



CENTRE CANADIEN *de* PROTECTION DE L'ENFANCE™

Aider les familles. Protéger les enfants.

EXPÉRIENCES ET PERSPECTIVES DES ENFANTS SUR LA CYBERVIOLENCE SEXUELLE

PISTES DE RÉFLEXION EN VUE D'UN RÉGIME CANADIEN DE SÉCURITÉ EN LIGNE



CENTRE CANADIEN de PROTECTION DE L'ENFANCE™

Aider les familles. Protéger les enfants.

Les sources de données de cette enquête sont indiquées à la section « Méthodologie ». D'autres détails sur la méthodologie sont donnés à l'annexe A. La collecte des données a été réalisée durant la période du 29 avril au 20 mai 2025. L'interprétation des résultats de l'enquête a été entièrement réalisée en interne par le personnel du Centre canadien de protection de l'enfance inc. Sauf erreurs et omissions. Les mentions d'entreprises spécifiques dans les résultats reflètent les expériences rapportées par les victimes qui ont participé à l'enquête; d'autres ados pourraient avoir vécu des expériences différentes avec les mêmes entreprises.

© 2025, Centre canadien de protection de l'enfance inc. (615, chemin Academy, Winnipeg, Manitoba, Canada), à l'exception des photos de banque d'images, qui sont utilisées avec l'autorisation de leur banque d'origine. Tous droits réservés. Les photos de banque d'images montrent des mannequins et servent à illustrer le propos. Il est permis de conserver et d'imprimer des copies du présent document au besoin pour des activités non commerciales (fins personnelles, éducation, recherche, etc.) à condition d'attribuer la source de l'information au titulaire du droit d'auteur lorsque des extraits du présent document sont cités ou référencés dans un autre document. Il est interdit de publier une copie du présent document sur Internet, en tout ou en partie. Il est toutefois permis de publier un lien vers son emplacement en ligne sur le(s) site(s) Internet du Centre canadien de protection de l'enfance inc.

« Cyberaide.ca » est une marque du Centre canadien de protection de l'enfance inc. déposée au Canada. « CENTRE CANADIEN de PROTECTION DE L'ENFANCE » est utilisé au Canada comme marque de commerce du Centre canadien de protection de l'enfance inc. Toutes les autres marques citées appartiennent à leurs détenteurs respectifs.

TABLE DES MATIÈRES

Résumé des principaux constats et recommandations	2
Un mot sur le Centre canadien de protection de l'enfance	3
Introduction	4
Méthodologie	6
Résultats	7
Expériences de cyberviolence sexuelle	7
Formes de cyberviolence sexuelle	7
Implication d'adultes	11
Lieux de perpétration	11
Réponses aux incidents	13
Connaissance d'autres personnes ayant vécu une expérience de cyberviolence sexuelle	16
Opinions sur les solutions	17
Réglementation	17
Mesures à la portée des applications et des plateformes	17
Principales constatations et recommandations	19
Conclusion	25
Annexe A : Méthodologie de l'enquête	26
Annexe B : Questions de sélection	27
Références	28

RÉSUMÉ DES PRINCIPAUX CONSTATS ET RECOMMANDATIONS



Près de 9 victimes sur 10 (86 %) ont subi de la cyberviolence dans des environnements de messagerie privée.

Recommandation : Les régimes de sécurité en ligne doivent imposer des obligations de diligence adéquates aux fonctionnalités et services de communication privés.



Des incidents sont survenus sur de nombreuses applications et plateformes populaires; 2 victimes sur 5 (39 %) ont subi de la violence sexuelle sur Snapchat^{MD}.

Recommandation : Les régimes de sécurité en ligne doivent s'appliquer à un large éventail de plateformes et prévoir une gradation d'obligations proportionnée aux facteurs de risque anticipés ou connus propres à chaque service.



Parmi les victimes qui ont fait un signalement à une application ou à une plateforme pour demander la suppression d'images nues ou sexuelles, 2 sur 3 (67 %) ont attendu plus d'une journée pour que l'image soit supprimée. Les victimes estiment également que les applications et les plateformes devraient empêcher la distribution non consensuelle d'images nues ou sexuelles d'ados.

Recommandation : Les régimes de sécurité en ligne doivent énoncer clairement que les fournisseurs de services en ligne sont tenus de prendre les moyens voulus pour détecter proactivement les images nues ou sexuelles de personnes mineures qui leur sont signalées, les vérifier et les supprimer rapidement.



Au moins 1 victime sur 4 (25 %) a vécu une expérience de cyberviolence sexuelle aux mains d'un adulte.

Recommandation : Les régimes de sécurité en ligne doivent obliger les fournisseurs de services en ligne à prévenir les interactions en ligne potentiellement dangereuses entre adultes et enfants. Il y aurait lieu également d'envisager une modification au *Code criminel* du Canada pour inclure les tactiques de leurre.



Plus de 1 victime sur 2 (52 %) a reçu une image nue ou sexuelle non désirée, et 1 victime sur 6 (17 %) a été mise en scène dans une image truquée (nue ou sexuelle).

Recommandation : Modifier le *Code criminel* pour ériger en infraction la création et le partage d'images hypertruquées (nues ou sexuelles) et voir si les infractions existantes couvrent adéquatement le cyberexhibitionnisme.



Plus de 9 victimes sur 10 (93 %) estiment que le Canada devrait prendre des mesures législatives pour obliger les applications et les plateformes à prévenir la cyberviolence. La plupart d'entre elles croient aussi en l'utilité de mesures de sécurité.

Recommandation : Le Canada devrait se doter d'un régime de sécurité en ligne exigeant que les applications et les plateformes soient conçues dans une optique de sécurité et que les enfants y bénéficient de protections renforcées.



UN MOT SUR LE CENTRE CANADIEN DE PROTECTION DE L'ENFANCE

Le Centre canadien de protection de l'enfance (CCPE) est un organisme de bienfaisance national voué à la protection de tous les enfants. Il veut réduire l'exploitation et les abus sexuels d'enfants et offre à cette fin des programmes, des services et des ressources aux familles, aux éducateurs, aux organismes de services à l'enfance et aux forces policières du Canada ainsi qu'à d'autres acteurs du dossier. Le CCPE gère aussi Cyberaide!ca^{MD}, la centrale canadienne de signalement des cas d'exploitation et d'abus sexuels d'enfants sur Internet; Projet Arachnid^{MC}, une suite d'outils tournés vers les victimes pour lutter contre la prolifération croissante des images d'abus pédosexuels sur Internet; et AidezMoiSVP.ca^{MC}, qui vient en aide à des personnes touchées par la publication en ligne d'images nues d'elles lorsqu'elles étaient âgées de moins de 18 ans ou par d'autres formes de cyberviolence sexuelle.

À travers ces initiatives et d'autres programmes, le CCPE soutient les survivantes et survivants d'abus pédosexuels enregistrés et diffusés sur Internet. Notre travail auprès d'eux nous permet de recueillir des informations contextuelles cruciales sur la nature des abus pédosexuels et de les porter à la connaissance des acteurs de la protection de l'enfance.

INTRODUCTION

Au Canada, le nombre d'enfants* victimes de cyberviolence sexuelle est alarmant¹.

Le flot d'incidents rapportés quotidiennement par la police et les médias donne un aperçu de la nature de ces violences : des opérations policières nationales mènent à des arrestations massives pour des crimes perpétrés sur Internet en lien avec du matériel d'abus et d'exploitation pédosexuels (MAEP)², des milliers de garçons et de jeunes hommes sont la cible de tactiques de sextorsion financière³, et des filles sont mises en scène nues dans des images réalistes créées à l'aide d'applications et de plateformes d'intelligence artificielle (IA) et mises en circulation dans les écoles canadiennes⁴. On estime que près du tiers des jeunes de 13 à 18 ans au Canada ont subi une forme de cyberviolence sexuelle⁵, une donnée qui concorde généralement avec ce qu'on observe dans d'autres pays^{6,7}.

Les autorités et les chercheurs reconnaissent que la cyberviolence sexuelle contre les enfants est un problème majeur de sécurité et de santé publique^{8,9,10,11} car les enfants qui en sont victimes peuvent en subir des répercussions psychologiques, émotionnelles et sociales susceptibles de perdurer jusqu'à l'âge adulte^{12,13,14,15}. Lorsque cette violence s'accompagne de photos ou de vidéos nues ou sexuelles, la possibilité que ces images continuent de circuler sur Internet suscite encore plus de honte, d'autocritique et d'inquiétude chez les enfants victimes^{16,17,18,19} et les amène parfois à subir d'autres incidents en ligne et hors ligne^{20,21}. La cyberviolence sexuelle

contre les enfants viole donc leurs droits à la vie privée, à la sécurité et à la protection contre l'exploitation²².

La cyberviolence sexuelle contre les enfants n'est pourtant pas un corollaire inévitable de la numérisation grandissante de nos vies. Les gouvernements peuvent mettre en place des politiques réfléchies pour obliger les services en ligne et les entreprises de technologie à protéger les utilisateurs de leurs plateformes numériques et prévenir la cyberviolence. Cette approche diffère de la réponse pénale ou policière, qui s'applique de façon essentiellement réactive aux seuls incidents qui franchissent le seuil de la légalité, sans considération pour le large éventail d'actes non criminels – souvent qualifiés de « limites mais licites ».

Il est encourageant de constater que plusieurs pays commencent déjà à se doter d'une législation sur la sécurité en ligne^{23,24,25}. Le Canada, en revanche, n'a pas encore réussi à légiférer sur un cadre global et national de sécurité en ligne.



Photo d'un mamequin. Pour illustrer le texte.

* Dans cette enquête, les mots « enfant » et « enfants » désignent des personnes âgées de moins de 18 ans.

En 2024, après près de deux ans de consultations, le gouvernement du Canada a présenté le projet de loi C-63, qui aurait donné lieu à une nouvelle loi intitulée *Loi sur les préjudices en ligne*. Ce projet de loi prévoyait un certain nombre de mesures, notamment des obligations de diligence pour certains services en ligne, des modifications à la loi concernant la déclaration obligatoire en cas de découverte de MAEP et des modifications au *Code criminel* et à la *Loi canadienne sur les droits de la personne*²⁶.

La plus grande préoccupation du CCPE à l'égard du projet de loi C-63 était le nombre extrêmement limité de services en ligne qui auraient fait l'objet d'une surveillance réglementaire, ainsi que l'absence de précisions quant à la manière dont les services en ligne s'acquitteraient des obligations de diligence proposées en l'absence d'une obligation corollaire d'identifier leurs utilisateurs mineurs^{27,28}. Bien que le projet de loi C-63 soit mort au feuillet au début de 2025 en raison de la prorogation du Parlement, le gouvernement du Canada et les principaux partis politiques fédéraux maintiennent tous leur engagement envers la protection des enfants sur Internet^{29,30,31,32}.

Le contexte est donc propice pour le gouvernement du Canada de se doter d'un solide régime de sécurité en ligne qui palliera les lacunes des tentatives précédentes et qui tiendra compte des enseignements tirés des expériences d'autres gouvernements; un régime qui tiendra les services en ligne responsables des préjudices rendus possibles par leur entremise et qui les obligera à protéger leurs utilisateurs, en particulier les enfants, contre la cyberviolence sexuelle. Pour un maximum d'efficacité, un régime de sécurité en ligne doit également s'appuyer sur l'expérience vécue. À cette fin, le CCPE livre ici les résultats de son enquête auprès de quelque 1300 ados canadiens qui ont été victimes de cyberviolence sexuelle. Leurs réponses apportent de précieuses informations, notamment sur les applications et les plateformes en cause, la réponse des plateformes à leurs signalements et leurs motifs de non-signalement. Les victimes ont aussi été appelées à se prononcer sur l'opportunité pour le Canada de se doter d'une réglementation en matière de sécurité en ligne et à sopeser l'efficacité de diverses mesures.



Photo d'un mannequin. Pour illustrer le texte.

MÉTHODOLOGIE

Le CCPE a élaboré un questionnaire et a retenu les services de Léger, une firme d'études de marché et de sondages, pour mener une enquête anonyme en ligne. Le questionnaire de l'enquête était disponible en français et en anglais. Les 1279 participants devaient répondre aux critères suivants :

- être âgés de 13 à 17 ans (inclusivement) au moment de l'enquête;
- habiter au Canada;
- avoir subi au moins une forme de cyberviolence sexuelle (voir la section « Formes de cyberviolence sexuelle »).

Pour obtenir des résultats représentatifs au niveau national, nous avons pondéré les données selon l'âge, le sexe et la province/territoire en fonction des données démographiques du recensement canadien de 2021. Les données démographiques sont présentées à la figure 1 et de plus amples détails sur la méthodologie de l'enquête sont donnés à l'annexe A.

Toutes les différences observées entre les groupes portent sur des comparaisons entre des groupes d'au moins 100 participants et sont statistiquement significatives à $p < 0,05$. En raison des arrondis, les totaux ne sont pas nécessairement toujours égaux à 100 %.

