



CENTRE CANADIEN *de* PROTECTION DE L'ENFANCE<sup>MC</sup>

*Aider les familles. Protéger les enfants.*

# PROJET ARACHNID : L'ACCESSIBILITÉ DES IMAGES D'ABUS PÉDOSEXUELS SUR INTERNET



Projet  
Arachnid<sup>TM</sup>

*Analyse des images d'abus pédosexuels et des images préjudiciables ou violentes liées à certains fournisseurs de services électroniques*

DOCUMENT DE SYNTHÈSE



**CENTRE CANADIEN de PROTECTION DE L'ENFANCE<sup>inc</sup>**

*Aider les familles. Protéger les enfants.*

**Note au lecteur :**

Ce document se veut une version condensée d'un rapport détaillé intitulé *Projet Arachnid : L'accessibilité des images d'abus pédosexuels sur Internet*

Les résultats détaillés, la méthodologie, les limites et les recommandations sont présentés dans la version intégrale du rapport, à [protegeonsnosenfants.ca/RapportPA](https://protegeonsnosenfants.ca/RapportPA)

Le Centre canadien de protection de l'enfance tient à remercier les organismes de protection de l'enfance de l'extérieur du Canada qui contribuent par leur collaboration à augmenter la capacité de Projet Arachnid à réduire l'accessibilité des images d'abus pédosexuels à l'échelle mondiale.

On peut consulter la liste complète des organismes qui participent à la classification des images dans Projet Arachnid à [ProjetArachnid.ca](https://ProjetArachnid.ca)

© 8 juin 2021, Centre canadien de protection de l'enfance inc. (CCPE). Tous droits réservés. Les données utilisées dans ce rapport sont détenues par le CCPE et toutes les analyses ont été menées par son personnel. Des efforts raisonnables ont été déployés pour assurer l'exactitude de toutes les informations présentées. Les sociétés citées sont désignées soit par le nom utilisé par l'hébergeur du site, soit par le nom figurant dans les conditions générales d'utilisation ou soit par le nom utilisé dans l'URL si aucun autre nom n'a pu être déterminé. « Cyberaide!ca » est une marque du CCPE déposée au Canada. « CENTRE CANADIEN de PROTECTION DE L'ENFANCE » et « Projet Arachnid » sont utilisés comme marques du CCPE. Toutes les autres marques citées appartiennent à leurs détenteurs respectifs, et leur mention ne constitue aucunement une marque d'approbation ou d'affiliation. Les symboles de marque de commerce, s'il y a lieu, ne sont pas employés dans les tableaux de données.

## LE CENTRE CANADIEN DE PROTECTION DE L'ENFANCE

Le Centre canadien de protection de l'enfance inc. (CCPE) est un organisme de bienfaisance voué à la protection de tous les enfants. Le CCPE gère Cyberaide.ca – la centrale canadienne de signalement des cas d'exploitation et d'abus sexuels d'enfants sur Internet – et offre d'autres services d'intervention, de prévention et d'éducation.

En janvier 2017, le CCPE a mis en place Projet Arachnid : une plateforme Web qui détecte les images d'abus pédosexuels connues et qui adresse, dans la mesure du possible, des demandes de suppression aux fournisseurs de services électroniques (FSÉ) qui les hébergent.

Le CCPE soutient aussi les survivant.e.s 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 des enfants.

## POURQUOI NOUS AVONS RÉDIGÉ CE RAPPORT

Le CCPE publie ce rapport dans le but d'illustrer comment les défaillances systémiques de l'industrie de la technologie et l'inaction des gouvernements entravent sérieusement la lutte contre la prolifération des images d'abus pédosexuels sur Internet. Les images d'abus pédosexuels perpétuent un cycle de souffrance pour les enfants du monde entier en les privant de leur sécurité personnelle et de leur droit à la vie privée, tout en leur causant un préjudice important et durable.

Réduire l'accessibilité de ces images doit être un objectif central de tout cadre destiné à protéger les enfants. Pour atteindre cet objectif, il faut bien comprendre comment les sociétés Internet — en particulier celles qui acceptent des contenus générés par leurs utilisateurs — facilitent l'accès aux images d'abus pédosexuels et aux images préjudiciables ou violentes<sup>1</sup> et contribuent à leur prolifération.

Les données primaires sont en grande partie détenues par des FSÉ privés qui sont peu enclins à déclarer proactivement des informations utiles sur la distribution, la modération et la suppression des contenus qu'ils hébergent. Ce manque de transparence empêche de bien saisir l'ampleur de la menace et fait obstacle à la mise en place de mesures législatives et réglementaires ainsi que de recours pour les victimes de ces crimes ou comportements abusifs.

En pareilles circonstances, l'élaboration de politiques ou de règlements fondés sur des données fiables pose un sérieux casse-tête. Le rapport vient remédier en partie à la situation en présentant des données recueillies de façon indépendante par Projet Arachnid sur l'accessibilité des images d'abus pédosexuels et des images préjudiciables ou violentes sur certaines plateformes. Le rapport propose aussi une feuille de route aux gouvernements qui, au nom des enfants, souhaiteraient obliger les FSÉ à rendre des comptes en les soumettant à une réglementation responsable à l'égard des enfants.

<sup>1</sup> Le terme *images préjudiciables ou violentes* englobe toutes les photos et vidéos associées à un abus pédosexuel ainsi que les photos et vidéos de nudité totale ou partielle d'enfants qui ont été rendues publiques et qui sont utilisées dans un contexte sexualisé ou associées à des commentaires à caractère sexuel. Il englobe aussi les photos et les vidéos rendues publiques d'enfants en situation d'abus, de torture ou de contention.

