CENTRE CANADIEN *de* PROTECTION DE L'ENFANCE[MC]

Aider les familles. Protéger les enfants.

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

Projet Arachnid[MD]

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

Photo de mannequin. Pour illustrer le texte.

CENTRE CANADIEN *de* PROTECTION DE L'ENFANCE[MC]

Aider les familles. Protéger les enfants.

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

© 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.

Photo de mannequin. Pour illustrer le texte.

TABLE DES MATIÈRES

SOMMAIRE

Le Centre canadien de protection de l'enfance (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.

Ce rapport a pour objectif de fournir aux gouvernements des données cruciales pour prendre les décisions qui auront le plus de chances de réduire efficacement l'accessibilité et la distribution des images d'abus pédosexuels sur Internet. L'analyse fait ressortir la nécessité de mettre en place des normes cohérentes et applicables pour obliger les fournisseurs de services électroniques (FSÉ) à rendre des comptes.

Organisation centrée sur les survivant.e.s, le CCPE a investi des ressources dans le développement de « Projet Arachnid », un outil spécialisé qui détecte les images d'abus pédosexuels sur le Web (visible et clandestin) et qui adresse des demandes de suppression aux FSÉ les plus susceptibles de pouvoir remédier immédiatement au maintien en ligne de ces images.

Le champ d'action de Projet Arachnid ne s'étend généralement pas aux plateformes semi-fermées que sont les médias sociaux grand public. Comme l'analyse présentée ici se limite à une sous-section du Web, elle sous-estime grossièrement l'accessibilité véritable des images d'abus pédosexuels sur Internet. Ce rapport n'attire donc pas l'attention sur les grands acteurs de l'industrie de la technologie, mais sur les grands réseaux de FSÉ méconnus qui contribuent au problème.

De l'analyse des trois années de la période étudiée (2018-2020), on peut dégager les constats suivants :

Projet Arachnid a détecté et vérifié plus de **5,4 millions d'images** et adressé des demandes de suppression à plus de **760 FSÉ** dans le monde.

Près de la moitié **(48 %) des images** détectées sont liées à un service d'hébergement de fichiers exploité par un opérateur de télécommunications français.

La grande majorité **(97 %) des images** d'abus pédosexuels détectées par Projet Arachnid étaient physiquement hébergées sur le Web visible. En revanche, le Web clandestin joue un rôle disproportionné en dirigeant les internautes vers des endroits du Web visible où se trouvent de telles images.

Projet Arachnid a fait la preuve de son efficacité avec un délai de suppression médian de **24 heures**. Il est toutefois troublant de constater que 10 % des images signalées sont restées en ligne plus de sept semaines (42 jours) avant de devenir inaccessibles.

Dans l'ensemble, les images d'adolescents plus âgés (à l'état post-pubère) mettent **beaucoup plus de temps** à être supprimées que les images de victimes plus jeunes (à l'état prépubère).

Près de la moitié **(48 %) des images** pour lesquelles Projet Arachnid a envoyé une demande de suppression avaient déjà été signalées au même fournisseur de services auparavant.

Au moment de la rédaction du présent rapport, le CCPE accuse un arriéré de plus de **32,8 millions d'images** suspectes[1] à examiner. Le rythme auquel Projet Arachnid détecte les images suspectes dépasse de loin les ressources humaines disponibles pour les examiner.

1 Le terme *images suspectes* s'entend d'images provenant uniquement de sites qui hébergent des images d'abus pédosexuels connues; il fait référence à des images dont il est raisonnable de penser qu'elles constituent des images d'abus pédosexuels ou des images préjudiciables ou violentes, mais qui n'ont pas encore été examinées.

Ces constats, en particulier les taux élevés de récidive et les délais de suppression souvent longs, donnent à penser que de nombreux FSÉ ne déploient pas suffisamment de ressources pour éliminer, ou du moins limiter, la présence d'images d'abus pédosexuels et d'images préjudiciables ou violentes sur leurs serveurs.

Même les résultats plutôt positifs en apparence occultent l'un des principaux aspects de la problématique. Certes, de nombreux FSÉ donnent suite aux demandes de suppression dans les 24 heures, mais 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 ciblées. Ils n'ont pas à subir de conséquences pour leur inaction en matière de prévention. Les forts taux de récidive d'images rapportés ici témoignent crument de cette réalité.

De nombreux FSÉ bénéficient actuellement de la large immunité que leur confère la loi aux États-Unis. Ils bénéficient en outre d'un climat général d'incertitude juridique et d'une réglementation inadaptée de l'espace numérique à l'échelle mondiale.