Figure 1. Données démographiques sur les victimes

Sexe		Orientation sexuelle		Race/origine ethnique		Région	
Fille	52 %	Hétérosexuel·le	87 %	Blanc·che	72 %	Ontario	34 %
Garçon	47 %	Bisexuel·le	4 %	Noir·e	8 %	Québec	19 %
Autre genre	1 %	Lesbienne	1 %	Sud-Asiatique	4 %	Colombie-Britannique	16 %
		Gai	1 %	Chinois·e	4 %	Alberta	14 %
		Pansexuel·le	1 %	Premières Nations	4 %	Saskatchewan	4 %
		Asexuel·le	1 %	Philippin·e	3 %	Manitoba	3 %
		En questionnement	1 %	Latino-Américain·e	3 %	Nouveau-Brunswick	3 %
		Queer	<1 %	Métis·se	2 %	Nouvelle-Écosse	3 %
		Bispirituel·le	<1 %	Arabe	2 %	Terre-Neuve-et-Labrador	2 %
		Se décrit autrement	<1 %	Juif·ve	1 %	Île-du-Prince-Édouard	1 %
		Préfère ne pas répondre	2 %	Asiatique du Sud-Est	1 %	Territoires du Nord-Ouest	1 %
		Ne sait pas	2 %	Asiatique occidental·e	<1 %	Nunavut	<1 %
				Autre race/origine ethnique	2 %		
				Préfère ne pas répondre	1 %		
				Ne sait pas	<1 %		

RÉSULTATS

Expériences de cyberviolence sexuelle

Formes de cyberviolence sexuelle

Pour participer à cette enquête, les ados devaient avoir subi au moins une des sept formes de cyberviolence sexuelle définies dans l'enquête.

Propos sexuels non désirés

Les propos sexuels non désirés sont de loin la forme de cyberviolence sexuelle la plus souvent rapportée par les victimes. Dans le questionnaire, ce terme était défini comme suit : « Essayer de te faire parler de sexe ou te dire des choses à caractère sexuel », sans que la victime soit d'accord (figure 2). Quatre victimes sur 5 (79 %) ont subi cette forme de cyberviolence sexuelle, qui a touché particulièrement les ados issus de minorités sexuelles et de genre (88 % contre 77 % des ados issus des majorités sexuelles et de genre** ; la figure 3 montre les différences entre les groupes). Signalons que cette forme de cyberviolence est la seule pour laquelle nous disposions d'échantillons suffisamment grands pour permettre des comparaisons statistiques stables entre les ados issus de minorités sexuelles et de genre comparativement aux ados issus des majorités. D'autres études ont établi que la prévalence des abus pédosexuels sur Internet est plus élevée chez les ados issus de ces minorités que chez les jeunes issus des majorités^{33,34}.

Violence sexuelle par l'image

Les autres formes de cyberviolence définies dans l'enquête sont des formes de violence sexuelle par l'image. Elles se rapportent toutes à des « images de nudité ou à caractère sexuel », qui sont définies dans le questionnaire comme « des photos ou des vidéos de toi nue, partiellement nue, ou qui sont de nature sexuelle ou sexuellement abusive ». Certaines de ces formes de violence se rapportent à de « vraie[s] image[s] nue[s] ou à caractère sexuel », en ce sens qu'elles ont été prises lorsque la victime était nue, qu'elle se livrait à une activité sexuelle consensuelle ou qu'elle subissait des abus sexuels. À la différence, les « images truquées » (nues ou sexuelles) sont des images de la victime qui ont été modifiées pour représenter celle-ci comme si elle était nue, qu'elle se livrait à une activité sexuelle consensuelle ou qu'elle subissait des abus sexuels. Ces images, qu'on appelle aussi parfois « images nues hypertruquées » ou « hypertrucages sexuels », peuvent être créées à l'aide d'un simple outil de retouche photo ou encore d'une application ou d'une plateforme spécialisée de « nudification » ou de « déshabillage » qui utilise l'IA^{35,36}.



Photo d'un mannequin. Pour illustrer le texte.

**Les conversations sexuelles
non désirées ont touché
4 victimes sur 5**



Photo d'un mannequin. Pour illustrer le texte.

** Les ados issus de minorités sexuelles et de genre avaient soit une identité sexuelle minoritaire et une identité de genre minoritaire, soit ces deux identités. Les ados issus des majorités sexuelles et de genre n'avaient pas d'identité sexuelle minoritaire ni d'identité de genre minoritaire.

Images nues ou sexuelles non sollicitées

Plus d'une victime sur 2 (52 %) a reçu des images nues ou sexuelles non sollicitées sur Internet. Les ados plus âgés ont reçu de telles images dans des proportions sensiblement plus élevées (55 % des 15-17 ans contre 47 % des 13-14 ans). Cette forme de cyberviolence sexuelle – à laquelle on réfère souvent par les termes « images intimes non sollicitées », « cyberexhibitionnisme » ou « dick pics » (lorsqu'il s'agit d'images d'organes génitaux masculins) – a été érigée en infraction dans certains pays comme le Royaume-Uni³⁷. Le *Code criminel* du Canada prévoit certaines infractions relatives à la distribution d'images sexuelles à des enfants, mais il y aurait lieu de voir si ces infractions couvrent entièrement tous les préjudices qu'un incident de cyberexhibitionnisme peut entraîner. Il convient de noter que l'infraction d'attentat à la pudeur, qui s'applique parfois aux incidents survenus en ligne, ne protège que les enfants de moins de 16 ans.

Pressions pour envoyer des images nues ou sexuelles

Plus de 2 victimes sur 5 (44 %) ont subi des pressions de la part d'un internaute pour qu'elles lui envoient des images nues ou sexuelles. Cette forme de cyberviolence a touché davantage les ados plus âgés (47 % des 15-17 ans contre 39 % des 13-14 ans) et les filles (50 % contre 38 % des garçons).

Menaces de distribution d'images nues ou sexuelles

Près de 1 victime sur 4 (23 %) rapporte que quelqu'un l'a menacée de publier, d'envoyer à d'autres personnes ou de montrer à d'autres personnes des images nues ou sexuelles d'elle (vraies ou « truquées »). Ces incidents ont vraisemblablement pris de nombreuses formes, dont la sextorsion.



Photo d'un mannequin. Pour illustrer le texte.

La sextorsion (extorsion sexuelle) consiste à menacer de partager des images de nudité ou à caractère sexuel d'une victime avec d'autres personnes (par exemple, proches et amis de la victime) dans le but de l'obliger à faire quelque chose^{38,39}. Il peut s'agir de vraies images de la victime (qui peut les avoir envoyées elle-même au sextorqueur), d'images « truquées » de la victime créées par le sextorqueur ou d'images de quelqu'un d'autre que la victime, mais qu'une autre personne pourrait prendre comme des images de la victime (par exemple, des photos d'organes génitaux).

Il n'y a pas si longtemps, la sextorsion était un moyen utilisé principalement pour forcer la victime à envoyer d'autres images à caractère sexuel, à se livrer à des actes sexuels ou à rester dans une relation⁴⁰. Dans ce type de scénario, le sextorqueur est soit une personne que la victime connaît dans la vraie vie (par exemple, un ami ou un ancien partenaire), soit une personne que la victime connaît seulement virtuellement^{41,42}.

En 2022, la sextorsion a pris une tout autre tournure. Les forces policières^{43,44,45,46} et les centrales de signalement^{47,48} observaient une montée en puissance des cas de **sextorsion financière**. Cette forme de sextorsion est généralement le fait de membres de groupes criminels organisés qui se font passer pour des jeunes filles ou des femmes attirantes sur les médias sociaux et qui envoient des demandes d'amitié à des victimes potentielles, principalement des jeunes garçons et des jeunes hommes⁴⁹. En contexte de sextorsion financière, les sextorqueurs passent souvent à l'action dès la première conversation. Ils commencent par proposer coquinement à leurs cibles un échange d'images nues, après quoi ils les menacent aussitôt de distribuer les images obtenues si elles refusent de leur envoyer de l'argent ou des cartes-cadeaux. Les techniques utilisées sont extrêmement agressives. Certains menaceront la victime de ruiner sa vie si elle ne paie pas, d'autres vont lui présenter sous la forme d'un compte à rebours en temps réel (par exemple, 10... 9... 8...) le temps qu'il lui reste pour payer ou faire une promesse de paiement^{50,51}.

La sextorsion peut avoir des effets dévastateurs sur les victimes. Malheureusement, plusieurs ados canadiens se sont enlevé la vie après avoir été victimes de sextorsion classique ou financière^{52,53}.

Distribution non autorisée d'images nues ou sexuelles

Une victime sur 5 (20 %) rapporte que quelqu'un a publié, envoyé à d'autres personnes ou montré à d'autres personnes des images nues ou sexuelles d'elle sans son autorisation. C'est la seule forme de cyberviolence qui s'est avérée plus fréquente chez les garçons que chez les filles (24 % contre 17 %) et qui pourrait être couverte par l'infraction de « publication non consentuelle d'une image intime » du *Code criminel*, qui peut souvent englober d'autres infractions liées à la violence conjugale, à la sextorsion ou au MAEP.

La distribution non autorisée d'images intimes peut prendre diverses formes, par exemple :

- lorsqu'un sextorqueur met à exécution sa menace d'envoyer les images nues de sa victime aux proches et amis de celle-ci;
- lorsqu'une jeune personne texte une photo nue d'elle à une personne avec qui elle a une relation amoureuse en lui demandant de la garder privée, mais que cette dernière retransmet par la suite la photo à un groupe d'amis;
- lorsqu'une jeune personne se photographie nue et enregistre la photo sur son appareil, mais que son téléphone est ensuite piraté par quelqu'un qui envoie la photo à d'autres personnes sur les médias sociaux;
- lorsque quelqu'un utilise une application pour créer un hypertrucage sexuel d'une jeune personne et texte l'image ainsi créée à des camarades de classe;
- lorsque quelqu'un enregistre secrètement une jeune personne pendant qu'elle se livre à une activité sexuelle et publie ensuite la vidéo sur un site pornographique.

Dans certaines situations, des photos ou vidéos nues ou sexuelles d'un enfant, partagées sans consentement, pourraient être considérées comme du **matériel d'abus et d'exploitation pédosexuels (MAEP)**.

Création non autorisée d'images truquées (nues ou sexuelles)

Environ 1 victime sur 6 (17 %) rapporte avoir été mise en scène dans une image truquée (nue ou sexuelle) sans son autorisation. Rappelons que les hypertrucages sexuels peuvent être créés à l'aide d'un simple outil de retouche photo sur un téléphone ou un ordinateur, ou encore avec des applications ou des plateformes de « nudification » ou de « déshabillage » plus nouvelles qui utilisent l'IA.

Copies non autorisées de vraies images (nues ou sexuelles)

Près de 1 victime sur 7 (15 %) rapporte que quelqu'un a créé une copie d'une image réelle (nue ou sexuelle) d'elle en enregistrant une conversation vidéo avec elle ou en prenant une capture d'écran de sa photo sans son autorisation. Le **capping** peut être en cause dans certains cas. Cette pratique consiste à capturer secrètement des images d'une personne nue ou se livrant à une activité sexuelle pendant une conversation vidéo ou une diffusion en direct. Certaines images nues ou sexuelles d'ados peuvent aussi avoir été copiées sans leur autorisation dans le contexte d'un incident de sextorsion ou de distribution non consentuelle d'images intimes.



Photo des mannequins. Pour illustrer le texte.

Figure 2. Répartition des victimes par forme de cyberviolence sexuelle*ScreenQ1-3 : Le texte intégral de la question est reproduit à l'annexe B.*

	Oui	Non	Je ne sais pas	Je préfère ne pas répondre
Essayer de te faire parler de sexe ou te dire des choses à caractère sexuel?	79 %	18 %	2 %	1 %
T'envoyer une photo ou vidéo à caractère sexuel ou de nudité? Par exemple, une photo d'organes génitaux ou une vidéo de personnes ayant des rapports sexuels.	52 %	46 %	1 %	1 %
Faire pression sur toi pour que tu lui envoies des images de toi nu-e ou à caractère sexuel (vraies ou truquées)?	44 %	52 %	2 %	2 %
Menacer de publier, d'envoyer ou de montrer à d'autres des images de toi nu-e ou à caractère sexuel (vraies ou truquées)?	23 %	73 %	3 %	1 %
Publier, envoyer ou montrer à d'autres une image de toi nu-e ou à caractère sexuel (vraie ou truquée), sans ton autorisation?	20 %	70 %	9 %	1 %
Créer une image truquée de toi nu-e ou à caractère sexuel en éditant ou en modifiant une image de toi?	17 %	73 %	9 %	1 %
Prendre une vraie image nue ou à caractère sexuel de toi en enregistrant une vidéo en direct ou en faisant une capture d'écran?	15 %	78 %	6 %	1 %

Figure 3. Répartition des victimes par forme de cyberviolence sexuelle – comparaisons entre les groupes*ScreenQ1-3 : Le texte intégral de la question est reproduit à l'annexe B.*

	Ensemble des victimes	Âge		Sexe		Minorités sexuelles et de genre	
		13-14	15-17	Garçon	Fille	Non	Oui
Essayer de te faire parler de sexe ou te dire des choses à caractère sexuel?	79 %	76 %	80 %	73 %	84 %	77 %	88 %
T'envoyer une photo ou vidéo à caractère sexuel ou de nudité? Par exemple, une photo d'organes génitaux ou une vidéo de personnes ayant des rapports sexuels.	52 %	47 %	55 %	53 %	51 %	52 %	56 %*
Faire pression sur toi pour que tu lui envoies des images de toi nu-e ou à caractère sexuel (vraies ou truquées)?	44 %	39 %	47 %	38 %	50 %	44 %	52 %*
Menacer de publier, d'envoyer ou de montrer à d'autres des images de toi nu-e ou à caractère sexuel (vraies ou truquées)?	23 %	22 %	24 %	23 %	23 %	23 %	27 %*
Publier, envoyer ou montrer à d'autres une image de toi nu-e ou à caractère sexuel (vraie ou truquée), sans ton autorisation?	20 %	20 %*	21 %	24 %	17 %	21 %	17 %*
Créer une image truquée de toi nu-e ou à caractère sexuel en éditant ou en modifiant une image de toi?	17 %	14 %*	19 %	18 %	16 %	17 %	19 %*
Prendre une vraie image nue ou à caractère sexuel de toi en enregistrant une vidéo en direct ou en faisant une capture d'écran?	15 %	11 %*	16 %	16 %	14 %*	14 %	16 %*

N.B. - *Taille du sous-groupe : < 100



Implication d'adultes

Une victime sur 4 (25 %) rapporte que, de tous les incidents de cyberviolence sexuelle qu'elle a subis, il est arrivé au moins une fois que l'auteur était un adulte (figure 4); ces victimes peuvent également avoir été la cible d'autres enfants. Une victime sur 5 (21 %) ne savait pas si un adulte s'en était déjà pris à elle, et plus de la moitié (53 %) disent n'avoir jamais subi de cyberviolence sexuelle de la part d'un adulte. On peut donc en déduire que ces victimes ont été la cible d'un autre enfant, ce qui, selon les données sur les crimes signalés à la police, n'est pas rare dans le cas de plusieurs formes de cyberviolence sexuelle, comme la distribution non consensuelle d'images intimes⁵⁴. Il est possible que certaines de ces victimes aient été la cible d'adultes qui se faisaient passer pour des enfants.