## OBJET DU RAPPORT

Le rapport livre une analyse des données recueillies par Projet Arachnid durant trois années complètes (2018-2020) concernant l'accessibilité des images d'abus pédosexuels et des images préjudiciables ou violentes publiquement accessibles sur le Web visible et le Web clandestin.

Mis au point par le CCPE, Projet Arachnid est un outil centré sur les victimes qui explore le Web<sup>2</sup> à la recherche d'images d'abus pédosexuels. La détection d'images d'abus pédosexuels ou d'images préjudiciables ou violentes déclenche aussitôt l'envoi d'une demande de suppression au FSÉ le plus susceptible de pouvoir remédier immédiatement au maintien en ligne de ces images. Ce processus automatisé s'exécute des milliers de fois par jour.

Ces activités ont permis au CCPE de compiler des données sur plus de 760 FSÉ à travers le monde. Le rapport présente une analyse détaillée de ces données ainsi que des informations sur les indicateurs de transparence suivants :

- **Délai de suppression** : Temps écoulé après l'envoi d'une demande de suppression pour qu'une photo ou une vidéo accessible à une URL donnée devienne inaccessible.
- **Récidive d'images** : Taux auquel les images ayant fait l'objet d'une demande de suppression auprès d'un FSÉ réapparaissent sur les serveurs du même FSÉ et sont de nouveau détectées par Projet Arachnid.

Les données analysées dans le rapport portent sur 5,4 millions d'images détectées dans une sous-section du Web visible. Le champ d'action du Projet Arachnid ne s'étend pas aux réseaux de partage poste à poste, aux plateformes semi-fermées (p. ex. Facebook<sup>MD</sup>, Twitter<sup>MD</sup>) et aux sites par abonnement. Inévitablement, donc, les chiffres présentés sous-estiment grossièrement l'accessibilité de ce type d'images sur Internet.

Le rapport met en relief le rôle central de certains FSÉ méconnus qui, par leur inaction ou leur lenteur à agir, favorisent l'accessibilité des images d'abus pédosexuels et des images préjudiciables ou violentes sur Internet.

## CONSTATS GÉNÉRAUX

Les constats généraux du rapport démontrent que l'on ne peut tout simplement pas s'en remettre aux FSÉ pour investir volontairement les ressources nécessaires pour réduire l'accessibilité des images d'abus pédosexuels.

Les délais inacceptablement longs de suppression des images signalées aux FSÉ et la réapparition d'images précédemment signalées sur les sites Web prouvent que les FSÉ, collectivement, se préoccupent peu de la sécurité et de la protection de la vie privée des enfants sur Internet.

Les résultats de l'analyse sont sans équivoque : les gouvernements doivent légiférer pour imposer des obligations légales aux FSÉ et les responsabiliser davantage, en particulier ceux qui acceptent des contenus générés par les utilisateurs.

Le rapport et ses recommandations apportent aux gouvernements et aux décideurs politiques les informations nécessaires pour prendre des décisions éclairées dans le but de réduire l'accessibilité et la distribution des images d'abus pédosexuels sur Internet.

---

2 Le Web désigne ici les parties du Web visible et du Web clandestin qui sont accessibles au public.

## LES PRINCIPAUX CONSTATS ET LEUR IMPORTANCE

### 1 Constat : Les FSÉ accusent des taux élevés de récurrence d'images

Près de la moitié (48 %) des images pour lesquelles Projet Arachnid a envoyé une demande de suppression avaient déjà été signalées au même FSÉ. Certains FSÉ accusent un taux de récurrence d'images supérieur à 80 %, indicateur que certaines images signalées réapparaissent constamment sur leurs serveurs.



#### POURQUOI C'EST IMPORTANT

Il existe des technologies de détection proactive qui permettent aux FSÉ de bloquer ou de supprimer les images d'abus pédosexuels mises en ligne par leurs utilisateurs. Ce constat montre que de nombreux FSÉ n'utilisent pas ces technologies ou les utilisent mal. Il donne aussi à penser que ces FSÉ n'ajoutent possiblement pas les images signalées à leurs listes de blocage pour empêcher qu'elles soient remises en ligne ultérieurement.

On peut déduire en outre que les hébergeurs n'exigent pas, dans leurs ententes contractuelles avec leurs clients, l'utilisation d'outils de détection proactive de base.



## 2 Constat : Longs délais de suppression pour de nombreuses images

Pour la période étudiée dans le rapport, le délai médian de suppression des images ciblées par Projet Arachnid est de 24 heures. Il est toutefois troublant de constater que 10 % des images signalées — sur lesquelles figurent des milliers de victimes — ont mis sept semaines (42 jours) ou plus avant de devenir inaccessibles.

Il est bon de savoir que les délais de suppression sont calculés à partir du moment où une demande de suppression est adressée à un FSÉ. Dans les faits, les images ciblées pour suppression étaient visibles depuis un certain temps déjà avant que Projet Arachnid ne les détecte. Si Projet Arachnid connaît le délai écoulé entre l'envoi d'une demande de suppression et la suppression de l'image en cause, seul le FSÉ sait depuis combien de temps ladite image était accessible sur Internet.



### POURQUOI C'EST IMPORTANT

Le fait que la moitié des images ciblées ont été supprimées dans les 24 heures suivant l'envoi de la demande de suppression doit être considéré dans le contexte global du problème. Prise isolément, cette statistique est encourageante, car elle montre que Projet Arachnid arrive à obtenir la suppression d'une part importante des images ciblées dans des délais relativement rapides. Or, elle occulte le fond du problème. Certes, de nombreux FSÉ donnent suite aux demandes de suppression dans les 24 heures, mais en l'absence d'obligations réglementaires, ils n'ont aucun intérêt commercial ou juridique à investir dans des mesures qui permettraient d'emblée de prévenir la mise en ligne ou la réapparition des images. Les forts taux de récurrence d'images témoignent crument de cette réalité.

