les enfants et les jeunes. Les approches interactives et ludiques ont des effets positifs sur leur sensibilisation aux risques en ligne et aux stratégies de grooming. Les évaluations font état d'une augmentation des connaissances et de l'engagement des participants et des éducateurs.

Cependant, les données probantes restent limitées. Peu d'études examinent les résultats à long terme, et la plupart s'appuient sur des mesures à court terme ou autodéclarées. La revue ne trouve que peu de preuves que la sensibilisation se traduise systématiquement par un changement de comportement durable ou une réduction du nombre de victimes au fil du temps.

La synthèse met en garde contre une confiance excessive dans ces interventions. Les approches comportementales et éducatives ne peuvent se substituer à la responsabilité des plateformes, à l'application de la loi ou aux mesures de protection au niveau du système. Les données disponibles soutiennent leur utilisation en tant que mesures complémentaires dans le cadre d'une réponse politique plus large, telle que la responsabilité des plateformes.

RÉSULTAT 4. SUIVRE ET INTERROMPRE LE FINANCEMENT

CONCLUSION

Les systèmes financiers constituent peut-être le levier le moins utilisé pour lutter contre les TF-CSEA.

L'étude révèle que les systèmes financiers sont les moins pris en compte, alors qu'ils pourraient constituer des points d'intervention très efficaces dans l'écosystème des TF-CSEA. Malgré des preuves évidentes que les paiements numériques facilitent la commercialisation et la propagation des abus sur les plateformes numériques, presque aucune des interventions évaluées ne perturbe directement les flux de paiement.

Un seul cas documenté a montré un effet indirect sur la perturbation des flux de revenus provenant des échanges de CSAM. Aucune publication évaluée par des pairs n'a examiné les interventions explicitement conçues pour bloquer, retarder ou empêcher les paiements associés aux TF-CSEA.

Les interventions financières existantes se concentrent principalement sur le suivi et le signalement des transactions après que le préjudice a été causé. Les cadres de lutte contre le blanchiment d'argent et les obligations de déclaration permettent aux institutions financières de partager des informations avec les forces de l'ordre. Cependant, nous ne disposons pas encore de preuves démontrant que ces mécanismes empêchent les transactions en temps réel.

Les rapports des organisations confirment cette tendance. La collaboration entre les institutions financières, les prestataires de services de paiement numériques et les forces de l'ordre facilite les enquêtes, mais ne perturbe pas les incitations

financières qui alimentent les abus. En conséquence, les TF-CSEA restent rentables et reproductibles.

La synthèse conclut que le fait de concentrer la responsabilité principalement sur les institutions financières et de ne pas perturber directement les paiements numériques peut représenter une occasion manquée cruciale. Comblers cette lacune en matière de recherche et de politique pourrait permettre de déplacer les interventions en amont et de cibler les structures économiques qui permettent aux abus de persister à grande échelle. Les interventions financières constituent un élément prometteur d'un ensemble plus large d'initiatives politiques visant à améliorer la responsabilité des plateformes dans la lutte contre l'exploitation numérique.

CONCLUSION

Cette synthèse fournit l'évaluation la plus complète actuellement disponible des interventions TF-CSEA. Les données montrent que les mesures existantes réduisent les préjudices, mais restent inégales et incomplètes. La plupart des interventions se concentrent sur la détection des abus après les faits, et beaucoup moins s'attaquent aux systèmes qui permettent aux abus de persister, de se multiplier et de générer des profits.

Les outils techniques jouent un rôle central et peuvent fonctionner au-delà des frontières. Cependant, leur efficacité dépend de l'autorité juridique, de la sécurité de l'accès aux données, des garanties et de la capacité d'application. Les interventions comportementales et éducatives réduisent les risques et sensibilisent davantage, mais les preuves d'un changement de comportement durable restent limitées, en particulier dans les études longitudinales, en raison du financement limité de la recherche. Les cadres juridiques et réglementaires ont un impact maximal lorsqu'ils harmonisent les infractions et imposent des obligations contraignantes dans toutes les juridictions.

Le fossé le plus important en matière de recherche et de politique concerne les systèmes financiers. Malgré leur rôle central dans la facilitation des TF-CSEA, les interventions perturbent rarement les flux de paiement. Les approches actuelles se concentrent sur le traçage des transactions après que le préjudice a été causé plutôt que sur la prévention des abus en interrompant leur financement.

D'importantes lacunes subsistent, en particulier en ce qui concerne la perturbation des paiements et les résultats à long terme des interventions. Les études menées depuis la fin de l'évaluation n'ont pas été intégrées à cette analyse. Néanmoins, les conclusions établissent un consensus scientifique clair. Garantir la responsabilité des plateformes et réduire les TF-CSEA nécessite une autorité juridique coordonnée, des systèmes techniques évolutifs, une capacité d'application soutenue et des mesures décisives pour perturber les flux financiers qui alimentent ces abus.