Une victime sur 4 a vécu une expérience de cyberviolence sexuelle aux mains d'un adulte

Figure 4. Répartition des victimes selon que l'auteur était ou non une personne adulte

Q4. Lorsque tu as vécu les expériences ci-dessus, est-ce un-e adulte qui t'a fait cela?

Oui	25 %
Non	53 %
Je ne sais pas	21 %
Je préfère ne pas répondre	1 %

Lieux de perpétration

Applications et plateformes

Snapchat est la plateforme sur laquelle les victimes ont le plus souvent subi de la violence sexuelle (figure 5); 2 victimes sur 5 (39 %) ont subi de la violence sur cette plateforme. Les filles sont particulièrement touchées : 46 % d'entre elles contre 32 % des garçons ont subi de la violence sexuelle sur Snapchat. Signalons également que Snapchat dépasse de près du double la somme des mentions récoltées par les deuxième et troisième plateformes les plus citées, à savoir Instagram^{MD} (20 %) et Facebook^{MD} (20 %). Les garçons sont plus nombreux que les filles à avoir subi de la violence sexuelle sur Facebook (23 % contre 18 %).

La liste des applications et des plateformes énumérées à la figure 5 montre clairement, comme d'autres études ont pu le constater^{55,56}, que la violence sexuelle contre les ados ne sévit pas que dans les coins les plus sombres d'Internet. Elle déferle aussi sur des plateformes et des applications bien connues de médias sociaux, de jeu et de messagerie privée.

Deux victimes sur 5 ont subi de la violence sexuelle sur Snapchat

Au moins 2 fois plus de victimes ont subi de la violence sexuelle sur Snapchat que sur n'importe quelle autre plateforme

Figure 5. Répartition des victimes pour chaque application et plateforme

Q5. En pensant aux expériences que tu nous as dit avoir vécues en ligne, sur quelles applications ou plateformes se sont-elles produites? Sélectionne toutes les réponses qui s'appliquent.

Snapchat ^{MD}	39 %	X ^{MC} (anciennement Twitter)	3 %
Instagram ^{MD}	20 %	Google Hangouts ^{MD} , Meet ^{MD} ou Chat ^{MD}	3 %
Facebook ^{MD}	20 %	Telegram ^{MD}	3 %
TikTok ^{MD}	15 %	Twitch ^{MD}	3 %
Discord ^{MD}	14 %	Reddit ^{MD}	2 %
Messenger ^{MC} (Facebook Messenger)	10 %	Pinterest ^{MD}	2 %
WhatsApp ^{MD}	9 %	Chatroulette ^{MC}	1 %
Roblox ^{MD}	8 %	Kik ^{MD}	1 %
Call of Duty ^{MD}	7 %	Signal ^{MC}	1 %
Fortnite ^{MD}	7 %	Tumblr ^{MD}	1 %
YouTube ^{MD}	6 %	Wizz ^{MC}	1 %
iMessage ^{MD} ou FaceTime ^{MD}	5 %	Autre application ou plateforme	4 %
Minecraft ^{MD}	4 %	Je ne sais pas	3 %
Grand Theft Auto ^{MD}	3 %	Je préfère ne pas répondre	2 %

Environnements en ligne

Certaines des applications et plateformes énumérées à la figure 5 (par exemple, les applications de messagerie privée Facebook Messenger^{MC}, WhatsApp^{MD} et iMessage^{MD}) sont des environnements privés. La plupart des autres applications et plateformes offrent non seulement des environnements de communication privés (messages privés, diffusions en direct privées, conversations de groupe ou groupes privés), mais aussi des espaces de communication publics (publications, fils, forums, commentaires, jeux) ouverts à tout le monde. C'est le cas de Snapchat, Facebook et Instagram, entre autres.

Pour la grande majorité des victimes, soit près de 9 sur 10 (86 %), les incidents de cyberviolence sexuelle se sont produits dans des environnements de communication privés (figure 6). Les adolescents plus âgés (89 % des 15-17 ans contre 82 % des 13-14 ans) sont encore plus touchés.

Un peu moins de 1 victime sur 5 (19 %) a subi de la cyberviolence sexuelle dans des environnements de communication publics.

Ces résultats concordent avec les informations contenues dans les milliers de signalements traités par Cyberaide.ca depuis plusieurs années : la plupart des incidents de cyberviolence sexuelle contre des enfants débutent ou sont rendus possibles dans le contexte de communications privées⁵⁷.

Près de 9 victimes sur 10 ont subi de la cyberviolence dans des environnements de messagerie privée

Cyberaide.ca est la centrale canadienne de signalement des cas d'exploitation et d'abus sexuels d'enfants sur Internet. Ce programme du CCPE reçoit et traite des signalements émanant du public concernant des activités illégales – photos et vidéos d'abus pédosexuels, trafic d'enfants, leurre informatique, distribution non consensuelle d'images intimes, etc. Les informations pertinentes sont ensuite retransmises aux forces policières et aux agences de protection de l'enfance pour enquête et suivi.

cyberaide!ca^{MD}

Figure 6. Répartition des victimes selon qu'elles ont subi de la violence sexuelle dans un environnement public ou privé

Q6. Toujours en pensant aux expériences que tu nous as dit avoir vécues en ligne, dans quel espace sur l'application ou la plateforme est-ce arrivé?

En privé (par exemple, par des messages personnels ou dans des conversations de groupe)	76 %	En privé (NET)	86 %
En privé et en public	11 %		
En public (par exemple, dans des publications, des forums ou des commentaires)	9 %	En public (NET)	19 %
Je ne sais pas	3 %		
Je préfère ne pas répondre	1 %		

Réponses aux incidents

Les victimes ont également été interrogées à savoir quelles mesures elles avaient prises, le cas échéant, à la suite de leur expérience de cyberviolence sexuelle. Il est encourageant de constater que la plupart ont cherché au moins une forme d'aide ou de soutien à un moment ou l'autre (figure 7).

Plus de 1 victime sur 2 (55 %) a rapporté la situation à une personne de confiance (par exemple, un ami, un parent ou un enseignant), les filles davantage que les garçons (59 % contre 51 %). Certaines victimes ont signalé la situation à la police (8 %)*** ou aux sites Cyberaide.ca ou AidezMoiSVP.ca du CCPE (4 %). Ces deux dernières données mettent en évidence le sous-signallement des incidents de cyberviolence sexuelle⁵⁸ et, corollairement, le fait que les données de signalement ne représentent qu'une petite fraction du nombre réel d'incidents de cyberviolence sexuelle perpétrés contre des ados au Canada.

Les victimes ont aussi été interrogées sur les démarches qu'elles ont entreprises auprès des applis ou des plateformes après leur expérience de cyberviolence sexuelle. Deux victimes sur 5 (38 %) – en particulier les filles (43 % contre 34 % des garçons) – se sont désabonnées du ou des comptes fautifs, les ont supprimés ou les ont mis en sommeil (ces mesures ne sont toutefois pas offertes sur toutes les plateformes). Seule 1 victime sur 5 (20 %) a signalé l'incident à la plateforme en cause. Les résultats de ces signalements sont détaillés dans les sections suivantes, ainsi que les raisons pour lesquelles la plupart de ces victimes n'ont pas fait de signalement à la plateforme en cause.

Un peu plus de 1 victime sur 5 (22 %) n'a parlé à personne de son expérience de cyberviolence sexuelle et ne l'a signalée nulle part.



Photo d'un mannequin. Pour illustrer le texte.

Une victime sur 5 n'a parlé à personne des cyberviolences sexuelles qu'elle a subies et ne les a signalées nulle part

*** Les formes de cyberviolence sexuelle dont il est question dans notre enquête ne constituent pas toutes des actes criminels au Canada.

Figure 7. Répartition des victimes selon les démarches qu'elles ont entreprises après leur expérience de cyberviolence sexuelle

Q7. Toujours en pensant aux expériences que tu nous as dit avoir vécues en ligne, est-ce que tu as fait l'une ou l'autre des choses suivantes? Sélectionne toutes les réponses qui s'appliquent.

J'en ai parlé à quelqu'un en qui j'ai confiance (par exemple, un-e ami-e, parent ou tuteur/tutrice, enseignant-e)	55 %
Je me suis désabonné-e ou j'ai bloqué, supprimé ou masqué la/les personne(s) en ligne	38 %
Je n'en ai parlé à personne ni signalé à qui que ce soit	22 %
Je l'ai signalé aux applications ou aux plateformes où cela s'est produit	20 %
Je l'ai signalé à la police	8 %
Je l'ai signalé à Cyberaide.ca ou AidezMoiSVP.ca	4 %
Aucune de ces réponses	5 %
Je ne sais pas	1 %
Je préfère ne pas répondre	1 %

Résultats des signalements aux applications et aux plateformes

Résolution

Beaucoup d'applications et de plateformes offrent des options pour signaler certains types de problèmes rencontrés par les utilisateurs, mais ces options s'avèrent souvent limitées et disparates^{59,60,61,62}.

Comme indiqué précédemment, 20 % (n=275) des victimes ont signalé l'incident qu'elles ont subi à l'application ou à la plateforme sur laquelle il est survenu. Elles ont signalé collectivement 514 incidents (figure 8). Dans la moitié des cas (53 %), les problèmes ont cessé après que la victime a signalé la situation à la plateforme, peut-être à la suite d'une intervention efficace de la part de la plateforme (par exemple, bannissement définitif du compte fautif) ou du fait que les problèmes avaient déjà cessé lorsque la victime les a signalés. Dans plus du tiers des cas (38 %), le signalement à la plateforme n'a pas mis fin à toutes les violences sexuelles subies par les ados sur ces plateformes.



Figure 8. Résolution des signalements aux applications et aux plateformes
Sur les 514 incidents signalés aux applications ou aux plateformes par 275 victimes

Q8. As-tu signalé ce(s) problème(s) à [plateformes indiquées à la Q5]?

Q8b. [Pour chacune des plateformes indiquées à la Q8 :] Que s'est-il passé après que tu as signalé le(s) problème(s)?

Le(s) problème(s) a/ont cessé	53 %
Le(s) problème(s) n'a/n'ont pas cessé	21 %
Le(s) problème(s) a/ont cessé parfois	17 %
Je ne sais pas	7 %
Je préfère ne pas répondre	2 %

Suppression d'images nues ou sexuelles

Cent trente-cinq victimes ont demandé à une application ou à une plateforme de supprimer une image nue ou sexuelle. Ces images doivent absolument être supprimées rapidement pour freiner leur distribution et prévenir d'autres incidents; plus elles sont supprimées rapidement, moins il y a de chances que d'autres personnes puissent les voir, les commenter de manière désobligeante, en faire des copies ou les partager sur d'autres plateformes. C'est pour ces raisons que plusieurs gouvernements ont adopté ou proposé des lois obligeant les services en ligne à supprimer les images nues ou sexuelles d'enfants dans un délai de 24 à 48 heures après avoir été informés de leur présence sur leurs serveurs^{63,64,65,66}.

Les victimes ont été interrogées à savoir quel avait été le plus long délai écoulé entre le signalement d'une image nue ou sexuelle à un service en ligne et sa suppression (figure 9). Pour 1 victime sur 4 (25 %), ce délai a été d'un jour au plus. Malheureusement, la plupart des autres victimes ont dû attendre beaucoup plus longtemps – de 1 à 6 jours pour 2 victimes sur 5 (40 %), d'une semaine à un mois pour plus d'une sur 10 (12 %) et plus d'un mois pour près d'une sur 10 (8 %). Au moment de l'enquête, 1 victime sur 20 (5 %) parmi ces dernières attendait toujours la suppression de ses images.