Dans ce contexte, les recommandations suivantes pourraient aider les gouvernements à élaborer des cadres réglementaires efficaces et cohérents pour remédier à la situation :

	**1. Instaurer et imposer un devoir de diligence assorti de sanctions financières en cas de manquement.**
	**2. Imposer certaines obligations légales aux fournisseurs de services électroniques en amont et à leurs clients en aval.**
	**3. Obliger les plateformes qui hébergent des contenus générés par les utilisateurs à utiliser des outils automatisés de détection proactive d'images.**
	**4. Établir des normes quant aux contenus qui, sans nécessairement être illégaux, restent préjudiciables ou violents à l'égard de personnes mineures.**
	**5. Imposer des normes de modération humaine.**
	**6. Fixer des exigences pour la vérification du consentement des sujets et de l'identité des utilisateurs.**
	**7. Instaurer des normes de conception de plateformes qui réduiront les risques et augmenteront la sécurité.**
	**8. Établir des normes quant aux mécanismes de signalement d'utilisateurs et des obligations de suppression d'images.**

L'urgence d'agir pour remédier au manque d'encadrement de l'espace numérique et à l'absence de sanctions significatives pour les graves préjudices causés aux enfants fait de plus en plus consensus au sein de l'opinion publique. Le présent rapport offre une feuille de route aux gouvernements pour élaborer des politiques et agir de concert dans la lutte mondiale et transfrontalière contre l'exploitation des enfants.

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.

Photo de mannequin. Pour illustrer le texte.

Collaborations avec des groupes de défense des intérêts des survivant.e.s

En plus de nos interventions individuelles auprès de survivant.e.s, nous collaborons avec plusieurs groupes de défense des intérêts des survivant.e.s :

Phoenix 11

Depuis plus de trois ans, le CCPE et l'organisme américain NCMEC (National Center for Missing and Exploited Children) travaillent avec les Phoenix 11, un groupe de survivantes d'abus pédosexuels enregistrés et, dans la plupart des cas, diffusés sur Internet. Ces survivantes se sont mobilisées pour dénoncer haut et fort l'insuffisance des moyens déployés face à la prolifération des images d'abus pédosexuels sur Internet.

Chicago Males

Le CCPE et le NCMEC ont commencé à travailler avec un groupe de survivants dans le but d'apprendre de leur vécu et de mieux comprendre la stigmatisation sociale qui afflige les hommes victimes d'abus sexuels. Les membres de ce groupe unissent leurs voix pour plaider en faveur des changements qui s'imposent dans la lutte contre les abus pédosexuels sur Internet et le soutien aux survivants.

Aramid Collective

En 2020, le CCPE a été mis en contact avec un groupe de survivant.e.s qui surveillent la diffusion de leurs images d'abus pédosexuels et qui les signalent aux hébergeurs pour en obtenir la suppression. Ce groupe utilise son savoir et sa voix pour défendre les intérêts des survivant.e.s et demander la suppression urgente des photos et des vidéos d'abus pédosexuels qui existent sur de nombreuses plateformes.

Mères de survivant.e.s d'abus pédosexuels

Pour en savoir plus sur les difficultés que vivent encore les familles de survivant.e.s des années après la fin des abus physiques, le CCPE a réuni un groupe de mères d'enfants victimes d'abus sexuels enregistrés et diffusés sur Internet. Elles nous ont appris qu'elles vivent un continuum émotionnel qui se perpétue bien au-delà de la « découverte » de l'abus et qui est souvent marqué par la perte de relations, l'instabilité financière et une préoccupation constante pour la sécurité de leurs enfants, entre autres choses. Leur éclairage est crucial pour orienter la création de ressources de soutien.

« Pendant très longtemps, on ne pouvait y changer quoi que ce soit. C'est sur Internet – un trou noir rempli de code exempt de toute loi. Il existe maintenant une solution pour lutter contre les images d'abus pédosexuels, et cette solution s'appelle Projet Arachnid. » ***– Une membre des Phoenix 11***

INTRODUCTION

Ce rapport vise à fournir aux acteurs du dossier, dont les gouvernements et les FSÉ, de précieuses informations qui leur permettront de prendre des mesures efficaces pour contrer la distribution des images d'abus pédosexuels sur Internet et l'accessibilité de ces images.

Les images d'abus pédosexuels perpétuent un cycle de souffrance pour les enfants 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 des mesures de protection des enfants.

Nous savons que l'une des clés pour résoudre ce problème est de bien comprendre comment les sociétés Internet — en particulier celles qui acceptent des contenus générés par les utilisateurs — facilitent l'accès aux images d'abus illégales et contribuent à leur prolifération.

La nature criminelle d'une bonne partie de ces images présente des obstacles du point de vue de la recherche, de la sensibilisation du public et de l'élaboration des politiques. Avec le temps, ces obstacles ont engendré une méconnaissance de la nature de ces images, de leur prolifération sur Internet et de la façon dont elles sont diffusées ou dont on y accède.

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. Lorsque les entreprises privées sont assujetties à une obligation de signalement, les données qu'elles déclarent ne sont pas vérifiées de manière indépendante et le contenu des signalements eux-mêmes est limité.

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 et les survivant.e.s.

En pareilles circonstances, l'élaboration de politiques ou de règlements fondés sur des données fiables pose un sérieux casse-tête. Le présent rapport apporte quelques éléments d'information 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[2] liées à certaines plateformes. Le présent 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.

2 La notion d'images *préjudiciables ou violentes* est définie à la page 10.

Photo de mannequin. Pour illustrer le texte.