Du point de vue de la réduction des préjudices subis par les victimes, dès qu'une image intime ou une image d'abus pédosexuels se retrouve sur Internet, il faut en accélérer le délai de suppression pour en limiter la distribution ou l'accessibilité. Plus le délai de suppression est long, plus le préjudice subi par la victime est grand.

Ce constat laisse à penser que de nombreux FSÉ ne mobilisent peut-être pas suffisamment de ressources pour gérer le volume de plaintes ou de demandes de suppression venant du public.



### 3 Constat : Les victimes adolescentes sont laissées pour compte

Le rapport constate que les images de victimes à l'état post-pubère, comparativement aux images de victimes prépubères, accusent des délais de suppression beaucoup plus longs (90<sup>e</sup> percentile : 56 jours pour les images d'enfants post-pubères contre 40 jours pour images d'enfants prépubères) et des taux de récurrence plus élevés (73 % pour les images d'enfants post-pubères contre 46 % pour images d'enfants prépubères).

Projet Arachnid détecte aussi beaucoup moins d'images d'enfants post-pubères (n=120 173) que d'images d'enfants prépubères (n=3 403 748) et d'images préjudiciables ou violentes. Cela dit, ce constat n'est probablement pas représentatif du volume réel d'images de victimes adolescentes sur Internet.

#### POURQUOI C'EST IMPORTANT

Les victimes adolescentes sont exposées plus longtemps et répétitivement à la victimisation.

La longueur des délais de suppression pour les images d'enfants plus âgés donne à penser que les FSÉ jugent moins urgent de supprimer les images de victimes adolescentes (images d'enfants post-pubères) que les images visiblement illégales (images d'enfants prépubères).

Cette difficulté de catégoriser des images lorsqu'il s'agit de victimes post-pubères non identifiées de même que la variabilité des normes juridiques en matière d'images d'abus pédosexuels et certaines pratiques policières ont fini par induire un biais de catégorisation en faveur des victimes plus jeunes.

Étant donné que la plupart des technologies de détection d'images (y compris Projet Arachnid) utilisent les empreintes numériques d'images vérifiées pour trouver des images suspectes sur Internet, les images découvertes par ces processus automatisés reflètent ce biais en faveur des images de victimes plus jeunes. Résultat : de nombreuses victimes adolescentes sont laissées pour compte.

En plus des obstacles technologiques qui existent, les analystes du CCPE observent aussi beaucoup de résistance chez certains FSÉ. Il arrive que des FSÉ contestent la validité d'une demande de suppression, estimant que la victime figurant dans l'image n'est pas mineure même si elle est connue du CCPE.



## 4 Constat : Un volume disproportionné d'images d'abus pédosexuels chez un même FSÉ

Près de la moitié (48 %) des images détectées par Projet Arachnid sont liées à un service d'hébergement de fichiers exploité par le géant français des télécommunications Free, propriété du groupe Iliad de Paris. Plus de 18 000 fichiers d'archive contenant collectivement près de 1,1 million d'images assimilables en apparence à des images d'abus pédosexuels ou à des images préjudiciables ou violentes ont été signalés à cet opérateur pendant les trois années de la période étudiée (2018-2020).

Dans de nombreux cas, le robot d'exploration de Projet Arachnid a détecté des liens vers ces fichiers d'archive à plusieurs endroits, autant sur le Web visible que sur le Web clandestin. La multiplicité de ces points d'accès aux fichiers d'archive fait en sorte que l'accessibilité des images d'abus pédosexuels et des images préjudiciables ou violentes sur les serveurs de Free dépasse les 2,7 millions de détections.

À partir de 2018, le CCPE a commencé à communiquer directement avec des employés de Free et à leur fournir des listes de liens directs menant à des fichiers d'archive hébergés sur leurs serveurs et contenant des images d'abus pédosexuels.

Projet Arachnid a continué d'envoyer des demandes de suppression à Free pour chaque nouvelle détection d'images d'abus pédosexuels et d'images préjudiciables ou violentes sur leurs serveurs. Selon les données de Projet Arachnid en date du 18 mai 2021, près de 3 000 fichiers d'archive ayant donné lieu à des demandes de suppression durant les trois années de la période étudiée étaient toujours publiquement accessibles.

### POURQUOI C'EST IMPORTANT

Le service d'hébergement de fichiers de Free est offert gratuitement, ne requiert pas l'ouverture d'un compte et offre un espace de stockage généreux. C'est un service populaire souvent mentionné dans des forums de discussion à caractère pédosexuel, autant sur le Web visible que sur le Web clandestin.

Au lieu de regarder les images sur une page Web pendant qu'elles y sont, les utilisateurs doivent les télécharger, créant du même coup de nouvelles copies des fichiers sur leur ordinateur. Ainsi, même si les images hébergées à la source finissent par être supprimées, des copies peuvent survivre sur des ordinateurs privés et peuvent très bien réapparaître sur Internet à une date ultérieure.

En outre, le volume d'images liées à Free semble indiquer qu'une bonne partie des images d'abus pédosexuels et des images préjudiciables ou violentes est rendue accessible par un nombre relativement peu élevé de FSÉ qui ont la cote auprès des personnes qui se livrent à des activités pédocriminelles. Dès lors, certaines actions stratégiques ciblées auraient le potentiel de réduire considérablement l'accessibilité de ces images sur Internet.