Parmi les victimes qui ont fait un signalement à une application ou à une plateforme pour demander la suppression d'images nues ou sexuelles, 2 sur 3 ont attendu plus d'une journée pour que l'image soit supprimée

Figure 9. Durée du plus long délai écoulé entre le signalement d'une image nue ou sexuelle à une application ou à une plateforme et sa suppression

Sur l'ensemble des victimes qui ont signalé une image nue ou sexuelle à une plateforme (n=135)

Q10. Lorsque tu as fait un signalement à une application ou plateforme, était-ce pour demander de retirer une image de toi nu-e ou à caractère sexuel? Si oui, combien de temps a-t-il fallu pour que l'application ou la plateforme retire une image de toi nu-e ou à caractère sexuel?

Moins d'une journée	25 %
Plus d'un jour (NET)	67 %
De 1 à 6 jours	40 %
De 1 semaine à 1 mois	12 %
Plus d'un mois	8 %
L'image n'a pas été supprimée	5 %



Motifs de non-signalement

Mille quatre victimes n'ont pas signalé leur expérience de cyberviolence sexuelle à l'application ou à la plateforme en cause. Interrogées sur leurs motifs de non-signalement, la plupart ont dit qu'elles ne pensaient pas que l'application ou la plateforme les aiderait (43 %; figure 10). Ce motif a été évoqué plus souvent par les filles que par les garçons (48 % contre 37 %). Parmi les autres principaux motifs invoqués, 30 % des victimes ont répondu qu'elles ignoraient la marche à suivre et 21 % ne voulaient pas que quelqu'un sache qu'elles avaient fait un signalement, peut-être par crainte de représailles de la part de l'auteur de l'incident⁶⁷. Même s'il est visé par un signalement anonyme, l'auteur de l'incident peut quand même être en mesure de deviner l'identité de la victime d'après le moment et la nature de la réponse de la plateforme (par exemple, bannir l'utilisateur fautif pour avoir partagé des images nues d'enfants) et avoir explicitement menacé la victime de conséquences en cas de dévoilement⁶⁸.

Certaines victimes n'ont pas fait de signalement par crainte de se faire bannir de la plateforme (13 %; une telle situation pourrait se produire, par exemple, si la personne a désobéi aux règles de la plateforme en partageant des images nues d'elle-même) ou parce que la plateforme ne disposait d'aucun mécanisme de signalement pour de tels incidents (9 %).

Figure 10. Motifs de non-signalement

Sur l'ensemble des victimes qui n'ont jamais signalé leur expérience à une plateforme (n=1004)

Q9 : Tu as dit que tu n'as pas signalé les expériences qui te sont arrivées en ligne. Lesquelles des raisons suivantes expliquent pourquoi tu n'as pas signalé ces incidents à l'application ou la plateforme? Sélectionne toutes les réponses qui s'appliquent.

Je n'ai pas pensé que l'appli ou la plateforme m'aiderait	43 %
Je ne savais pas comment faire un signalement	30 %
Je ne voulais pas que quelqu'un sache que j'avais fait un signalement	21 %
J'ai eu peur qu'on m'interdise l'accès	13 %
Il n'y avait nulle part où le signaler	9 %
Une autre raison	9 %
Je ne sais pas	12 %
Je préfère ne pas répondre	3 %

Connaissance d'autres personnes ayant vécu une expérience de cyberviolence sexuelle

En plus d'avoir elles-mêmes vécu une expérience de cyberviolence sexuelle, plus de 2 victimes sur 3 (69 %) connaissaient personnellement une autre personne ayant subi au moins une des formes de cyberviolence sexuelle définies dans l'enquête (figure 11). C'était plus souvent le cas chez les filles que chez les garçons (74 % contre 63 %).

Deux victimes sur 3
connaissent une autre personne qui a
vécu une expérience de cyberviolence
sexuelle

Figure 11. Répartition des victimes selon qu'elles connaissent ou non d'autres victimes de cyberviolence sexuelle

Q10b. Et connais-tu personnellement quelqu'un (autre que toi) à qui les choses suivantes sont arrivées en ligne d'une manière que cette personne ne souhaitait pas et sans son autorisation?

Oui, pour au moins une forme de cyberviolence sexuelle	69 %
Non, ne sait pas ou préfère ne pas répondre dans tous les cas	31 %



Opinions sur les solutions

La grande majorité des ados victimes de cyberviolence sexuelle sont favorables à la réglementation des entreprises de technologie et estiment que les applications et les plateformes pourraient faire beaucoup de choses pour empêcher d'autres ados de subir le même sort.

Réglementation

De plus en plus, les fournisseurs de services en ligne sont légalement tenus de respecter des normes de sécurité conçues pour protéger leurs utilisateurs, en particulier les enfants^{69,70,71}. Le Canada ne dispose toujours pas de telles mesures, et les ados victimes de cyberviolence sexuelle veulent que ça change : plus de 9 victimes sur 10 (93 %) conviennent que le Canada devrait prendre des mesures législatives pour obliger les applications et les plateformes à prévenir la cyberviolence. De ce nombre, 3 sur 4 (74 %) se disent fortement d'accord (figure 12). Il est à noter que le soutien à la réglementation des services en ligne au Canada semble plus fort chez les jeunes que chez les adultes^{72,73}.

Neuf victimes sur 10 pensent que le Canada devrait prendre des mesures législatives pour obliger les applications et les plateformes à prévenir la cyberviolence

Figure 12. Répartition des victimes selon leur degré d'appui à la réglementation

Q10c : À quel point es-tu d'accord ou en désaccord avec ce qui suit? Au Canada, il devrait y avoir des lois qui obligent les applications et les plateformes à prévenir les abus.

D'accord (NET)	93 %
Tout à fait d'accord	74 %
Plutôt d'accord	19 %
Ni d'accord ni en désaccord	4 %
Plutôt en désaccord	1 %
Tout à fait en désaccord	1 %
Je ne sais pas	1 %
Je préfère ne pas répondre	0 %

Mesures à la portée des applications et des plateformes

De manière volontaire ou par force de loi, les applications et les plateformes en ligne peuvent prendre des mesures pour rendre leurs services plus sûrs. La grande majorité des ados victimes de cyberviolence sexuelle estiment que les applications et les plateformes pourraient faire beaucoup de choses pour empêcher d'autres ados de subir le même sort (figure 13).

Plusieurs de ces mesures entrent dans la catégorie « sécurité dès la conception ». Il s'agit d'une approche dans laquelle les applications et les plateformes anticipent les dérives et conçoivent leurs services de manière à réduire au minimum les risques d'utilisation de leurs services à des fins malveillantes. Ces mesures ont été jugées utiles par au moins 85 % des victimes. La mesure que les victimes jugent la plus utile consiste à empêcher que des ados puissent être contactés par une personne qu'ils ont bloquée ou signalée (92 %). Les filles sont plus nombreuses que les garçons à croire en l'utilité de cette mesure (94 % contre 90 %). Une étude antérieure remet toutefois en question l'efficacité du blocage ou du signalement d'utilisateurs problématiques, ayant constaté que la moitié des enfants ont été recontactés par ces mêmes utilisateurs, soit à partir d'un nouveau compte sur la même plateforme, soit à partir d'un nouveau compte sur une autre plateforme⁷⁴. Les victimes interrogées dans le cadre de cette enquête pensent également qu'il serait utile que les applications et les plateformes soient conçues à la base dans une optique de sécurité pour empêcher : que des images nues ou sexuelles d'ados puissent être partagées sans leur autorisation (91 %); que des utilisateurs puissent créer des comptes en se faisant passer pour autrui (90 %); que des inconnus puissent entrer en contact avec des ados ou leur envoyer des messages (85 %).

Les victimes voient d'un bon œil la mise à disposition d'outils bien conçus pour signaler les problèmes et les abus. Environ 9 victimes sur 10 croient en l'utilité des mesures suivantes pour réduire la cyberviolence sexuelle contre les ados, si les applications et les plateformes en étaient dotées : proposer des moyens faciles pour leur signaler les problèmes (92 %; 94 % des filles contre 90 % des garçons); agir rapidement pour aider les ados qui signalent un problème (91 %; 93 % des filles contre 88 % des garçons); s'assurer qu'une vraie personne aide les ados qui signalent un problème (87 %).

Environ 3 victimes sur 4 (74 %) pensent que les applications et les plateformes préviendraient davantage la cyberviolence sexuelle contre les ados si elles étaient obligées de proposer aux parents des moyens de surveiller les activités en ligne de leurs enfants. Cette mesure est celle que les victimes jugent la moins utile. Une explication possible serait qu'elles n'ont envie que leurs parents surveillent leurs comptes. Les victimes qui doutent de l'efficacité des outils de surveillance parentale parlent peut-être aussi en connaissance de cause : à travers Cyberaide.ca et d'AidezMoiSVP.ca, nous avons souvent connaissance de cas où l'utilisation d'outils de surveillance par les parents n'a pas empêché leurs enfants de subir de la cyberviolence sexuelle. Dans les faits, ces outils ne peuvent rien contre de nombreuses menaces à la sécurité des enfants, notamment la possibilité pour des étrangers adultes d'entrer en contact avec de jeunes utilisateurs^{75,76}.

Figure 13. Répartition des victimes selon leur degré d'appui à diverses mesures de sécurité destinées à prévenir la cyberviolence sexuelle contre des ados

Q11. Toujours en pensant à ce qui peut arriver aux gens en ligne, comme quelqu'un qui leur parle d'une manière sexuelle sans qu'ils le veuillent ou qui partage des images d'eux nus ou à caractère sexuel sans leur permission. À ton avis, à quel point chacune des idées suivantes serait-elle utile pour empêcher que les ados subissent ce type de choses? Obliger les applications et les plateformes à...

	Utile (NET)	Très utile	Plutôt utile	Ni utile ni inutile	Plutôt inutile	Très inutile	Je ne sais pas	Je préfère ne pas répondre
Empêcher que les ados soient contacté·e·s par des personnes qu'ils/elles ont bloquées ou signalées	92 %	72 %	20 %	4 %	2 %	1 %	1 %	0 %
Proposer des moyens faciles pour leur signaler des problèmes	92 %	67 %	25 %	4 %	2 %	1 %	1 %	0 %
Empêcher que des images nues ou sexuelles d'ados soient partagées sans leur autorisation	91 %	72 %	19 %	4 %	2 %	1 %	1 %	0 %
Agir rapidement pour aider les ados qui leur signalent un problème	91 %	69 %	22 %	5 %	2 %	1 %	2 %	0 %
Empêcher les gens de créer des comptes en prétendant être quelqu'un d'autre	90 %	69 %	21 %	6 %	2 %	1 %	1 %	0 %
S'assurer qu'une vraie personne aide les ados qui signalent un problème	87 %	59 %	28 %	6 %	2 %	1 %	3 %	0 %
Empêcher les inconnus d'entrer en contact avec les ados ou de leur envoyer des messages	85 %	62 %	22 %	8 %	3 %	2 %	2 %	0 %
Proposer aux parents/tuteurs des moyens de surveiller les activités en ligne des ados	74 %	44 %	30 %	13 %	6 %	4 %	2 %	1 %

PRINCIPALES CONSTATATIONS ET RECOMMANDATIONS

Ce rapport fait état des expériences d'ados canadiens qui ont été victimes de cyberviolence sexuelle. Des adultes comme d'autres jeunes de leur âge leur ont fait subir des propos sexuels non désirés et toutes sortes de violences par l'image, comme leur envoyer des images nues non sollicitées ou les menacer de partager des images nues d'elles avec d'autres personnes. Ces formes de cyberviolence s'avèrent souvent aussi des manifestations de violence sexiste qui reflètent des schémas de pouvoir et de contrôle et qui touchent les filles de manière disproportionnée. Il existe une exception notoire : les garçons sont plus touchés que les filles par la distribution non consentie d'images nues ou sexuelles, peut-être en raison de la montée de la sextorsion financière. Mais le plus inquiétant, c'est que les ados ont subi ces violences sur les plateformes et les applications de médias sociaux, de jeu et de messagerie privée les plus populaires au Canada.

La grande majorité des victimes n'ont pas signalé les violences qu'elles ont subies sur ces applications et plateformes, souvent parce qu'elles ne pensaient pas que les plateformes pouvaient les aider, et, parfois, parce qu'elles ne savaient pas comment s'y prendre pour faire un signalement. Malheureusement, beaucoup de celles qui ont néanmoins signalé ces violences à un service en ligne rapportent que leurs démarches n'ont pas permis de résoudre le problème ou d'obtenir la suppression rapide de leurs images nues ou sexuelles.

Ces résultats montrent une fois de plus que les fabricants d'applications et plateformes en ligne peuvent et doivent faire davantage pour empêcher les ados de subir des violences sexuelles dans les environnements numériques qu'ils conçoivent, et qu'ils doivent aussi améliorer leur réponse aux incidents qui leur sont signalés. De fait, la plupart des victimes estiment que le Canada devrait se doter de lois pour obliger les applications et les plateformes à prévenir ces violences. Elles sont aussi très en faveur de diverses solutions potentielles.