PROJET ARACHNID : UNE SOLUTION TECHNOLOGIQUE POUR DÉTECTER LES IMAGES D'ABUS PÉDOSEXUELS

Projet Arachnid est une solution novatrice du CCPE pour combattre la prolifération grandissante des images d'abus pédosexuels sur Internet.

Lancé en 2017, cet outil centré sur les victimes explore le Web[3] 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.

Fonctionnement

Projet Arachnid détecte les images d'abus pédosexuels en explorant des adresses URL publiquement accessibles qui ont été signalées à Cyberaide.ca ainsi que des contenus situés à des adresses URL du Web visible et du Web clandestin qui sont connues pour héberger des images d'abus pédosexuels. Lorsque des images (photos, vidéos ou fichiers d'archive) sont détectées à une adresse URL, le système compare leurs empreintes numériques à une banque d'empreintes numériques d'images vérifiées. Si le système détecte une correspondance entre les empreintes numériques, une demande de suppression est automatiquement adressée à l'administrateur du contenu ou à l'hébergeur.

Projet Arachnid revérifie les adresses délinquantes toutes les 24 heures et continue d'envoyer des demandes de suppression jusqu'à ce que les images en cause ne soient plus détectées. Par sa capacité de traiter des dizaines de milliers d'images à la seconde, Projet Arachnid surpasse largement les méthodes habituellement utilisées pour trouver ces images préjudiciables et en obtenir la suppression.

La majeure partie des empreintes numériques conservées dans la banque d'images vérifiées ont été prélevées sur des photos et des vidéos examinées par des analystes du CCPE, par des équipes d'analystes d'autres centrales de signalement vouées à la protection des enfants et par des forces policières canadiennes et internationales.

Shield par Projet Arachnid

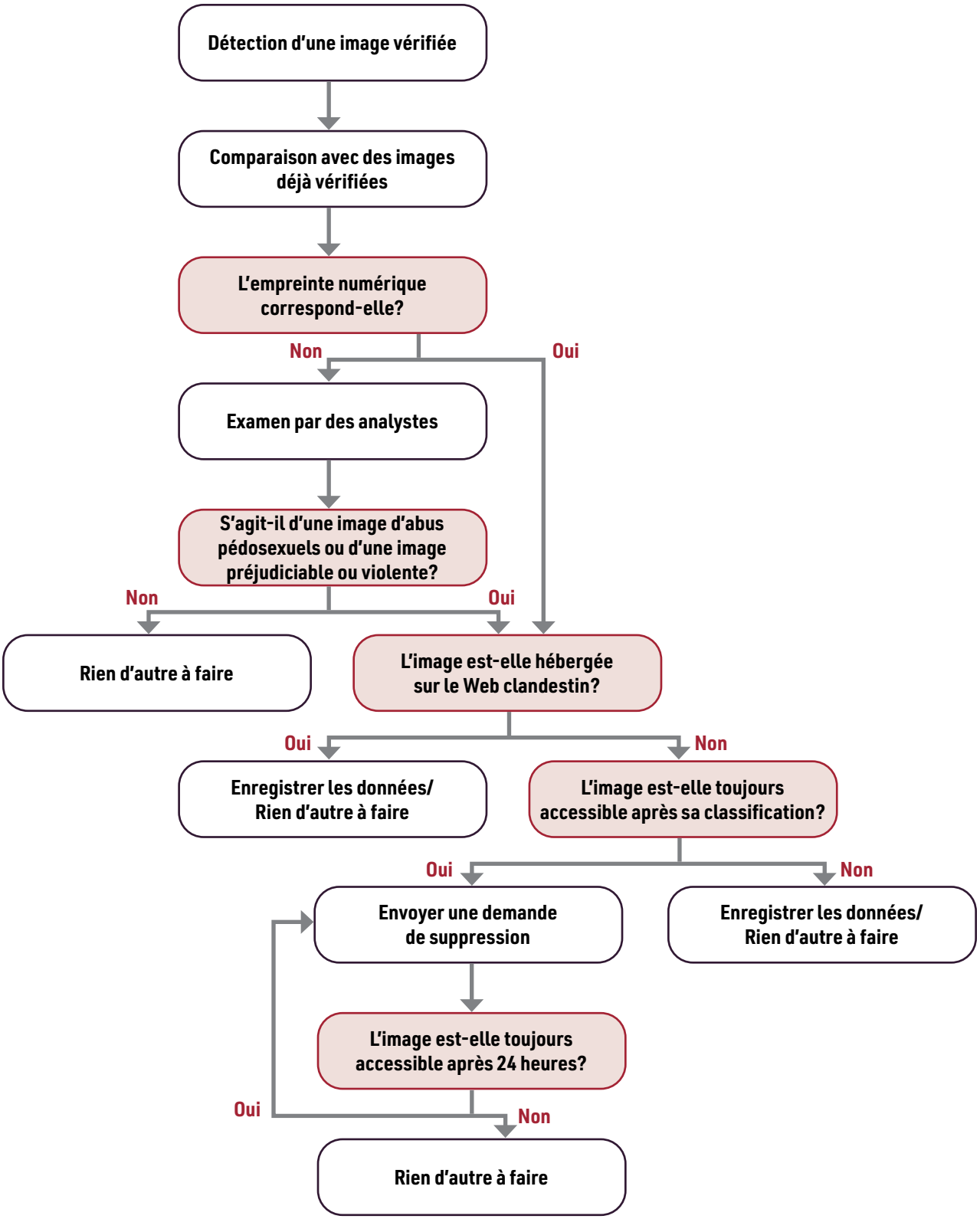
En plus chercher activement les images nocives sur le Web visible, la plateforme de Projet Arachnid met gratuitement à la disposition de l'industrie un outil pour faciliter la détection proactive des images d'abus pédosexuels connues.