## 5 Constat : Le Web clandestin est la principale voie d'accès aux images d'abus pédosexuels, mais pas le lieu d'hébergement privilégié

La grande majorité des images détectées par Projet Arachnid (97 %) sont physiquement hébergées sur le Web visible. Or, le Web clandestin — et plus particulièrement le réseau Tor, son sous-ensemble le plus fréquenté — semble être le principal moyen utilisé pour diriger les internautes vers des endroits où trouver des images d'abus pédosexuels sur le Web visible.

Les distributeurs de ces images déposeront sur des sites d'hébergement gratuit des fichiers d'archive cryptés et protégés par mot de passe contenant des centaines de photos ou de vidéos. Ils se tourneront ensuite vers des forums du Web clandestin, où ils publieront les liens et les mots de passe permettant de télécharger et d'ouvrir ces fichiers.

Le réseau Tor, accessible seulement au moyen de navigateurs spécialisés, masque l'identité des utilisateurs sur les sites qu'ils consultent. L'anonymisation et le chiffrement du trafic se font toutefois au prix d'un ralentissement non négligeable du temps de chargement des pages et des vitesses de téléchargement. Les services d'archivage et d'hébergement d'images du Web visible s'avèrent dès lors des options plus intéressantes pour mettre en ligne de grandes collections de fichiers multimédias, car ils offrent des vitesses de téléchargement nettement supérieures.

Certains FSÉ — dont quelques-uns sont mis en relief dans le rapport — permettent à des utilisateurs anonymes de publier directement des images sur leurs plateformes à partir du réseau Tor.



### POURQUOI C'EST IMPORTANT

Pour combattre la prolifération des images d'abus pédosexuels, les régulateurs doivent bien comprendre ce principe de vases communicants entre le Web visible et le Web clandestin.

À défaut de mettre en place des mesures de sécurité réseau pour bloquer le trafic suspect ou les internautes qui cherchent à dissimuler leur véritable adresse IP, un FSÉ attirera souvent des internautes qui se serviront de sa plateforme pour mener des activités indésirables.

Ce constat permet néanmoins d'envisager une possibilité. Puisque la majorité des images détectées se trouvent sur le Web visible, il est possible de les lier à un FSÉ, et donc de les cibler pour suppression. Ainsi, l'imposition d'une réglementation gouvernementale à l'ensemble de l'industrie permettrait vraisemblablement de réduire considérablement l'accessibilité des images d'abus pédosexuels sur Internet.

## COUP D'ŒIL SUR L'ANALYSE DES DONNÉES

De 2018 à 2020, Projet Arachnid a détecté à travers ses activités d'exploration plus de 5,4 millions de photos et de vidéos vérifiées comme étant des images d'abus pédosexuels et des images préjudiciables ou violentes (**Figure 1.0**) sur les serveurs de plus de 760 FSÉ dans le monde entier.

Au moment de la rédaction du rapport, le CCPE accuse un arriéré de plus de 32,8 millions d'images suspectes à examiner. En effet, le rythme auquel Projet Arachnid détecte les images suspectes<sup>3</sup> dépasse de loin les ressources humaines disponibles pour les examiner.

Pour les trois années de la période étudiée, le nombre d'images ciblées pour suppression par Projet Arachnid se chiffre à 626 110 (**Figure 1.0**). Trois facteurs expliquent l'écart important qui sépare le nombre de détections sur Internet et le nombre d'images ciblées pour suppression :

- 1 Les fichiers d'archive, qui contiennent parfois des centaines d'images, sont souvent traités par Projet Arachnid comme une initiative de suppression massive. Une demande de suppression peut donc porter sur de nombreuses images, mais elle ne comptera que pour une seule demande.
- 2 Souvent, le temps qu'une image soit vérifiée, elle aura été supprimée ou ne sera plus accessible, et elle n'aura plus à faire l'objet d'une demande de suppression. Il s'agit ici d'une conséquence de l'arriéré d'images à examiner.
- 3 Certaines images ont été trouvées sur le Web clandestin et l'identité du FSÉ est donc inconnue. Hormis la collecte de données, rien d'autre ne peut être fait dans ce genre de situations.

**Figure 1.0**

### Projet Arachnid – Sommaire des résultats (2018-2020)



N. B. Le nombre d'images vérifiées ciblées pour suppression ne tient pas compte du contenu des fichiers d'archive (qui peuvent contenir plusieurs milliers d'images), car une seule demande est envoyée pour l'ensemble du fichier.

Dans le rapport, nous présentons (**Tableau 1.0**) les données recueillies sur les FSÉ où Projet Arachnid a détecté au moins 5 000 images ou fichiers ayant fait l'objet d'une ou plusieurs demandes de suppression. Toutefois, pour des raisons techniques liées au traitement des images contenues dans les fichiers d'archive, les données se rapportant à un FSÉ en particulier — l'opérateur de télécommunications français Free — sont traitées différemment par Projet Arachnid et ne figurent donc pas dans le **Tableau 1.0**.

Le **Tableau 1.0** présente les principaux indicateurs se rapportant au nombre d'images détectées, aux délais de suppression et aux taux de récidence pour certains FSÉ. Soulignons que le nombre d'images détectées pour un FSÉ donné dépend d'une multitude de facteurs, dont le nombre de signalements venant du public, la nature du site Web et la nature de son contenu. Il faut donc exercer une certaine prudence lorsque l'on compare les données propres aux FSÉ.

3 Le terme *images suspectes* réfère à des images provenant uniquement de sites qui hébergent des images d'abus pédosexuels connues; il fait référence à des images dont il est raisonnable de soupçonner qu'elles constituent des images d'abus pédosexuels, mais qui n'ont pas encore été examinées.