Les recommandations issues de nos constats visent donc à nourrir la réflexion autour de l'élaboration d'un éventuel régime de la sécurité en ligne au Canada. Nos recommandations s'appuient sur les perspectives et les expériences d'ados victimes de cyberviolence sexuelle.

Nous invitons les fournisseurs de services en ligne à adopter volontairement les éléments techniques de nos recommandations. Cependant, devant l'incapacité chronique des entreprises de technologie à s'occuper sérieusement de la sécurité des enfants⁷⁷, nous adressons nos recommandations aux gouvernements et aux décideurs politiques qui ont la capacité de mettre en place une législation sur la sécurité en ligne.

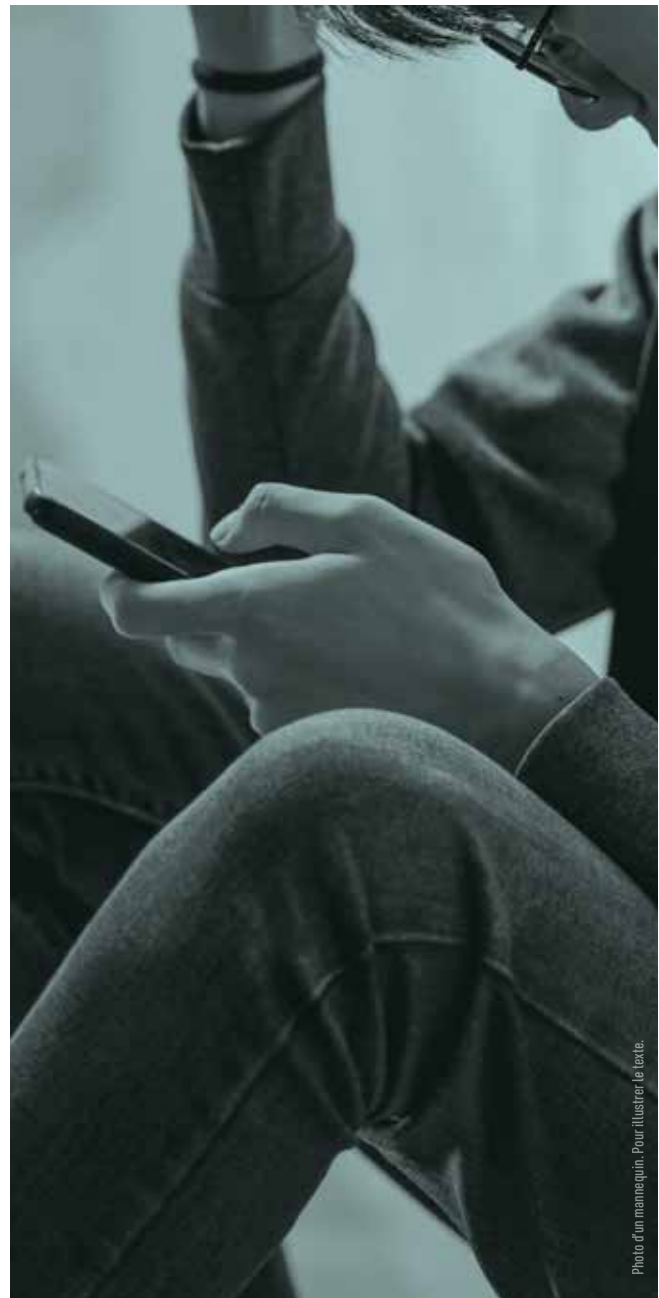


Photo d'un mannequin. Pour illustrer le texte.

Près de 9 victimes sur 10 (86 %) ont subi de la cyberviolence dans des environnements de messagerie privée.

Recommandation : Les régimes de sécurité en ligne doivent imposer des obligations de diligence adéquates aux fonctionnalités et services de communication privés.

Si un régime de sécurité a pour objectif de protéger les enfants et de prévenir la cyberviolence, alors il doit accorder une attention particulière au fait que les fonctionnalités et services de communication privés portent une part considérable de responsabilité dans la facilitation de la cyberviolence sexuelle contre les ados au Canada.

Les victimes interrogées dans cette enquête ont pour la plupart subi des incidents de violence sexuelle dans des environnements numériques privés; près de 9 sur 10 d'entre elles (86 %) rapportent que les incidents se sont produits sur des services de messagerie privée, par exemple dans le contexte d'un échange de messages privés ou de conversations au sein de groupes fermés. Ce constat reflète également les tendances observées dans les milliers de signalements examinés par notre organisation dans le cadre des activités de Cyberaide.ca⁷⁸.

Il faut savoir que certains services en ligne (par exemple, WhatsApp, Signal^{MC} et iMessage) sont destinés exclusivement aux communications privées, tandis que d'autres services (par exemple, Snapchat, Instagram et Discord^{MD}) offrent à la fois des fonctionnalités de communication privée et des fonctionnalités de communication publique. Les régimes de sécurité en ligne doivent s'appliquer également à ces deux fonctionnalités et services de communication privés. Pour réduire les risques, on pourrait par exemple exiger que ces fonctionnalités et services :

- permettent aux utilisateurs de signaler les abus commis par d'autres utilisateurs;
- resserrent les paramètres de sécurité et de confidentialité par défaut, au lieu de privilégier des réglages visant à maximiser l'engagement;
- utilisent les données de signalement (par exemple, les comptes qui ont été bloqués ou signalés par de nombreux utilisateurs) pour bannir les utilisateurs problématiques de leurs plateformes;
- mettent les utilisateurs en garde lorsque, par exemple, un message vient d'un compte qui a été créé récemment ou qui fait l'objet de nombreuses plaintes de la part d'autres utilisateurs;
- permettent aux utilisateurs de délimiter géographiquement leur réseau de communication.

Beaucoup d'autres mesures peuvent être mises en place; pour un exposé détaillé, on consultera notre déclaration à ce sujet⁷⁹.

Des incidents sont survenus sur de nombreuses applications et plateformes populaires; 2 victimes sur 5 (39 %) ont subi de la violence sexuelle sur Snapchat.

Recommandation : Les régimes de sécurité en ligne doivent s'appliquer à un large éventail de plateformes et prévoir une gradation d'obligations proportionnée aux facteurs de risque anticipés ou connus propres à chaque service.

Beaucoup d'incidents de cyberviolence sexuelle sont survenus sur des services de médias sociaux grand public, mais aussi sur d'autres services en ligne. Les plateformes de jeux, les applications de messagerie privée et les petits services de médias sociaux moins connus sont d'autres espaces où les ados subissent des violences sexuelles (figure 5).

Parallèlement à cette enquête, d'autres études ont montré que les délinquants publient et distribuent souvent du MAEP sur des forums Web et des services d'hébergement de fichiers marginaux^{80,81,82}.

Ces résultats soulignent l'importance d'imposer des obligations de sécurité à tous les services en ligne, en particulier ceux qui permettent les interactions directes entre utilisateurs et la publication de contenus générés par les utilisateurs. À partir de là, d'autres facteurs (niveaux de risque, nature du service, probabilité que des enfants l'utilisent, etc.) peuvent permettre de déterminer les autres obligations réglementaires qu'il y a lieu d'imposer.

Enfin, compte tenu du grand nombre de fois où Snapchat a été citée par les victimes interrogées dans cette enquête, nous jugeons utile de souligner que cette plateforme a récemment fait valoir qu'elle devrait être exemptée de la nouvelle loi australienne – intitulée *Online Safety Amendment (Social Media Minimum Age) Act 2024*⁸³ – qui fixe à 16 ans l'âge minimal pour utiliser certaines plateformes de médias sociaux. Snapchat a soutenu qu'elle est principalement une plateforme de messagerie privée et qu'elle ne devrait donc pas être considérée comme une plateforme de médias sociaux⁸⁴. Cet exemple montre combien il est important de disposer de régimes de sécurité en ligne qui prévoient une gradation d'obligations proportionnée aux risques.

Parmi les victimes qui ont fait un signalement à une application ou à une plateforme pour demander la suppression d'images nues ou sexuelles, 2 sur 3 (67 %) ont attendu plus d'une journée pour que l'image soit supprimée. Les victimes estiment également que les applications et les plateformes devraient empêcher la distribution non consensuelle d'images nues ou sexuelles d'ados.

Recommandation : Les régimes de sécurité en ligne doivent énoncer clairement que les fournisseurs de services en ligne sont tenus de prendre les moyens voulus pour détecter proactivement les images nues ou sexuelles d'enfants qui leur sont signalées, les vérifier et les supprimer rapidement.



Photo des mannequins. Pour illustrer le texte.

La plupart des victimes ont subi au moins une forme de violence sexuelle par l'image, comme la distribution non autorisée d'images nues ou sexuelles. Lorsqu'elles ont pris l'initiative de demander aux plateformes de supprimer leurs images, la plupart ont dû patienter entre un jour et plusieurs mois. Nous ne les avons pas interrogées sur ce qui s'était passé entre-temps, mais d'autres études indiquent que le maintien en ligne de telles images risque d'aggraver le préjudice subi par les victimes^{85,86,87}.

Pour stopper la distribution des images et la cyberviolence sexuelle, un régime canadien de sécurité en ligne devrait obliger les services à supprimer les images nues ou sexuelles d'enfants dans un délai de 24 heures après avoir été informés de leur présence sur leurs serveurs, comme le proposait le projet de loi C-63, *Loi sur les préjudices en ligne*⁸⁸. Un régime de sécurité en ligne devrait aussi, à l'instar de l'Australie⁸⁹, prévoir des mesures d'exécution à défaut pour un service d'obtempérer dans les 24 heures.

Les victimes ont également souligné l'importance d'empêcher la distribution d'images nues ou sexuelles. Presque toutes pensent qu'il serait utile que les applications et les plateformes soient conçues pour empêcher que des images nues ou sexuelles d'ados soient partagées sans leur autorisation. Un régime canadien de sécurité en ligne devrait exiger que les services en ligne adoptent des outils de détection proactive (par exemple, des technologies de correspondance par hachage cryptographique et perceptuel) capables de bloquer le transfert et la redistribution de MAEP connu. Beaucoup de services en ligne utilisent ces technologies⁹⁰, mais il reste à en généraliser l'utilisation et à encadrer celle-ci par des normes.



Au moins 1 victime sur 4 (25 %) a vécu une expérience de cyberviolence sexuelle aux mains d'un adulte.

Recommandation : Les régimes de sécurité en ligne doivent obliger les fournisseurs de services en ligne à prévenir les interactions en ligne potentiellement dangereuses entre adultes et enfants. Il y aurait lieu également d'envisager une modification au *Code criminel* du Canada pour inclure les tactiques de leurre.

En l'absence d'un régime de sécurité en ligne au Canada, de nombreuses applications et plateformes ne font rien pour empêcher un adulte d'envoyer des messages à un enfant, d'échanger des images avec lui et de l'appeler par vidéo. Dans ces environnements non surveillés, les interactions inappropriées entre enfants et adultes sont monnaie courante. Ces mêmes adultes peuvent aussi se faire passer pour des enfants.

Ils peuvent s'en prendre à des enfants et ne s'en privent pas. D'ailleurs, 1 victime sur 4 (25 %) a dit savoir que l'auteur de l'incident était un adulte. D'autres n'en étaient pas certaines, mais il est possible qu'elles aient été la cible d'un adulte qui se faisait passer pour un enfant ou un adolescent. La violence par les pairs, moins répandue, est aussi un phénomène inquiétant sur lequel nous reviendrons dans nos autres recommandations, mais c'est surtout la violence par les adultes qui nous intéresse ici, car sa prévention requiert une approche particulière.

Un régime de sécurité en ligne devrait obliger les services en ligne à se doter de mécanismes adéquats de vérification de l'âge. Afin de prévenir les interactions inappropriées entre utilisateurs adultes et enfants, les services en ligne pourraient, par exemple, être tenus d'utiliser des technologies efficaces de confirmation de l'âge ou de vérifier l'identité des nouveaux utilisateurs au moment de leur intégration.

L'imposition de la confirmation de l'âge, voire de la vérification des utilisateurs, pourrait aussi prévenir la création de fausses identités et de faux comptes⁹¹, une tactique couramment utilisée pour entrer en contact avec des enfants sur Internet et s'en prendre à eux⁹². D'ailleurs, la quasi-totalité des victimes estiment que la mise en place de mesures pour empêcher la création de faux comptes contribuerait à prévenir la cyberviolence sexuelle.

Pour compléter ces exigences, le Parlement pourrait aussi envisager de modifier l'infraction de leurre dans le *Code criminel*. Cela pourrait se faire, par exemple, par l'insertion d'une liste non exhaustive de facteurs à considérer par les juges dans leur analyse du motif de la communication, un peu comme au paragraphe 153(1.2) du *Code criminel*. L'un de ces facteurs pourrait être que l'accusé a faussement déclaré son âge, en particulier s'il s'est présenté comme une personne âgée de moins de 18 ans.

On pourrait aussi envisager la création d'une nouvelle infraction pour la fausse déclaration de l'âge à des fins malveillantes. Par exemple, la loi australienne prévoit une infraction pouvant inclure des situations où « une personne déclare faussement son âge sur Internet dans le but de causer du tort à une autre personne âgée de moins de 16 ans⁹³ » [traduction libre].