RÉFÉRENCES

- [1] M. Lamond et al., “2025 Into the Light Index on Global Child Sexual Exploitation and Abuse: Supplemental Thematic Analysis Report,” Oct. 2025. [Online]. Available: <https://www.research.ed.ac.uk/en/publications/2025-into-the-light-index-on-global-child-sexual-exploitation-and/>
- [2] International Panel on the Information Environment [K. Pothong, S. Kaynak, D. Fry, S. Ghai, S. Livingstone, A. Phippen, C. R. Soriano, L. M. Given, P. N. Howard, M. Valente, S. Valenzuela (eds.)], “Detecting, Deterring, Investigating, and Prosecuting Technology-Facilitated Child Sexual Exploitation and Abuse: A Systematic Review,” Zurich, Switzerland: IPIE, 2026. Synthesis Report, SR2026.1, doi: 10.61452/UZUS7376.

REMERCIEMENTS

Contributeurs

Auteurs rédacteurs : Kruakae Pothong (scientifique consultante, Thaïlande/Royaume-Uni), Selcan Kaynak (présidente du groupe d'experts, Turquie), Deborah Fry (membre du groupe d'experts, États-Unis/Royaume-Uni), Sakshi Ghai (membre du groupe d'experts, Inde), Sonia Livingstone (membre du groupe d'experts, Royaume-Uni), Andy Phippen (membre du groupe d'experts, Royaume-Uni), Cheryll Ruth Soriano (membre du groupe d'experts, Philippines), Lisa M. Given (membre du comité scientifique et méthodologique de l'IPIE, Australie), Mariana Valente (présidente du groupe stratégique droit et politique de l'IPIE), Philip Howard (président-directeur général de l'IPIE, Canada/Royaume-Uni), Sebastián Valenzuela (directeur scientifique et président du comité scientifique et méthodologique de l'IPIE, Chili). Revues indépendantes : Elena Martellozzo et Sun Sun Lim. Revue juridique : David Kelly. Conception : Domenico Di Donna. Révision : Beverley Sykes. Nous remercions le secrétariat de l'IPIE pour son soutien : Lola Gimferrer, Jessica Gold, Egerton Neto, Wiktoria Schulz, Donna Seymour, Anna Staender et Alex Young.

Citation préférée

Le Résumé pour les décideurs politiques de l'IPIE fournit un aperçu de haut niveau de l'état des connaissances et est rédigé pour un large public. Un rapport de synthèse de l'IPIE utilise des techniques de méta-analyse scientifique, d'étude systématique et d'autres outils d'agrégation des preuves, de généralisation des connaissances et d'établissement d'un consensus scientifique. Il est rédigé à l'intention d'un public d'experts. Un rapport technique de l'IPIE aborde des questions de méthodologie ou fournit une analyse politique sur un problème réglementaire précis. Tous les rapports sont disponibles sur le site web de l'IPIE (www.IPIE.info).

Ce document doit être cité comme suit :

International Panel on the Information Environment [K. Pothong, S. Kaynak, D. Fry, L. M. Given, S. Ghai, S. Livingstone, A. Phippen, C. R. Soriano, P.N. Howard, M. Valente, S. Valenzuela (eds.)], « Lutter contre l'exploitation numérique : Recommandations pour prévenir et lutter contre l'exploitation et les abus sexuels des enfants facilités par la technologie », Zurich, Suisse : IPIE, 2026. Résumé à l'intention des décideurs politiques, SFP2026.1, doi: 10.61452/HPBS9755.

Financeurs

L'International Panel on the Information Environment (IPIE, Panel international sur l'environnement de l'information) remercie ses organismes de financement

pour leur soutien. Pour une liste complète des partenaires financiers, consultez le site www.ipie.info. Les opinions, résultats, conclusions ou recommandations exprimés dans ce rapport sont ceux de l'IPIE et ne reflètent pas nécessairement les points de vue des financeurs.

Déclaration d'intérêts

Les rapports de l'IPIE sont élaborés et révisés par un réseau mondial de chercheurs affiliés et de scientifiques consultants qui constituent des groupes scientifiques spécialisés et des équipes de collaborateurs. Tous les contributeurs et réviseurs remplissent des déclarations d'intérêts, qui sont examinées par l'IPIE aux stades appropriés du travail.

Informations sur les droits d'auteur



Ce document est placé sous licence Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0).

À PROPOS DE L'IPIE

L'International Panel on the Information Environment (IPIE) est une organisation scientifique indépendante et mondiale qui s'engage à fournir les connaissances scientifiques les plus exploitables sur les menaces qui pèsent sur l'environnement de l'information dans le monde. Basé en Suisse, l'IPIE a pour mission de fournir aux décideurs politiques, à l'industrie et à la société civile des évaluations scientifiques indépendantes sur l'environnement mondial de l'information en organisant, en évaluant et en valorisant la recherche, dans le but général d'améliorer l'environnement mondial de l'information. Des centaines de chercheurs du monde entier contribuent aux rapports de l'IPIE.

Pour plus d'informations, veuillez contacter l'International Panel on the Information Environment (IPIE), secretariat@ipie.info. Seefeldstrasse 123, B.P. 8034 Zurich, Suisse.



International Panel on
the Information
Environment

Seefeldstrasse 123
P.O. Box 8034 Zurich
Switzerland