Shield par Projet Arachnid permet aux administrateurs de contenu ou aux hébergeurs de comparer proactivement les images entrantes ou existantes sur leurs serveurs avec la banque d'empreintes numériques de Projet Arachnid. Les FSÉ peuvent intégrer cet outil dans leur stratégie globale de modération de contenu afin d'améliorer et d'accélérer la détection et la suppression des images d'abus pédosexuels ou des images préjudiciables ou violentes.

On trouvera une présentation plus détaillée de Projet Arachnid à ProjetArachnid.ca

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

Projet Arachnid en action

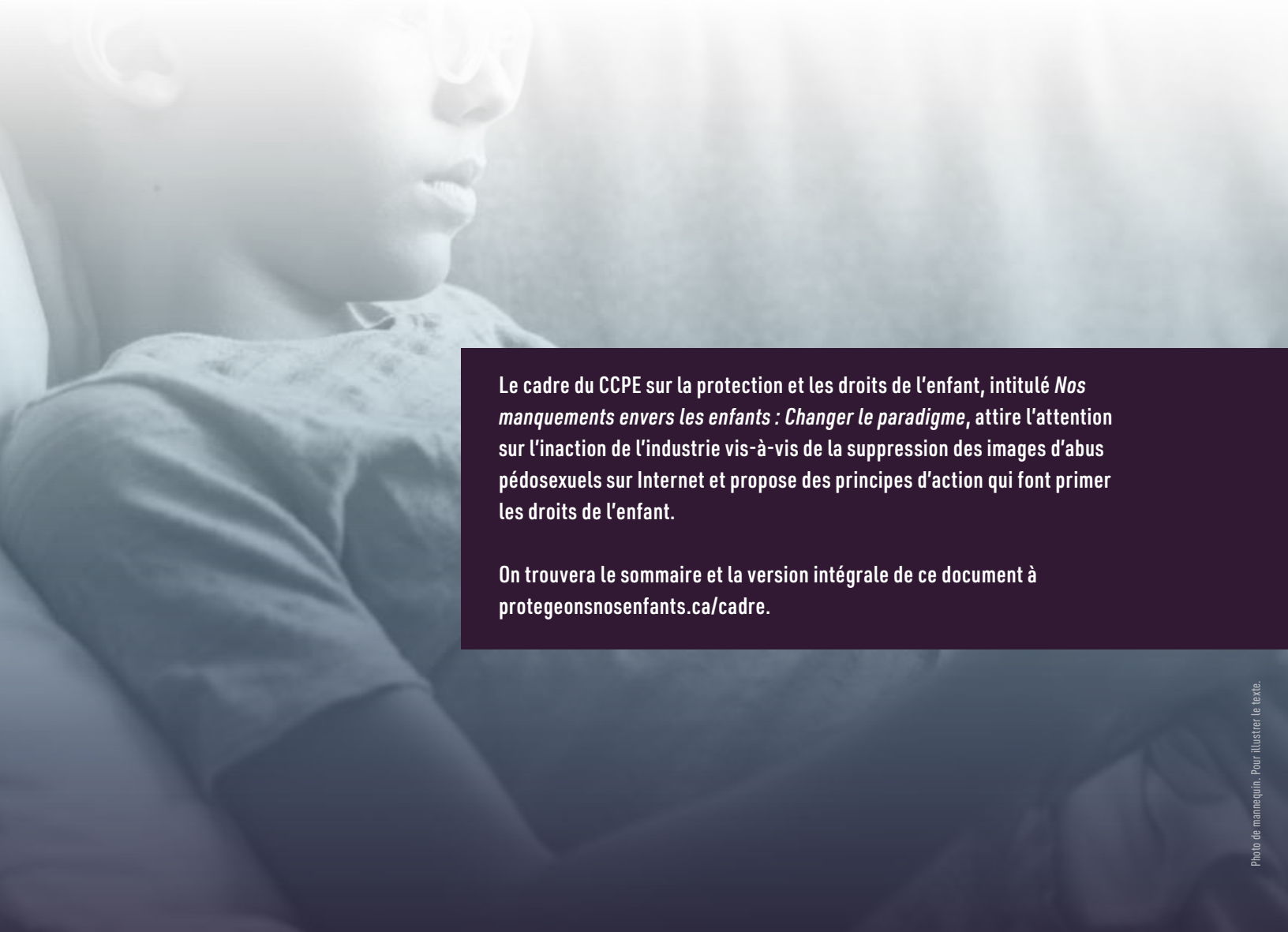


IMAGES ILLÉGALES ET IMAGES PRÉJUDICIABLES OU VIOLENTES : LE CADRE DU CCPE

Les efforts de suppression d'images ont tendance à porter principalement sur des images dont l'illégalité ne fait aucun doute. Malheureusement, cette approche étroite et restrictive est en décalage avec la violence perpétrée contre les enfants sur Internet. Elle permet à un grand nombre d'images préjudiciables ou violentes de circuler en toute impunité puisqu'elles ne dérogent apparemment pas à une définition pénale, surtout si on les considère en dehors du contexte plus large dans lequel elles ont été produites et distribuées.