Enfin, la vérification de l'âge des utilisateurs permet aussi de soutenir, voire de réaliser plusieurs autres objectifs fondamentaux en matière de sécurité en ligne. Par exemple, certains régimes de sécurité en ligne imposent aux fournisseurs de services en ligne des obligations de diligence spécifiques aux enfants^{94,95,96}. Or, en l'absence d'une obligation corollaire d'établir l'âge de leurs utilisateurs, on voit mal comment ces services pourraient s'acquitter de ces obligations.

Plus de 1 victime sur 2 (52 %) a reçu une image nue ou sexuelle non désirée, et 1 victime sur 6 (17 %) a été mise en scène dans une image truquée (nue ou sexuelle).

Recommandation : Modifier le *Code criminel* pour ériger en infraction la création et le partage d'images hypertruquées (nues ou sexuelles) et voir si les infractions existantes couvrent adéquatement le cyberexhibitionnisme.

Dans l'état actuel des choses, certaines des formes de violence définies dans cette enquête franchissent le seuil de la légalité au Canada, mais pas toutes.

La création et la distribution d'images nues hypertruquées est une forme de cyberviolence sexuelle qui n'est pas expressément abordée dans le droit canadien. De nombreuses victimes rapportent avoir été mises en scène dans une image « truquée » (nue ou sexuelle). Nous ne leur avons pas demandé d'où venaient ces images, mais il est probable qu'au moins une partie d'entre elles aient été créées à l'aide d'applications et de plateformes de « nudification » ou de « déshabillage » qui utilisent l'IA et qui sont faciles à trouver⁹⁷. Si la définition du MAEP dans le *Code criminel* est suffisamment large pour englober les images créées à l'aide d'outils IA, on ne peut en dire autant de la définition de l'infraction de distribution non consensuelle d'images intimes. La législation canadienne pourrait interdire la publicité et la disponibilité de tels outils, criminaliser ces images et fixer des délais pour en accélérer la suppression. Des mesures par rapport aux images nues générées par l'IA ont été adoptées aux États-Unis⁹⁸ et ont été récemment annoncées par le gouvernement australien⁹⁹.

Une autre forme de cyberviolence sexuelle à laquelle il faudrait s'attarder est le cyberexhibitionnisme, qui a touché plus de la moitié des victimes interrogées dans cette enquête. Certains de ces incidents pourraient être considérés comme criminels, mais, selon les circonstances, il n'est pas toujours évident de savoir s'il y a correspondance avec des infractions au *Code criminel*, et, si oui, avec quelles infractions. Le Royaume-Uni¹⁰⁰, par exemple, a criminalisé l'envoi intentionnel d'images d'organes génitaux non sollicitées dans le but de causer de la détresse à la personne destinataire ou d'en tirer une gratification sexuelle sans considération pour la détresse que ces images pourraient causer à cette dernière. Une telle loi pourrait également s'appliquer aux images réelles ou générées par l'IA, aux images des organes génitaux de l'expéditeur ou d'une autre personne, et aux incidents touchant des victimes de tous âges.



Photo d'un mannequin. Pour illustrer le texte.

Plus de 9 victimes sur 10 (93 %) estiment que le Canada devrait prendre des mesures législatives pour obliger les applications et les plateformes à prévenir la cyberviolence. La plupart d'entre elles croient aussi en l'utilité de mesures de sécurité.

Recommandation : Un régime de sécurité en ligne doit exiger que les applications et les plateformes soient conçues dans une optique de sécurité et que les enfants y bénéficient de protections renforcées.

Du fait de leur vécu, les ados victimes de cyberviolence sexuelle sont bien placés pour se prononcer sur les mesures à prendre pour protéger les enfants sur Internet. Ils se montrent très favorables à des lois obligeant les applications et les plateformes à prévenir la cyberviolence sexuelle ainsi qu'à plusieurs mesures de sécurité dès la conception, qui consistent, pour les applications et les

plateformes, à anticiper les dérives et à apporter les modifications voulues de manière à réduire au minimum les risques d'utilisation de leurs services à des fins malveillantes. Il peut s'agir, par exemple, de modifications au niveau de l'interface et des fonctionnalités, de mises en garde et d'options de configuration. Outre les mesures évoquées plus haut, environ 9 victimes sur 10 (92 %) pensent qu'il serait utile, dans une logique de prévention de la cyberviolence sexuelle, d'empêcher que des ados puissent être recontactés par une personne qu'ils ont bloquée ou signalée, ou d'empêcher des inconnus d'entrer en contact avec des ados ou de leur envoyer des messages (85 %).

Environ 9 victimes sur 10 estiment aussi que la mise à disposition d'outils bien conçus pour signaler les problèmes et les abus contribuerait à réduire la cyberviolence sexuelle contre les ados. Par exemple, des moyens faciles pour signaler les problèmes (92 %) et un suivi rapide par une vraie personne (87 %).

Ailleurs dans le monde, les lois sur la sécurité en ligne imposent déjà plusieurs mesures de ce genre. Par exemple, en Australie et au Royaume-Uni, les services en ligne sont tenus d'offrir des mécanismes de signalement réactifs et faciles à utiliser^{101,102}. Le Royaume-Uni a également adopté en 2020 le *UK Children's Code* (officiellement connu sous le nom d'*Age Appropriate Design Code*)¹⁰³, qui exige la prise en compte de l'intérêt supérieur des enfants dans la conception des services en ligne. Ce code se décline en 15 normes qui imposent l'intégration de protections pour les enfants à même ces services (par exemple, des paramètres de confidentialité resserrés par défaut, une collecte de données minimale, des contrôles parentaux transparents et l'interdiction de techniques d'incitation inappropriées).

Enfin, les victimes ont été appelées à se prononcer également sur l'utilité de la surveillance parentale comme moyen de protéger les ados contre la cyberviolence sexuelle. Cette mesure a été jugée utile par 3 victimes sur 4 (74 %), ce qui en fait la mesure la moins bien vue, bien qu'elle soit jugée utile par la plupart des victimes. En conséquence, la surveillance parentale et, plus généralement, les contrôles parentaux devraient être considérés comme faisant partie des nombreuses mesures que les services en ligne devraient mettre en place pour réduire les risques de cyberviolence sexuelle contre les enfants. Ces outils ne sauraient à eux seuls être jugés suffisants, quand on sait que les contrôles parentaux sont activés sur moins de 1 % des comptes d'enfants sur Discord et Snapchat¹⁰⁴. Cela pourrait indiquer que le paramétrage de ces outils s'avère trop complexe ou que les parents eux-mêmes ne croient pas en l'efficacité des contrôles mis à leur disposition.



Photo d'un jeune homme. Pour illustrer le texte.

CONCLUSION

La cyberviolence sexuelle contre les ados est très répandue au Canada et elle survient principalement dans le contexte de communications privées sur des plateformes grand public utilisées par des millions de Canadiennes et de Canadiens. Les expériences partagées par près de 1300 victimes révèlent des défaillances systémiques : les plateformes, souvent, ne font rien pour prévenir les cyberviolences sexuelles, et, en cas d'incident, leurs réponses sont lentes et inadéquates. Ces violences ne sont pas inévitables; elles reflètent des choix de conception et des vides réglementaires. Les ados victimes de cyberviolence sexuelle sont largement en faveur de lois fortes et de mesures de sécurité dès la conception pour protéger les enfants sur Internet, signalant que l'action volontaire des entreprises de technologie ne suffit pas.

Un régime détaillé de sécurité en ligne pour le Canada doit imposer des obligations exécutoires de diligence, exiger la suppression rapide des contenus abusifs et préjudiciables, et prévenir les interactions dangereuses entre adultes et enfants. Il devrait aussi interdire les menaces émergentes, comme les images nues hypertruquées générées par l'IA. La protection des enfants sur Internet ne relève pas seulement du respect de leur droit à la sécurité; elle reconnaît aussi leur droit à la vie privée et à la protection contre l'exploitation. Le Canada peut tirer des leçons des expériences des victimes et s'inspirer des expériences d'autres pays qui se sont dotés de régimes de sécurité en ligne pour faire encore mieux.



Photo d'un mannequin. Pour illustrer l'article.

ANNEXE A : MÉTHODOLOGIE DE L'ENQUÊTE

En mars 2025, le CCPE a créé un questionnaire et a retenu les services de la firme Léger pour mener l'enquête en ligne auprès d'un échantillon national représentatif de jeunes de 13 à 17 ans vivant au Canada et ayant subi au moins une forme de cyberviolence sexuelle. Leurs parents devaient autoriser leur enfant à participer. Le questionnaire de l'enquête était disponible en français et en anglais.

Léger a envoyé des invitations à participer aux parents qui font partie de son panel de recherche (LEO). Les parents et leurs enfants ont donné leur consentement éclairé, après quoi l'enfant a été appelé à répondre à sept questions de sélection pour déterminer s'il avait déjà subi une quelconque forme de cyberviolence sexuelle. Les enfants qui n'avaient jamais subi au moins une des formes définies dans l'enquête ont été exclus.

Les questions de sélection appelaient les jeunes à s'en tenir à des expériences qui s'étaient produites sans leur autorisation ou d'une manière qu'ils ne souhaitaient pas. Nous avons choisi cette orientation parce que nous voulions interroger les ados sur des violences pouvant être perpétrées par des adultes ou des enfants, ainsi que sur des expériences non désirées susceptibles d'inciter les victimes à entreprendre des démarches en conséquence. Nos données ne reflètent donc pas toutes les formes d'exploitation et d'abus sexuels pouvant survenir sur Internet. Elles excluent, par exemple, les expériences auxquelles des ados auraient consenti alors qu'ils n'étaient pas légalement aptes à le faire aux termes de la loi canadienne.

L'échantillon final était composé de 1279 jeunes de 13 à 17 ans qui ont subi au moins une des formes de cyberviolence sexuelle définies dans l'enquête. La collecte des données a été réalisée durant la période du 29 avril au 20 mai 2025. Une marge d'erreur ne peut pas être associée à un échantillon non probabiliste comme celui-ci. À des fins de comparaison, un échantillon probabiliste de 1279 répondants aurait une marge d'erreur maximale de $\pm 2,7\%$, et ce, 19 fois sur 20. Les données ont été pondérées en fonction des données du recensement canadien de 2021. Toutes les analyses de données ont été réalisées par Léger.

ANNEXE B :

QUESTIONS DE SÉLECTION

Dans cette section, nous te poserons des questions sur des choses qui te sont peut-être arrivées quand tu étais en ligne. Par « en ligne », nous entendons tout ce qui se passe lorsque tu accèdes à Internet à partir d'un ordinateur, un téléphone, une tablette ou un appareil de jeu.

Pour rappel :

- Tes réponses sont totalement anonymes. Personne ne saura comment tu as répondu - ni tes parents, ni les personnes chargées de l'enquête, ni personne d'autre.
- Il n'y a pas de bonnes ou de mauvaises réponses. Les seules « bonnes » réponses sont celles qui sont vraies pour toi.

Tu peux sauter n'importe quelle question ou arrêter de répondre à l'enquête à tout moment.

ScreenQ1. Quelqu'un t'a-t-il déjà fait ce qui suit en ligne, sans que tu sois d'accord? Rappel : Par « en ligne », nous entendons tout ce qui se passe lorsque tu accèdes à Internet à partir d'un ordinateur, un téléphone, une tablette ou un appareil de jeu.

- Essayer de te faire parler de sexe ou te dire des choses à caractère sexuel? Par exemple, te faire des commentaires sexuels sur ton corps.
- T'envoyer une photo ou vidéo à caractère sexuel ou de nudité? Par exemple, une photo d'organes génitaux ou une vidéo de personnes ayant des rapports sexuels.

ScreenQ2. Les prochaines questions portent sur « les images de nudité ou à caractère sexuel ». Nous entendons par là des photos ou des vidéos de toi nu-e, partiellement nu-e, ou qui sont de nature sexuelle ou sexuellement abusive. [Note aux programmeurs : Cette définition devrait apparaître par effet de survol sur toutes les occurrences du terme « images de nudité ou à caractère sexuel » dans l'enquête.]

Quelqu'un t'a-t-il déjà fait ce qui suit en ligne, sans que tu sois d'accord?

- Prendre une vraie image nue ou à caractère sexuel de toi en enregistrant une vidéo en direct ou en faisant une capture d'écran?
- Créer une image truquée de toi nu-e ou à caractère sexuel en éditant ou en modifiant une image de toi?

ScreenQ3. Encore une fois, pense à des « images de nudité ou à caractère sexuel » (des photos ou des vidéos de toi nu-e, partiellement nu-e, ou qui sont de nature sexuelle ou sexuellement abusive). Quelqu'un t'a-t-il déjà fait ce qui suit en ligne?

- Faire pression sur toi pour que tu lui envoies des images de toi nu-e ou à caractère sexuel (vraies ou truquées)?
- Menacer de publier, d'envoyer ou de montrer à d'autres des images de toi nu-e ou à caractère sexuel (vraies ou truquées)?
- Publier, envoyer ou montrer à d'autres une image de toi nu-e ou à caractère sexuel (vraie ou truquée), sans ton autorisation?