## L'accessibilité des images d'abus pédosexuels mobilise une chaîne de FSÉ

Bien que le rapport établisse des recoupements entre certains FSÉ et l'accessibilité des images d'abus pédosexuels et des images préjudiciables ou violentes, il convient de noter que les données présentées ici ne sauraient à elles seules dresser un portrait complet du rôle de chaque FSÉ.

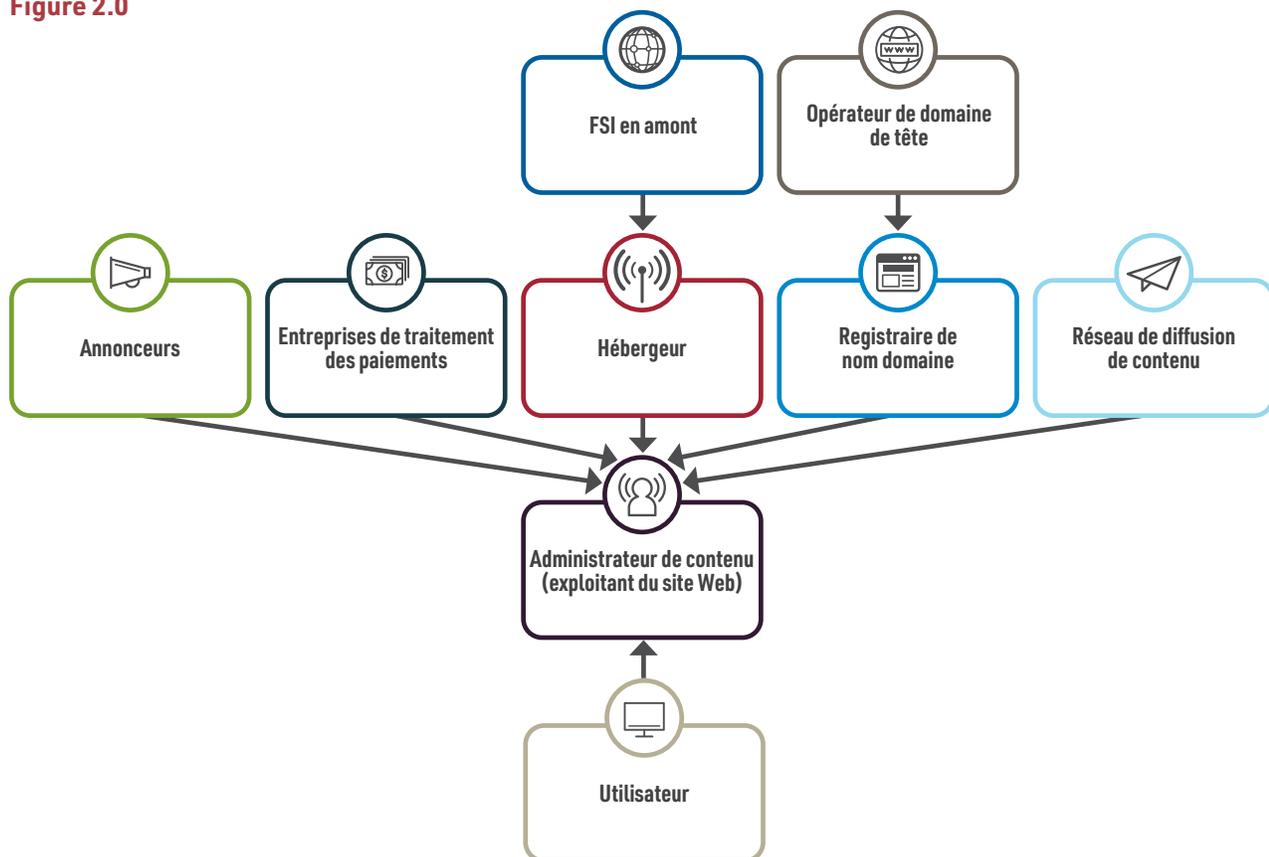
L'envoi des demandes de suppression aux FSÉ dépend généralement d'une combinaison de facteurs. Au final, c'est le degré de contrôle des FSÉ sur les images ciblées, leur réactivité aux demandes de suppression et la disponibilité de leurs coordonnées qui permettent de déterminer à qui les demandes sont adressées.

Les données propres aux FSÉ dans le rapport se rapportent aux entreprises à qui Projet Arachnid envoie des demandes de suppression; ces données ne reflètent pas l'entièreté de la chaîne de FSÉ qui concourent à l'accessibilité de chacune des photos ou des vidéos détectées.

La **Figure 2.0** illustre un point crucial : l'existence d'une seule photo ou vidéo sur Internet nécessite au final la collaboration de multiples fournisseurs de services, qui ont généralement tous une certaine capacité de limiter ou d'arrêter la prolifération des images d'abus pédosexuels et des images préjudiciables ou violentes sur certains services.

Le CCPE compte ajuster ses pratiques de collecte de données pour mieux rendre compte, dans ses prochains rapports, du rôle des FSÉ dans l'accessibilité des images d'abus pédosexuels sur Internet.