Il est évident que le fait de limiter les efforts de suppression aux images manifestement illégales s'avère une approche malavisée et insuffisante du point de vue de la protection des enfants à l'échelle mondiale. Soucieux de remédier à cette triste situation, le CCPE a élaboré en 2019 un cadre pour la protection et les droits de l'enfant sur la base d'informations issues de sa proche collaboration avec des survivant.e.s et de la mise en œuvre de Projet Arachnid. Ce cadre établit un nouvel ensemble de principes d'action qui placent l'intérêt supérieur et la protection des enfants au centre des efforts de suppression d'images.

Suite à la publication de ce cadre, le champ d'activité de Cyberaide.ca et de Projet Arachnid s'est progressivement élargi de sorte que les images jusque là mises de côté soient désormais prises en compte.



Le cadre du CCPE sur la protection et les droits de l'enfant, intitulé *Nos manquements envers les enfants : Changer le paradigme*, attire l'attention sur l'inaction de l'industrie vis-à-vis de la suppression des images d'abus pédosexuels sur Internet et propose des principes d'action qui font primer les droits de l'enfant.

On trouvera le sommaire et la version intégrale de ce document à protegeonsnosenfants.ca/cadre.

Photo de mannequin. Pour illustrer le texte.

Photo de mannequin. Pour illustrer le texte.

Images d'abus pédosexuels et images préjudiciables ou violentes

Les demandes de suppression et les initiatives de collecte de données du CCPE visent principalement deux catégories d'images :

1. les photos et les vidéos qui, selon l'examen qui en a été fait, répondent à une définition pénale;
2. les photos et les vidéos préjudiciables ou violentes d'enfants qui ne répondent pas nécessairement à une définition pénale.

Les images préjudiciables ou violentes d'enfants qui ne répondent pas à une définition pénale peuvent néanmoins violer les conditions générales d'utilisation d'un FSÉ. Ces images pourraient aussi s'avérer abjectes au point qu'aucun FSÉ respectable ne les hébergerait, surtout si ledit FSÉ est assujetti à des normes ou à un organisme de réglementation.

Par exemple, de nombreuses plateformes interdisent la diffusion d'images non autorisées de personnes mineures, de données personnelles ou de matériel protégé par le droit d'auteur ainsi que le harcèlement et le conditionnement *(grooming)* d'enfants.

Dans ce rapport, le terme « images préjudiciables ou violentes » désigne des photos et des vidéos qui sont potentiellement associées à un abus pédosexuel, qui mettent en scène des enfants partiellement nus et qui ont été rendues publiques ou qui sont utilisées dans un contexte sexuel. Il englobe aussi les photos et les vidéos rendues publiques d'enfants en situation d'abus, de torture ou de contention.

Voici quelques exemples typiques d'images considérées préjudiciables ou violentes :

- la photo d'un enfant au visage maculé d'une substance qui semble être du sperme;
- les premières images fixes d'une vidéo d'agression sexuelle connue qui montrent l'enfant encore vêtu ou partiellement dénudé et qui ont été prises avant l'agression proprement dite. Prises isolément, ces images ne répondront pas nécessairement à une définition pénale, mais elles font partie d'un plus grand ensemble d'images illégales;
- des images d'enfants ou d'adolescents en maillot de bain qui ont été dérobées sur des comptes de médias sociaux et publiées sur des sites voués à l'exploitation sexuelle des enfants;
- des images à caractère sexuel d'un enfant qui, dans l'intention de suggérer la disponibilité sexuelle de l'enfant, représentent celui-ci dans des positions ou des actes qui relèvent de la sexualité adulte. Ici, l'enfant peut être entièrement ou partiellement vêtu.
- des photos ou des vidéos de violence physique ou de torture à l'encontre d'un enfant.

Où se trouvent les images d'abus pédosexuels et les images préjudiciables ou violentes

On s'imagine souvent à tort que les images d'abus pédosexuels et les images préjudiciables ou violentes ne se trouvent que sur le Web clandestin. Or, la majorité des images illégales détectées par Projet Arachnid se cachent au grand jour sur le Web visible; on les trouve sur des services d'hébergement d'images et de fichiers, des forums et des réseaux de diffusion de contenu, et des sites de pornographie adulte grand public et spécialisés.