RÉFÉRENCES

- ¹ Savage, L. (2024). L'exploitation sexuelle des enfants en ligne : un profil statistique des affaires déclarées par la police au Canada, 2014 à 2022 », *Statistique Canada*. <https://www150.statcan.gc.ca/n1/pub/85-002-x/2024001/article/00003-fra.htm>
- ² Gendarmerie royale du Canada. (2025). *Le projet STEEL mène à l'arrestation de 106 auteurs de délits sexuels en ligne sur des enfants*. <https://grc.ca/fr/nouvelles/2025/03/projet-steel-mene-larrestation-106-auteurs-delits-sexuels-en-ligne-sur-enfants>
- ³ Pedersen, K. et Wesley, A. (2023, 2 novembre). Social media apps that facilitate sextortion blamed for not doing enough to prevent it. *CBC News*. <https://www.cbc.ca/news/canada/sextortion-social-media-apps-victims-1.7014262>
- ⁴ Presse canadienne (2024, 3 février). AI brings deepfake pornography to the masses, as Canadian laws play catch-up. *CTV News*. <https://www.ctvnews.ca/vancouver/article/ai-brings-deepfake-pornography-to-the-masses-as-canadian-laws-play-catch-up/>
- ⁵ Nau, C., Reyes, E., Dietzel, C., Dodge, A., Dunn, S. et Mendes, K. (2025). « Canadian youth and technology-facilitated sexual violence: Findings from a 2024 general population survey among Canadian teens », *DIY: Digital Safety*. <https://doi.org/10.5683/SP3/HBJOCW>
- ⁶ Chauviré-Geib, K., Gerke, J., Haag, A. C., Sachser, C., Finkelhor, D., Rassenhofer, M., et Fegert, J. M. (2025). « The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. Population-based surveys fail to capture the full picture », *Child Abuse & Neglect*, vol. 164, 107452.
- ⁷ Walsh, K., Mathews, B., Parvin, K., Smith, R., Burton, M., Nicholas, M., Napier, S., Cubitt, T., Erskine, H., Thomas, H. J., Finkelhor, D., Higgins, D. J., Scott, J. G., Flynn, A., Noll, J., Malacova, E., Le, H. et Tran, N. (2025). « Prevalence and characteristics of online child sexual victimization: Findings from the Australian Child Maltreatment Study », *Child Abuse & Neglect*, vol. 160, 107186. <https://doi.org/10.1016/j.chiabu.2024.107186>
- ⁸ Gouvernement du Canada (2023). L'exploitation sexuelle des enfants sur Internet. *Sécurité publique Canada*. <https://www.securitepublique.gc.ca/cnt/cntrng-crm/chld-sxl-xpltt-ntrnt/index-fr.aspx>
- ⁹ International Centre for Missing & Exploited Children (2025). *Global experts call for new approach to protect children from 'pandemic' of sexual exploitation and abuse*. <https://www.icmec.org/press/global-experts-call-for-new-approach-to-protect-children-from-pandemic-of-sexual-exploitation-and-abuse/>
- ¹⁰ Fry, D. et Lambourne, Z. (2025). Public health and child sexual exploitation and abuse. *Childlight*. <https://www.childlight.org/uploads/publications/Public-health-paper-survey-June-2025.pdf>
- ¹¹ Organisation mondiale de la santé (2022). *What works to prevent online violence against children?* <https://iris.who.int/server/api/core/bitstreams/0ce56bbf-4535-405e-9bd6-e143f64ae2ba/content>
- ¹² Gewirtz-Meydan, A., Walsh, W., Wolak, J. et Finkelhor, D. (2018). « The complex experience of child pornography survivors », *Child Abuse & Neglect*, vol. 80, p. 238-248.
- ¹³ Schmidt, F., Varese, F. et Bucci, S. (2023). « Understanding the prolonged impact of online sexual abuse occurring in childhood », *Frontiers in Psychology*, vol. 14, 1281996. <https://doi.org/10.3389/fpsyg.2020.606218>
- ¹⁴ Colburn, D., Mitchell, K. J., Gewirtz-Meydan, A., Finkelhor, D., Turner, H. A. et O'Brien, J. E. (2025). « Life impact following childhood Image-Based Sexual Abuse victimization among a sample of young adults », *Child Abuse & Neglect*, vol. 167, 107584. <https://doi.org/10.1016/j.chiabu.2025.107584>
- ¹⁵ Mitchell, K. J., Colburn, D., Finkelhor, D., Gewirtz-Meydan, A., Turner, H. A. et Jones, L. M. (2025). « Links between image-based sexual abuse and mental health in childhood among young adult social media users », *Child Abuse & Neglect*, vol. 164, 107471. <https://doi.org/10.1016/j.chiabu.2025.107471>
- ¹⁶ Hanson, E. (2016). The Impact of Online Sexual Abuse on Children and Young People. Dans J. Brown (Éd.), *Online risk to children: Impact, protection and prevention* (1^{re} éd., p. 97-122). Wiley Blackwell. <https://doi.org/10.1002/9781118977545.CH6>

- ¹⁷ Gewirtz-Meydan, A., Walsh, W., Wolak, J. et Finkelhor, D. (2018). « The complex experience of child pornography survivors », *Child Abuse & Neglect*, vol. 80, p. 238-248.
- ¹⁸ Centre canadien de protection de l'enfance (2024). *Enquête auprès des survivantes et survivants : Rapport intégral 2017* (en anglais). https://ProtegeonsNosEnfants.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf
- ¹⁹ Finkelhor, D., Turner, H., Colburn, D. et Mitchell, K. J. (2025). « Persisting concerns about image exposure among survivors of image-based sexual exploitation and abuse in childhood », *Psychological Trauma: Theory, Research, Practice and Policy*, vol. 17 (suppl. 1), p. S88-S93. <https://doi.org/10.1037/tra0001815>
- ²⁰ Centre canadien de protection de l'enfance (2024). *Le vécu des survivant·es d'abus pédosexuels avec prise d'images : Comment l'inaction des entreprises de technologie conduit à la peur, à la traque et au harcèlement*. https://ProtegeonsNosEnfants.ca/pdfs/C3P_ExperiencesOfCSAMSurvivors_fr.pdf
- ²¹ Ringrose, J., Regehr, K. et Milne, B. (2021). *Understanding and combatting youth experiences of image-based sexual harassment and abuse*. <https://www.ascl.org.uk/ASCL/media/ASCL/Our%20view/Campaigns/Understanding-and-combatting-youth-experiences-of-image-based-sexual-harassment-and-abuse-full-report.pdf>
- ²² Haut-Commissariat aux droits de l'homme (2021). *Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique*. Nations unies. <https://www.ohchr.org/fr/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>
- ²³ Online Safety Act, 2021, no. 76. <https://www.legislation.gov.au/C2021A00076/latest/text>
- ²⁴ Online Safety Act 2023, c. 50. <https://www.legislation.gov.uk/ukpga/2023/50/enacted>
- ²⁵ Règlement 2022/2065. Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques). <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R2065>
- ²⁶ Projet de loi C-63, *Loi édictant la Loi sur les préjudices en ligne, modifiant le Code criminel, la Loi canadienne sur les droits de la personne et la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet et apportant des modifications corrélatives et connexes à d'autres lois*, 1^{re} session, 44^e législature. 2024. <https://www.parl.ca/documentviewer/fr/44-1/projet-loi/C-63/premiere-lecture>
- ²⁷ Centre canadien de protection de l'enfance (2024). *L'exclusion des fonctions de messages privés du projet de loi sur les préjudices en ligne laisse planer une grave menace pour les enfants*. <https://www.ProtegeonsNosEnfants.ca/fr/zone-medias/blogue/2024/loi-sur-les-prejudices-en-ligne-messages>
- ²⁸ Centre canadien de protection de l'enfance (2024). *L'obligation de confirmation de l'âge est nécessaire afin que les services réglementés puissent remplir leurs obligations à l'égard des enfants au titre du projet de loi sur les préjudices en ligne*. <https://www.ProtegeonsNosEnfants.ca/fr/zone-medias/blogue/2024/verification-des-factures-en-ligne>
- ²⁹ Parti libéral du Canada (2025). *Sécuriser*. <https://liberal.ca/fr/plateforme/securiser/>
- ³⁰ Parti conservateur du Canada (2025). *Le changement : Pour une vie abordable. Pour des rues sécuritaires. Pour le Canada d'abord*. https://canada-first-for-a-change.s3.us-west-2.amazonaws.com/20250418_CPCPlatform_8-5x11_FR-pages.pdf
- ³¹ Nouveau Parti démocratique (2025). *Du cœur au ventre pour vous*. <https://www.npd.ca/engagements>
- ³² Bloc Québécois (2025). *Choisir le Québec : Plateforme politique 2025*. <https://www.blocquebecois.org/wp-content/uploads/2025/03/blocqcplateforme-2025web.pdf>
- ³³ Turner, H. A., Finkelhor, D. et Colburn, D. (2023). « Predictors of online child sexual abuse in a U.S. national sample », *Journal of Interpersonal Violence*, vol. 38, n° 11-12, p. 7780-7803. <https://doi.org/10.1177/08862605221149090>
- ³⁴ Turner, H. A., Finkelhor, D., Mitchell, K. et Colburn, D. (2024). « Prevalence of technology-facilitated abuse among sexual and gender minority youths », *JAMA Network Open*, vol. 7, n° 2, e2354485. <https://doi.org/10.1001/jamanetworkopen.2022.34471>
- ³⁵ Centre canadien de protection de l'enfance (2025). *Dangers d'Internet : IA et hypertrucages*. <https://cyberaide.ca/fr/dangers-internet/ia-et-hypertrucages/>

- ³⁶ Thorn (2025). *Deepfake nudes & young people: Navigating a new frontier in technology-facilitated nonconsensual sexual abuse and exploitation*. https://info.thorn.org/hubfs/Research/Thorn_DeepfakeNudes&YoungPeople_Mar2025.pdf
- ³⁷ *Online Safety Act 2021*, section 187. <https://www.legislation.gov.uk/ukpga/2023/50>
- ³⁸ Thorn (2025). *Sexual extortion & young people: Navigating threats in digital environments*. https://info.thorn.org/hubfs/Research/Thorn_SexualExtortionandYoungPeople_June2025.pdf
- ³⁹ Centre canadien de protection de l'enfance (2025). *Dangers d'Internet : La sextorsion*. <https://cyberaide.ca/fr/dangers-internet/sextorsion/>
- ⁴⁰ Thorn (2017). *Sextorsion : Summary findings from a 2017 survey of 2,097 survivors*. https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf
- ⁴¹ Thorn (2017). *Sextorsion : Summary findings from a 2017 survey of 2,097 survivors*. https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf
- ⁴² Finkelhor, D., Turner, H. et Colburn, D. (2022). « Prevalence of online sexual offenses against children in the US », *JAMA Network Open*, vol. 5, n° 10, e2234471. <https://doi.org/10.1001/jamanetworkopen.2022.34471>
- ⁴³ City of Calgary (2022). *Police issue warning of online extortion scam targeting young boys*. <https://newsroom.calgary.ca/police-issue-warning-of-online-extortion-scam-targeting-young-boys/>
- ⁴⁴ Gibson, C. (2022, 17 mai). Red Deer RCMP issue warning about increase in sextortion reports. *Global News*. <https://globalnews.ca/news/8841770/red-deer-rcmp-sextortion-warning/>
- ⁴⁵ Presse canadienne (2022, 9 juin). Ontario police warn public of online sextortion scams circulating. *CTV News*. <https://www.ctvnews.ca/toronto/article/ontario-police-warn-public-of-online-sextortion-scams-circulating/>
- ⁴⁶ Derksen, D. et Klippenstein, T. (2022, 6 juin). Pembina Valley RCMP raise awareness of sextortion scams. *Pembina Valley Online*. <https://www.pembinavalleyonline.com/articles/pembina-valley-rcmp-raise-awareness-of-sextortion-scams>
- ⁴⁷ Centre canadien de protection de l'enfance (2022). *Sextorsion : Les garçons sont la cible de tactiques agressives sur Instagram et Snapchat, selon une analyse de Cyberaide.ca*. <https://cyberaide.ca/fr/campagnes-et-medias/communiqués/2022/analyse-donnees-sextorsion/>
- ⁴⁸ Siemaszko, C. (2022, 8 mai). 'Sextortionists' are increasingly targeting young men for money. The outcome can be deadly. *NBC News*. <https://www.nbcnews.com/tech/tech-news/sextortionists-are-increasingly-targeting-young-men-money-outcome-can-rcna27281>
- ⁴⁹ Centre canadien de protection de l'enfance (2022). *Analyse des publications de victimes de sextorsion financière sur r/Sextortion*. https://ProtegeonsNosEnfants.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_fr.pdf
- ⁵⁰ Raffile, P., Goldenberg, A., McCann, C. et Finkelstein, J. (2024). A digital pandemic: Uncovering the role of 'Yahoo Boys' in the surge of social media-Enabled financial sextortion targeting minors. *Network Contagion Research Institute*. https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf
- ⁵¹ Thorn (2024). *Trends in financial sextortion: An investigation of sextortion reports in NCMEC CyberTipline data*. https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf
- ⁵² CBC (2013, 15 septembre). *The sextortion of Amanda Todd*. <https://www.cbc.ca/player/play/video/1.2429059>
- ⁵³ McMillan, D., Pederson, K. et Tomlinson, A. (2025, 3 octobre). Sextorters are targeting young boys online – and flaunting how rich the scam is making them. *CBC*. <https://www.cbc.ca/news/marketplace/sextortion-teen-boys-canada-1.7648267>
- ⁵⁴ Savage, L. (2024). L'exploitation sexuelle des enfants en ligne : un profil statistique des affaires déclarées par la police au Canada, 2014 à 2022 », *Statistique Canada*. <https://www150.statcan.gc.ca/n1/pub/85-002-x/2024001/article/00003-fra.htm>
- ⁵⁵ Thorn (2025). *Sexual extortion & young people: Navigating threats in digital environments*. https://info.thorn.org/hubfs/Research/Thorn_SexualExtortionandYoungPeople_June2025.pdf