**Figure 2.0**



**Tableau 1.0**

<b>Sommaire des résultats se rapportant aux FSÉ (2018-2020)</b>					
<b>Nom du FSÉ</b>	<b>Type de service</b>	<b>Images vérifiées ciblées pour suppression</b>	<b>Délai de suppression (50<sup>e</sup> - médiane)</b>	<b>Délai de suppression (90<sup>e</sup> percentile)</b>	<b>Taux de récurrence</b>
ImageVenue	Administrateur de contenu	143 892	1 jour	1 jour	87,5 %
Serverel	Hébergeur	72 412	6 jours	60 jours	93,5 %
CloudFlare	Réseau de diffusion de contenu	49 183	1 jour	27 jours	48,6 %
Incrediserve LTD	Hébergeur	39 400	3 jours	53 jours	34,0 %
Trichan	Administrateur de contenu	34 157	1 jour	138 jours	26,2 %
NFOrce Entertainment B.V.	Hébergeur	23 211	8 jours	70 jours	5,9 %
ImgOutlet.com	Administrateur de contenu	18 582	2 jours	4 jours	4,9 %
ImgView.net	Administrateur de contenu	10 640	2 jours	6 jours	5,3 %
FranTech Solutions	Hébergeur	9 729	13 jours	40 jours	65,3 %
ImgDew.com	Administrateur de contenu	9 192	2 jours	6 jours	5,8 %
Host Sailor	Hébergeur	8 740	1 jour	15 jours	68,6 %
ColoCrossing	Hébergeur	7 809	27 jours	127 jours	35,5 %
ALFA TELECOM s.r.o.	Hébergeur	7 472	1 jour	4 jours	93,6 %
DataWeb Global Group B.V.	Hébergeur	7 103	1 jour	2 jours	11,4 %
ImgMaze.com	Administrateur de contenu	6 841	2 jours	6 jours	4,5 %
Liteserver Holding B.V.	Hébergeur	6 766	1 jour	43 jours	86,4 %
ImageBam	Administrateur de contenu	6 339	1 jour	1 jour	3,2 %
OVHcloud	Hébergeur	6 281	3 jours	23 jours	11,4 %

Ce tableau ne montre que les FSÉ qui accusent au moins 5 000 images ayant donné lieu à une demande de suppression..

Le FSÉ Free (dl.free.fr), qui héberge l'un des plus grands volumes d'images détectées, ne figure pas dans ce tableau, car les données le concernant ont été traitées différemment.

## RECOMMANDATIONS

Internet est un espace sans frontières où les FSÉ, pour échapper à la réglementation, choisiront inévitablement la voie de la moindre résistance pour structurer ou restructurer leurs activités, ou hébergeront ou relocaliseront leur contenu là où leurs activités seront tolérées.

Pour ces raisons, la lutte contre l'exploitation sexuelle des enfants nécessite une réponse coordonnée et internationale de la part des gouvernements disposés à adopter des normes mondiales pour la distribution des contenus sur Internet.

Les recommandations qui suivent découlent de la vaste expérience du CCPE en matière de réduction de l'accessibilité des images d'abus pédosexuels et des images préjudiciables ou violentes sur Internet. Pour les gouvernements et les décideurs politiques, ces recommandations seront d'une grande utilité dans l'élaboration de mesures réglementaires efficaces à destination des FSÉ dans une logique de protection des enfants.

### RECOMMANDATION 1 : Instaurer et imposer un devoir de diligence assorti de sanctions financières en cas de manquement

Les FSÉ qui omettent de se conformer aux exigences réglementaires ou de faire primer la sécurité des enfants sur Internet doivent encourir des sanctions financières proportionnelles à la gravité du préjudice causé.

Ces sanctions devraient à tout le moins prendre en considération les facteurs suivants :

- le nombre d'images en cause;
- le nombre d'utilisateurs qui ont vu les images;
- le nombre de fois où les images ont été republiées ou partagées;
- les délais de suppression;
- la gravité des images;
- le nombre, l'âge et la visibilité des victimes figurant dans les images.

De plus, à la réception d'un signalement de contenu problématique, les FSÉ en amont doivent être tenus financièrement responsables des images distribuées par leurs clients en aval qui pourraient avoir contrevenu aux exigences réglementaires.

## **RECOMMANDATION 2 : Imposer certaines obligations légales aux fournisseurs de services électroniques en amont et à leurs clients en aval**

Internet transcende les frontières et il n'existe guère de mesures réglementaires ou législatives concertées pour encadrer les activités des sociétés Internet. Au lieu de cela, l'espace numérique s'articule autour d'une multitude d'accords complexes et interdépendants entre toutes sortes d'entités qui ne sont pas toujours soumises aux mêmes lois et qui n'ont pas nécessairement la même tolérance face aux contenus illégaux.

Toutes les sociétés liées par ces accords contractuels ont un rôle à jouer pour que ces contenus soient rendus accessibles aux utilisateurs finaux. Ainsi, en cas de problème, chaque entité de ce système doit être soumise à des obligations contractuelles permettant de résoudre le problème et être tenue de soumettre ses propres clients à des obligations contractuelles similaires. Lorsqu'un acteur de la chaîne n'est pas soumis à de telles obligations ou qu'il ne veut ou ne peut pas forcer ses propres clients à respecter ses propres conditions, cette faille peut être exploitée et permettre ainsi au problème de prendre de l'ampleur.

De nombreux pays ont adopté des mesures législatives et réglementaires pour assurer la protection des consommateurs dans les domaines de l'assurance, de la vente de marchandises et de la protection de la vie privée; ils devraient en faire autant pour gérer ce qu'Internet est devenu. Il faut mettre en place des obligations légales et réglementaires qui fixent des normes minimales de base non négociables. Chaque acteur de la chaîne de fournisseurs doit être tenu par la loi d'adhérer à ces normes de base dans le cadre de ses propres activités et de soumettre ses clients à ces mêmes normes. Les règles doivent être harmonisées entre les pays de sorte qu'un FSÉ puisse être associé à au moins une personne réelle, et les pays doivent mettre fin aux interminables échappatoires juridiques qui permettent aux sociétés de s'exonérer de toute responsabilité légale à l'égard des préjudices qu'elles causent.