Ce tableau donne une vue d'ensemble de la variété d'endroits où Projet Arachnid et les analystes de Cyberaide.ca ont trouvé des images d'abus pédosexuels ou des images préjudiciables ou violentes[4] :

Type	Exemples de services et de plateformes
Sites d'hébergement d'images	Imgur[MD], ImageShack[TM], Flickr[MD], PostImage
Sites d'hébergement de fichiers	Megaupload, Dropbox[MD], WeTransfer[MC], dl.free.fr
Fournisseurs de services infonuagiques, serveurs privés virtuels, hébergeurs Web traditionnels	Amazon[MD] AWS[MC], Microsoft[MD] Azure[MC], Rackspace[MD], GoDaddy[MD], DreamHost[MD]
Réseaux de diffusion de contenu (CDN)	Cloudflare[MD], Fastly[MD], Akamai[MD]
Forums et clavardoirs du Web clandestin	Sites principalement hébergés à des adresses en .onion du réseau Tor.
Résultats/cache des moteurs de recherche	Google[MD], Bing[MD], Yahoo![MD], Yandex[MD]
Forums/Clavardoirs/Services de messagerie	Reddit[MD], Twitch[MD], 4chan[MC], Discord[MC], WhatsApp[MD], Kik[MD]
Sites de pornographie adulte (spécialisés)	Intérêts particuliers/fétichisme, pornodivulgation
Sites de pornographie adulte (grand public)	Pornhub[MD], XVIDEOS[MC], YouPorn[MD]
Médias sociaux	Twitter[MD], Facebook[MD], Instagram[MD], Snapchat[MD]

4 Ces exemples ne reflètent pas toutes les possibilités; ils ne servent qu'à illustrer les différents types afin d'éclairer le lecteur.

Toutes les marques de commerce identifiées par le symbole « [MD] » sont enregistrées par leur propriétaire au Canada et aux États-Unis; toutes les marques de commerce identifiées par le symbole « [MC] » sont enregistrées uniquement aux États-Unis.

MÉTHODOLOGIE

Collecte des données

Projet Arachnid détecte les images d'abus pédosexuels et les images préjudiciables ou violentes connues ou potentielles de trois façons :

1. en explorant les adresses URL publiquement accessibles qui ont déjà été signalées à Cyberaide.ca;
2. en explorant les adresses URL publiquement accessibles et les images qui ont été signalées directement à l'API de Projet Arachnid par les entreprises participantes;
3. en explorant certains secteurs du Web clandestin et du Web visible connus pour héberger des images d'abus pédosexuels.

Lorsque Projet Arachnid détecte des images suspectes, ces images sont examinées puis catégorisées par des analystes spécialement formés du CCPE et d'autres centrales de signalement participantes.

Projet Arachnid conserve alors les fichiers ainsi que les données pertinentes s'y rapportant, dont la date de détection et les entités à qui des signalements ont été adressés. C'est sur ces données primaires que repose l'analyse présentée ici.

Catégories d'images

Pour les besoins du présent rapport, les images sont organisées en trois catégories simplifiées dérivées du processus d'examen interne de Projet Arachnid.

Images d'enfants prépubères
Cette catégorie regroupe des images d'abus pédosexuels susceptibles de répondre à une définition pénale d'une image d'abus pédosexuels. Les victimes représentées sur ces images sont à l'état prépubère ou au début de la puberté.

Images d'enfants post-pubères
Cette catégorie regroupe des images d'abus pédosexuels susceptibles de répondre à une définition pénale d'une image d'abus pédosexuels. Les victimes représentées sur ces images sont à l'état post-pubère, et il a été établi qu'elles étaient enfants au moment où les images ont été produites. Entrent aussi dans cette catégorie des images d'enfants aux derniers stades de la puberté.

Images préjudiciables ou violentes
Cette catégorie regroupe des images d'enfants qui ne semblent pas répondre aux définitions pénales utilisées dans plusieurs pays, mais qui pourraient néanmoins violer les conditions générales d'utilisation d'un FSÉ. Ces images peuvent aussi porter atteinte à la vie privée ou à la sécurité d'un enfant ou être associées à des images d'abus pédosexuels. Pour une description plus détaillée de cette catégorie d'images, voir le cadre du CCPE (p. 10).

Principales mesures de transparence

Images détectées, images ciblées pour suppression et demandes de suppression

Projet Arachnid génère des données qui peuvent être analysées à l'aide de plusieurs mesures. La quantification de l'offre d'images et des demandes de suppression se fait de trois manières :

Images détectées
Il s'agit du nombre total d'images d'abus pédosexuels et d'images préjudiciables ou violentes détectées par Projet Arachnid. Cette mesure correspond au nombre total de fichiers (photos, vidéos et fichiers d'archive multimédias) détectés dans les parties d'Internet explorées par Projet Arachnid. Dans le présent rapport, le terme « images détectées » désigne des fichiers qui ont été examinés par un analyste et qui constituent soit des images d'abus pédosexuels, soit des images préjudiciables ou violentes.