- ⁵⁶ Centre canadien de protection de l'enfance (2022). *Analyse des publications de victimes de sextorsion financière sur r/Sextortion*. https://ProtegeonsNosEnfants.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_fr.pdf
- ⁵⁷ Centre canadien de protection de l'enfance (2024). *L'exclusion des fonctions de messages privés du projet de loi sur les préjudices en ligne laisse planer une grave menace pour les enfants*. <https://www.ProtegeonsNosEnfants.ca/fr/zone-medias/blogue/2024/loi-sur-les-prejudices-en-ligne-messages>
- ⁵⁸ Savage, L. (2024). L'exploitation sexuelle des enfants en ligne : un profil statistique des affaires déclarées par la police au Canada, 2014 à 2022 », *Statistique Canada*. <https://www150.statcan.gc.ca/n1/pub/85-002-x/2024001/article/00003-fra.htm>
- ⁵⁹ Centre canadien de protection de l'enfance (2020). *Analyse des mécanismes de signalement d'images d'abus pédosexuels sur les plateformes grand public*. <https://ProtegeonsNosEnfants.ca/fr/ressources-et-recherche/signalement-plateformes/>
- ⁶⁰ Bejar, A., Cybersecurity for Democracy, fairplay, Molly Rose Foundation et ParentSOS (2025). *Teen accounts, broken promises: How Instagram is failing to protect minors*. <https://fairplayforkids.org/wp-content/uploads/2025/09/Teen-Accounts-Broken-Promises-How-Instagram-is-failing-to-protect-minors.pdf>
- ⁶¹ Centre canadien de protection de l'enfance (2022). *Analyse des publications de victimes de sextorsion financière sur r/Sextortion*. https://ProtegeonsNosEnfants.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_fr.pdf
- ⁶² UNICEF (2025). *Protecting children in online gaming: Mitigating risks from organized violence*. <https://www.unicef.org/innocenti/media/11836/file/UNICEF-Innocenti-Protecting-Children-Online-Gaming-Working-Paper-2025.pdf>
- ⁶³ eSafety Commissioner (2025). *Child sexual abuse online*. <https://www.esafety.gov.au/key-topics/illegal-restricted-content/child-sexual-abuse-online>
- ⁶⁴ S.146 – 119th Congress (2025-2026): TAKE IT DOWN Act (2025, May 19). <https://www.congress.gov/bill/119th-congress/senate-bill/146/text>
- ⁶⁵ S.1829 – 119th Congress (2025-2026). STOP CSAM Act of 2025 (2025, May 21). <https://www.congress.gov/bill/119th-congress/senate-bill/1829/text>
- ⁶⁶ Projet de loi C-63, *Loi édictant la Loi sur les préjudices en ligne, modifiant le Code criminel, la Loi canadienne sur les droits de la personne et la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet et apportant des modifications corrélatives et connexes à d'autres lois*, 1^{re} session, 44^e législature. 2024. <https://www.parl.ca/documentviewer/fr/44-1/projet-loi/C-63/premiere-lecture>
- ⁶⁷ Safer by Thorn (2024). *Youth tell the truth about safety tools: Advice on how to improve these tools from actual teens*. <https://safer.io/resources/youth-tell-the-truth-about-safety-tools-advice-on-how-to-improve-these-tools-from-actual-teens/>
- ⁶⁸ Friedman-Hauser, G. et Katz, C. (2025). « "She has a history of making things up": Examining the disclosure and reporting of online sexual abuse among children with disabilities », *Child Abuse & Neglect*, vol. 163. <https://doi.org/10.1016/j.chiabu.2025.107398>
- ⁶⁹ Règlement 2022/2065. Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques). <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R2065>
- ⁷⁰ Online Safety Act 2023, c. 50. <https://www.legislation.gov.uk/ukpga/2023/50/enacted>
- ⁷¹ Online Safety Act, 2021, no. 76. <https://www.legislation.gov.au/C2021A00076/latest/text>
- ⁷² Léger (2024). *Online content regulation: Survey of Canadians*. https://leger360.com/wp-content/uploads/2024/04/Leger-x-CP-_-Online_Content_Regulation-1.pdf
- ⁷³ Lockhart, A. (2025). Survey of online harms in Canada 2025. *The Dias*. <https://dais.ca/wp-content/uploads/2025/05/OnlineHarms2025.pdf>
- ⁷⁴ Thorn (2023). *Responding to online threats: Minors' perspectives on disclosing, reporting, and blocking in 2021*. https://info.thorn.org/hubfs/Research/Thorn_ROT_Monitoring_2021.pdf
- ⁷⁵ Revealing Reality (2025). *A digital playground: The real guide to Roblox*. <https://think.revealingreality.co.uk/roblox-real-guide>

- ⁷⁶ Bejar, A., Cybersecurity for Democracy, fairplay, Molly Rose Foundation et ParentSOS (2025). *Teen accounts, broken promises: How Instagram is failing to protect minors*. <https://fairplayforkids.org/wp-content/uploads/2025/09/Teen-Accounts-Broken-Promises-How-Instagram-is-failing-to-protect-minors.pdf>
- ⁷⁷ Centre canadien de protection de l'enfance (2025). *Bilan en matière de cyberviolence : Chronologie de l'incapacité des entreprises de technologie à protéger leurs utilisateurs*. <https://ProtegeonsNosEnfants.ca/fr/zone-medias/chronologie-de-la-technologie/>
- ⁷⁸ Centre canadien de protection de l'enfance (2024). *L'exclusion des fonctions de messages privés du projet de loi sur les préjudices en ligne laisse planer une grave menace pour les enfants*. <https://www.ProtegeonsNosEnfants.ca/fr/zone-medias/blogue/2024/loi-sur-les-prejudices-en-ligne-messages>
- ⁷⁹ Centre canadien de protection de l'enfance (2024). *L'exclusion des fonctions de messages privés du projet de loi sur les préjudices en ligne laisse planer une grave menace pour les enfants*. <https://www.ProtegeonsNosEnfants.ca/fr/zone-medias/blogue/2024/loi-sur-les-prejudices-en-ligne-messages>
- ⁸⁰ Centre canadien de protection de l'enfance (2021). *Projet Arachnid : L'accessibilité des images d'abus pédosexuels sur Internet*. https://protegeonsnosenfants.ca/pdfs/CCPE_ProjectArachnidReport_fr.pdf
- ⁸¹ Barker, K., Neufeld, K. H. S., Marcoux, J. et Podprugin, O. (2025). Uncovering and overcoming offender tactics for distributing child sexual abuse and exploitation material on file hosting services [Manuscrit en préparation]. Centre canadien de protection de l'enfance
- ⁸² Salter, M. et Richardson, L. (2021). « The Trichan takedown: Lessons in the governance and regulation of child sexual abuse material », *Policy & Internet*, vol. 13, n° 3, p. 385-399. <https://doi.org/10.1002/poi3.256>
- ⁸³ Parliament of Australia (2024). Online Safety Amendment (Social Media Minimum Age) LOI 2024. <https://www.legislation.gov.au/C2024A00127/asmade/text>
- ⁸⁴ Rintoul, C. (2025, 28 octobre). Social media ban: Snapchat argues its platform is not 'toxic' and should be exempt from under-16s ban. *The Nightly*. <https://thenightly.com.au/politics/social-media-ban-snapchat-argues-its-platform-is-not-toxic-and-should-be-exempt-from-under-16s-ban-c-20495005>
- ⁸⁵ Centre canadien de protection de l'enfance (2024). *Le vécu des survivant-es d'abus pédosexuels avec prise d'images : Comment l'inaction des entreprises de technologie conduit à la peur, à la traque et au harcèlement*. https://content.c3p.ca/pdfs/C3P_ExperiencesOfCSAMSurvivors_fr.pdf
- ⁸⁶ McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A. et Powell, A. (2020). « 'It's torture for the soul': The harms of image-based sexual abuse », *Social & Legal Studies*, vol. 30, n° 4, p. 541-562. <https://doi.org/10.1177/0964663920947791>
- ⁸⁷ Hellevik, P. M., Haugen, L. E. A. et Överlien, C. (2025). « Outcomes of image-based sexual abuse among young people: A systematic review », *Frontiers in Psychology*, n° 16, 1599087. <https://doi.org/10.3389/FPSYG.2025.1599087/BIBTEX>
- ⁸⁸ Projet de loi C-63, *Loi édictant la Loi sur les préjudices en ligne, modifiant le Code criminel, la Loi canadienne sur les droits de la personne et la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet et apportant des modifications corrélatives et connexes à d'autres lois*, 1^{re} session, 44^e législature. 2024. <https://www.parl.ca/documentviewer/fr/44-1/projet-loi/C-63/premiere-lecture>
- ⁸⁹ eSafety Commissioner (2024). *Image-based abuse scheme: Regulatory guidance*. <https://www.esafety.gov.au/sites/default/files/2024-02/Image-Based-Abuse-Scheme-Regulatory-Guidance-Feb2024.pdf>
- ⁹⁰ eSafety Commissioner (2025). *A baseline for online safety transparency: The first regular report on child sexual exploitation and abuse, and sexual extortion*. <https://www.esafety.gov.au/sites/default/files/2025-11/BOSE-full-report-CSEA-sexual-extortion-periodic-notices-Nov2025Update.pdf?v=1762905600021>
- ⁹¹ eSafety Commissioner (2024). *Tech trends issue paper: Age assurance*. https://www.esafety.gov.au/sites/default/files/2024-07/Age-Assurance-Issues-Paper-July2024_0.pdf?v=1721088000021
- ⁹² Centre canadien de protection de l'enfance (2022). *Analyse des publications de victimes de sextorsion financière sur r/Sextortion*. https://ProtegeonsNosEnfants.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_fr.pdf

- ⁹³ Criminal Code Amendment (Protecting Minors Online) Act (No. 50) 2017 (Cth). Explanatory Note. <https://www.ato.gov.au/law/view/document?LocID=%22NEM%2FEM201720%2FNAT%2FATO%2F00001%22&PiT=99991231235958>
- ⁹⁴ Ofcom (2025). *Quick guide to Protection of Children Codes*. <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/quick-guide-to-childrens-safety-codes>
- ⁹⁵ Commission européenne (2025). *La Commission publie des lignes directrices sur la protection des mineurs*. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>
- ⁹⁶ eSafety Commissioner (2025). *Learn about the Online Safety Act*. <https://www.esafety.gov.au/newsroom/whats-on/online-safety-act>
- ⁹⁷ Marr, B. (2025, 28 juillet). AI apps are undressing women without consent and it's a problem. *Forbes*. <https://www.forbes.com/sites/bernardmarr/2025/07/28/ai-apps-are-undressing-women-without-consent-and-its-a-problem/>
- ⁹⁸ TAKE IT DOWN Act, S.146, 119th Cong. (2025). <https://www.congress.gov/bill/119th-congress/senate-bill/146/all-actions>
- ⁹⁹ Department of Infrastructure, Transport, Regional Development, Communication and the Arts (2025). *Taking a stand against abusive technology*. [Communiqué de presse]. <https://minister.infrastructure.gov.au/wells/media-release/taking-stand-against-abusive-technology>
- ¹⁰⁰ *Online Safety Act 2021*, section 187. <https://www.legislation.gov.uk/ukpga/2023/50/section/187>
- ¹⁰¹ eSafety Commissioner (2025). *Register of industry codes and industry standards for online safety*. <https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards#register-of-industry-standards>
- ¹⁰² Ofcom (2025). *Protection of Children Code of Practice for user-to-user services*. <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/protection-of-children-code-of-practice-for-user-to-user-services.pdf?v=403579>
- ¹⁰³ Information Commissioner's Office (s.d.). *Age-appropriate design: A code of practice for online services*. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>
- ¹⁰⁴ Tenbarge, K. (2024, 29 mars). Fewer than 1% of parents use social media tools to monitor their children's accounts, tech companies say. *NBC News*. <https://www.nbcnews.com/tech/social-media/fewer-1-parents-use-social-media-tools-monitor-childrens-accounts-tech-rcna145592>



CENTRE CANADIEN de PROTECTION DE L'ENFANCE^{MC}

Aider les familles. Protéger les enfants.

 protegeonsnosenfants.ca

 [@cdnchildprotect.bsky.social](https://twitter.com/cdnchildprotect)

 [Centre canadien de protection de l'enfance](https://www.facebook.com/Centre.canadien.de.protection.de.l'enfance)

 [@cdnchildprotect](https://www.instagram.com/cdnchildprotect)