Les règles doivent s'appliquer à tout le moins aux entités qui fournissent des services d'hébergement d'images ou de fichiers et comporter au moins les éléments suivants :

- des définitions prédéfinies et des obligations de suppression pour les images d'abus pédosexuels et les images préjudiciables ou violentes;
- des mesures de responsabilisation à prendre par le fournisseur lorsque des images illégales ou des images préjudiciables ou violentes sont hébergées par un de ses clients;
- des sanctions sévères et significatives pour les fournisseurs qui négligent de prendre certaines mesures lorsque leurs clients contreviennent aux obligations de suppression.



### **RECOMMANDATION 3 :** **Obliger les plateformes qui hébergent des contenus générés par les utilisateurs à utiliser des outils automatisés de détection proactive des images**

Il arrive souvent que des images d'abus pédosexuels et des images préjudiciables ou violentes précédemment signalées réapparaissent sur les serveurs d'un FSÉ. On peut remédier à la situation à l'aide de technologies automatisées de reconnaissance d'empreintes numériques.

La réglementation doit obliger les plateformes qui hébergent des contenus générés par les utilisateurs à utiliser des outils de détection proactive des images. Elle doit aussi établir clairement les exigences minimales d'une stratégie de détection automatique efficace, sachant qu'il existe un large éventail de technologies de détection d'images. Ces mesures doivent inclure l'obligation d'ajouter les empreintes numériques des images supprimées à des listes de blocage afin d'empêcher leur remise en ligne.

Des sanctions significatives doivent être prévues et imposées en cas d'échec à empêcher la remise en ligne d'images dont les empreintes numériques correspondent celles d'images précédemment supprimées.

Ces obligations doivent également s'appliquer comme condition de service aux clients d'un fournisseur de services notamment si ce dernier met son infrastructure à la disposition de services d'hébergement d'images et de fichiers.

## **RECOMMANDATION 4 :** **Établir des normes quant aux contenus qui, sans nécessairement être illégaux, restent préjudiciables ou violents à l'égard de personnes mineures**

Il est fondamentalement problématique d'utiliser, hors contexte, les définitions des images d'abus pédosexuels au sens du droit pénal pour décider si telle ou telle photo ou vidéo devrait être retirée de la vue du public. Le fait de limiter un cadre réglementaire à des définitions aussi restrictives permet à un grand nombre d'images préjudiciables ou violentes à l'endroit d'enfants de proliférer sur Internet.

Voici quelques exemples de matériel préjudiciable ou violent qui ne répondrait pas nécessairement à une définition pénale dans tous les pays :

- une série d'images, dont certaines ont été prises avant ou après l'enregistrement de l'acte d'abus;
- des images d'enfants en maillot de bain distribuées sur des forums voués à la sexualisation des enfants;
- des images d'enfants en train d'uriner;
- des images d'enfants vêtus ou à demi vêtus dans des poses provocantes (désignées à tort comme du « mannequinat juvénile »);
- des images de violence physique ou de torture à l'encontre d'enfants;
- de l'information sur des tactiques de conditionnement ou d'abus d'enfants;
- des textes qui décrivent des abus pédosexuels ou qui visent à promouvoir de tels abus;
- des commentaires sexuels sur une photo ou une vidéo d'un enfant;
- des renseignements personnels dévoilés au sujet d'un enfant.

Ce genre de matériel doit être bien défini et incorporé dans la réglementation et pris en compte dans la définition des images d'abus pédosexuels ou de la violence faite aux enfants dans le contexte de tout cadre ou de toute initiative de grande envergure visant à protéger les enfants.

## RECOMMANDATION 5 : Imposer des normes de modération humaine

La détection proactive automatisée repose sur la comparaison des images entrantes avec des banques d'images précédemment supprimées. Cette technologie s'avère donc inefficace pour détecter des images nouvellement créées ou des images encore jamais détectées puisqu'il n'existe pas d'images avec lesquelles des correspondances peuvent être établies.

La modération humaine est donc un moyen de défense essentiel contre les images d'abus pédosexuels et les images préjudiciables ou violentes pour les plateformes qui acceptent des contenus générés par les utilisateurs.

La réglementation doit fixer des exigences précises concernant :

- le bon encadrement des équipes de modération de contenu;
- la formation continue des modérateurs, notamment en ce qui concerne l'évaluation de la maturité sexuelle;
- le nombre de modérateurs à prévoir en fonction du volume de contenu entrant.

La réglementation doit aussi faire en sorte que les contenus générés par les utilisateurs sur les plateformes qui autorisent la pornographie et la nudité dans leurs conditions générales d'utilisation fassent l'objet d'une vérification manuelle avant publication.

Il est essentiel que les pratiques de modération soient alignées sur les définitions des images d'abus pédosexuels et des images préjudiciables ou violentes dans le cadre réglementaire global.

## **RECOMMANDATION 6 :** **Fixer des exigences pour la vérification du** **consentement des sujets et de l'identité des** **utilisateurs**

Les plateformes non modérées qui acceptent des contenus venant d'utilisateurs anonymes sont souvent utilisées pour distribuer des images d'abus pédosexuels et des images préjudiciables ou violentes.

Les FSÉ qui acceptent des contenus générés par les utilisateurs, en particulier ceux dont l'offre de contenu se compose en tout ou en partie de matériel pornographique et d'images de nudité, risquent davantage d'être confrontés à des images d'abus pédosexuels et des images préjudiciables ou violentes.

La réglementation doit :

- préciser clairement des règles proportionnelles au niveau de risque des sites pour vérifier l'identité des utilisateurs;
- préciser en quoi consiste la vérification et fixer des exigences pour la conservation, la consultation et la divulgation des données de vérification;
- dans le cas de contenus pornographiques ou choquants, fixer des exigences précises concernant la vérification de l'âge des sujets figurant sur les photos et les vidéos;
- dans le cas de contenus pornographiques ou choquants, fixer des exigences précises concernant la vérification du consentement de tous les sujets aux actes enregistrés ainsi qu'à la distribution des images.