La source d'une même image peut être incorporée et visible dans plusieurs sites Web. Étant donné que chaque endroit où l'image d'un enfant est visible constitue une atteinte individuelle au droit de cet enfant à la vie privée et à la dignité, Projet Arachnid considère chaque occurrence comme une détection unique. Une détection peut aussi être vue comme une observation individuelle de l'image en question à un endroit donné du Web.

Images ciblées pour suppression
Il s'agit du nombre d'images détectées qui ont donné lieu à l'envoi d'une demande de suppression à un FSÉ. Pour des raisons qui seront expliquées plus loin, les images détectées ne donnent pas toutes lieu à des demandes de suppression.

Demandes de suppression
Une image ciblée pour suppression peut donner lieu à l'envoi d'une ou plusieurs demandes de suppression à un FSÉ. Projet Arachnid renvoie une demande de suppression au FSÉ toutes les 24 heures jusqu'à ce que l'image en question ne soit plus détectée.

Délais de suppression

Le calcul des délais de suppression est basé sur le nombre de jours écoulés entre l'envoi d'une demande de suppression à un FSÉ pour une image donnée à une adresse URL donnée et la date à laquelle Projet Arachnid a détecté la même image à la même adresse pour la dernière fois. Étant donné que le système revérifie l'accessibilité des images signalées toutes les 24 heures après l'envoi d'une demande de suppression, la durée d'accessibilité des liens aux images est précise à 24 heures près. Lorsque l'URL d'une image devient inactive moins de 24 heures après l'envoi d'une demande de suppression, le délai de suppression est arrondi au jour près pour les besoins de notre analyse.

Il est bon de noter qu'une image peut devenir inaccessible pour diverses raisons qui n'ont pas nécessairement rapport avec l'intervention du FSÉ ciblé ou la demande de suppression qui lui a été adressée par Projet Arachnid.

Compte tenu de la gravité du préjudice causé aux victimes par l'exposition publique ne serait-ce que d'une seule photo ou vidéo, nous insisterons ici sur les délais de suppression pour le 90^{e} percentile. Cette mesure correspond à la durée maximale pendant laquelle la majorité (90 %) des adresses URL sont restées actives sur Internet à partir du moment où elles ont donné lieu à l'envoi d'une demande de suppression à un FSÉ.

Récidive d'images

Il s'agit du nombre de fois qu'une photo ou une vidéo qui avait été supprimée suite à l'envoi d'une demande de suppression par Projet Arachnid est détectée de nouveau à une date ultérieure chez le même FSÉ, mais à une adresse URL différente. Dans ce rapport, il y a récidive d'une image lorsque réapparaît une empreinte numérique SHA-1 identique à celle de l'image supprimée. Le SHA-1 est une fonction de hachage cryptographique permettant d'associer à une image une empreinte numérique unique qui la distingue des autres images. Une correspondance SHA-1 implique une correspondance cryptographique exacte; deux images quasi identiques ou deux variantes de la même image ne seraient pas considérées ici comme des correspondances.

Photo de mannequin. Pour illustrer le texte.

Pour donner un sens aux taux de récidive d'images présentés ici, il faut savoir qu'une détection ne sera considérée comme une récidive que si le CCPE avait initialement déterminé que l'image en question était une image d'abus pédosexuels ou une image préjudiciable ou violente. Cette détermination initiale est basée entre autres sur la présence ou non de l'image ou de son empreinte numérique dans les bases de données d'images d'abus pédosexuels connues utilisées par Projet Arachnid ainsi que sur une évaluation visuelle indépendante du développement physique et des signes de maturation sexuelle du ou des sujets figurant sur l'image. Elle tient compte aussi d'indicateurs visibles de l'endroit où l'image a pu être prise et du contexte dans lequel elle a été détectée.

Pour un FSÉ qui déciderait de ne pas supprimer une image à la demande du CCPE, la réapparition de cette image ne serait pas considérée comme une récidive du point de vue dudit FSÉ.

Limites

Nous tenons à apporter les précisions suivantes pour situer les conclusions du présent rapport dans le bon contexte.

1. Il est probable que, dans la quasi-totalité des cas, les données propres aux FSÉ dans ce rapport sous-estiment le nombre réel d'images d'abus pédosexuels et d'images préjudiciables ou violentes qui pourraient être associées à tel ou tel FSÉ. La présence d'une photo ou d'une vidéo sur Internet nécessite l'intervention de plusieurs fournisseurs de services ayant chacun un rôle particulier.

   Or, le Projet Arachnid dans sa forme actuelle est conçu pour adresser la demande de suppression au FSÉ le plus susceptible d'y donner suite, de sorte que les données propres aux FSÉ ne se rapportent ici qu'à un seul acteur de la chaîne pour une image donnée. Dans ses prochains rapports, le CCPE veut élargir son approche afin de dresser un portrait plus complet du rôle des FSÉ dans la diffusion des images d'abus pédosexuels et des images préjudiciables ou violentes.