## **RECOMMANDATION 7 :** **Instaurer des normes de conception de plateformes qui réduiront les risques et augmenteront la sécurité**

En plus de prendre des mesures de modération proactives et réactives, les plateformes doivent diminuer encore davantage la prolifération d'images d'abus pédosexuels et d'images préjudiciables ou violentes en dissuadant l'utilisation de leurs services à cette fin.

La réglementation doit obliger les FSÉ à :

- interdire la mise en ligne de contenus générés par des utilisateurs qui viennent d'un nœud de sortie Tor, qui passent par un réseau privé virtuel ou qui utilisent d'autres techniques de dissimulation d'adresse IP;
- bloquer les termes de recherche et les noms de forums et de clavardoirs associés aux images d'abus pédosexuels et aux images préjudiciables ou violentes;
- supprimer ou suspendre les comptes d'utilisateurs qui distribuent des images d'abus pédosexuels ou des images préjudiciables ou violentes ou qui accèdent à de telles images;
- prévoir la séparation des enfants et des adultes dans la conception même des plateformes numériques ou, à défaut, mettre en place des règles et des protections additionnelles;
- offrir aux utilisateurs un mécanisme simple et réactif pour porter plainte aux administrateurs du contenu.
- prévoir des mesures (vérification d'âge, etc.) pour empêcher les enfants d'accéder à des contenus destinés à un public adulte.

## **RECOMMANDATION 8 : Établir des normes quant aux mécanismes de signalement d'utilisateurs et des obligations de suppression d'images**

La modération humaine ne permet pas toujours de détecter les images d'abus pédosexuels et les images préjudiciables ou violentes. Les FSÉ doivent donc offrir des interfaces simples pour signaler un utilisateur ou formuler une plainte et être soumis à des obligations de suppression précises.

La réglementation devrait établir des normes claires en ce qui concerne :

- la possibilité de pouvoir signaler directement tout utilisateur et tout type de contenu (photos, vidéos, pages Web, commentaires, messages, etc.);
- l'inclusion de catégories de signalement précises (notamment pour les images d'abus pédosexuels) afin d'assurer un traitement prioritaire des contenus présentant un degré de risque élevé;
- la suspension ou la mise hors ligne instantanée des contenus associés à des signalements d'images d'abus pédosexuels ou d'images préjudiciables ou violentes jusqu'à leur examen (plutôt que leur maintien en ligne en attendant leur examen);
- l'imposition de délais pour l'examen et la suppression des images suite à la réception d'une plainte;
- la conservation des informations relatives à l'image, à l'utilisateur qui l'a mise en ligne, aux communications avec le plaignant et aux mesures prises suite à la plainte;
- le signalement obligatoire des images à une autorité ou à une centrale de signalement désignée et les exigences de transparence concernant leur suppression ou leur non-suppression.

## CONCLUSION

De nombreuses sociétés Internet se préoccupent peu de la sécurité et du droit à la vie privée des enfants sur Internet. Le flou juridique qui règne dans l'espace numérique ainsi que l'absence de réglementation claire ou de transparence contribuent largement à la prolifération des images d'abus pédosexuels et des images préjudiciables ou violentes sur Internet.

Le rapport, basé sur trois années de données recueillies par Projet Arachnid, analyse les caractéristiques de 5,4 millions de photos et de vidéos d'abus pédosexuels et d'images préjudiciables ou violentes détectées sur les serveurs de 760 FSÉ.

Il en ressort que de nombreuses sociétés Internet tardent souvent à donner suite aux demandes de suppression d'images et accusent des taux de récurrence élevés. Ce constat montre que de nombreux FSÉ ne déploient pas suffisamment de ressources pour réduire sensiblement voire éliminer la présence d'images d'abus pédosexuels et d'images préjudiciables ou violentes sur leurs serveurs.

Le rapport montre aussi :

- que le Web clandestin facilite l'accès aux images d'abus pédosexuels sur le Web visible;
- qu'un nombre relativement peu élevé de FSÉ peut avoir un impact considérable sur l'accessibilité des images d'abus pédosexuels sur Internet;
- que les statistiques sur les victimes adolescentes sous-estiment largement la véritable ampleur des préjudices qu'elles subissent;
- que certains FSÉ peu connus facilitent beaucoup l'accessibilité des images d'abus pédosexuels et des images préjudiciables ou violentes sur Internet;
- qu'il faut aussi s'intéresser aux autres acteurs de la chaîne de FSÉ qui facilitent l'accessibilité des images d'abus pédosexuels sur Internet.

Le rapport suggère fortement que l'on ne peut attendre de l'industrie qu'elle investisse volontairement des ressources pour prévenir la prolifération des images d'abus pédosexuels et des images préjudiciables ou violentes. Il fait état d'un besoin pressant de mettre en place des normes cohérentes, applicables et universelles pour obliger les FSÉ à rendre des comptes.

À la lumière de ces résultats, huit grandes recommandations fondées sur des données probantes sont présentées aux gouvernements soucieux de réduire l'accessibilité et la distribution des images d'abus pédosexuels sur Internet et de prendre des mesures pour faire primer la sécurité des enfants.

Le rapport offre à la fois une feuille de route et un incitatif pour étendre comme il se doit à l'espace numérique notre devoir de diligence envers les enfants.



**CENTRE CANADIEN de PROTECTION DE L'ENFANCE**<sup>MC</sup>

*Aider les familles. Protéger les enfants.*

 [protegeonsnosenfants.ca](http://protegeonsnosenfants.ca)

 @ProtegerEnfant

 Centre canadien de protection de l'enfance