2. Les données recueillies pour un FSÉ donné correspondent uniquement à ce que Projet Arachnid a pu relever à un moment précis, sur la base des signalements reçus du public ou des priorités d'exploration. Elles ne reflètent pas nécessairement la totalité des images d'abus pédosexuels publiquement accessibles sur les serveurs d'un FSÉ. Le nombre d'images détectées ou la tendance des détections dans le temps pour un service donné ne sont pas toujours représentatifs du volume total d'images d'abus pédosexuels ou d'images préjudiciables ou violentes qu'un FSÉ peut héberger.

   Les médias sociaux, services de messagerie et autres plateformes fermées ou semi-fermées sont de ce fait largement hors de portée de Projet Arachnid. En l'occurrence, les données recueillies par Projet Arachnid ne refléteront pas le volume réel d'images d'abus pédosexuels et d'images préjudiciables ou violentes sur les serveurs de ces FSÉ.

3. 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.

4. Les FSÉ ne sont pas des entités juridiques immuables, et il n'est pas toujours évident de déterminer l'opérateur d'un service donné. Les FSÉ peuvent évoluer, fusionner, se scinder et se repositionner au fil du temps. Les données sur les plateformes de sociétés affiliées ne sont pas nécessairement combinées.

ANALYSE

Durant les trois années de la période étudiée (2018-2020), Projet Arachnid a détecté par ses activités d'exploration plus de 5,4 millions d'images d'abus pédosexuels et d'images préjudiciables ou violentes vérifiées (**Tableau 1.1**). Ces images ont été détectées sur les serveurs de plus de 760 fournisseurs de services électroniques à travers le monde.

Le **Tableau 1.2** montre que les analystes du CCPE et leurs collaborateurs d'autres centrales de signalement ailleurs dans le monde ont examiné collectivement plus de 4,9 millions d'images uniques dans les trois années de la période étudiée. Ce travail alimente une banque grandissante d'empreintes numériques utilisées pour améliorer la qualité des détections futures.

Au moment de la rédaction du présent rapport, le CCPE accuse un arriéré de plus de 32,8 millions d'images suspectes à examiner (**Tableau 1.2**). En effet, le rythme auquel Projet Arachnid détecte les images suspectes dépasse de loin les ressources humaines disponibles pour les examiner.

Pour ces trois années, 626 110 images ont été détectées et ciblées pour suppression par Projet Arachnid (**Tableau 1.1**). Trois facteurs expliquent l'écart important qui sépare le nombre d'images détectées 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 plusieurs 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.

Tableau 1.1

Projet Arachnid : Les grands chiffres

	2018	2019	2020	Total
Détections d'images vérifiées	1 411 203	2 494 316	1 511 194	**5 416 713**
Images vérifiées ciblées pour suppression	57 685	301 990	266 435	**626 110**
Demandes de suppression envoyées	502 162	1 699 017	1 633 698	**3 834 877**

Le terme « image vérifiée » désigne une image qu'un analyste, après examen, considère comme étant soit une image d'abus pédosexuels, soit une image préjudiciable ou violente.

Tableau 1.2

Images suspectes et arriéré d'images à examiner

	Total
Nombre total d'images suspectes détectées	**37 854 878**
Images à examiner	**32 899 122**
Images examinées	**4 955 756**

Le terme « image suspecte » réfère à toute image dont on peut raisonnablement penser qu'elle constitue une image d'abus pédosexuels, mais qui n'a pas encore été soumise au processus d'examen du CCPE.

Détections d'images vérifiées

Sur les 5,4 millions d'images vérifiées que Projet Arachnid a détectées durant les trois années de la période étudiée, 2,9 % (n=158 950) étaient hébergées directement sur des services en .onion du réseau Tor (un sous-ensemble du Web clandestin); le reste (5,2 millions d'images) était hébergé directement sur le Web visible (**Tableau 2.1**). Pour les trois années de la période étudiée, le nombre moyen de photos et de vidéos détectées chaque jour se chiffre à près de 5 300.

Comme le montre la **Figure 1.1**, le nombre de détections dans le temps ne montre aucune tendance particulière. Le robot d'exploration de Projet Arachnid n'est pas réglé sur un ensemble prédéterminé de sites Web. Il explore plutôt certaines parties du Web en fonction de renvois par hyperliens, de signalements venant du public et de nombreux autres facteurs. Il est bon de préciser que, par leur nature même, les sites et les services qui distribuent des images d'abus pédosexuels ont parfois une durée de vie limitée ou doivent souvent changer d'hébergeur avant d'en trouver un qui tolérera ce genre de contenu.

Dans bien des cas, un même réseau de sites peut donner lieu à un nombre formidablement élevé de détections et soudainement disparaître à cause des pressions exercées par Projet Arachnid ou pour d'autres raisons, entraînant du même coup une chute abrupte des détections. D'où les variations importantes du nombre de détections et, plus généralement, de l'activité de Projet Arachnid d'une période à l'autre.

Tableau 2.1

Détections d'images vérifiées, par partie du Web

Partie du Web	2018	2019	2020	Total
Web visible	1 358 109	2 437 230	1 462 424	**5 257 763**
Tor	53 094	57 086	48 770	**158 950**

Le terme « Tor » fait référence au plus grand réseau du Web clandestin.

Figure 1.1

Détections d'images vérifiées, par partie du Web

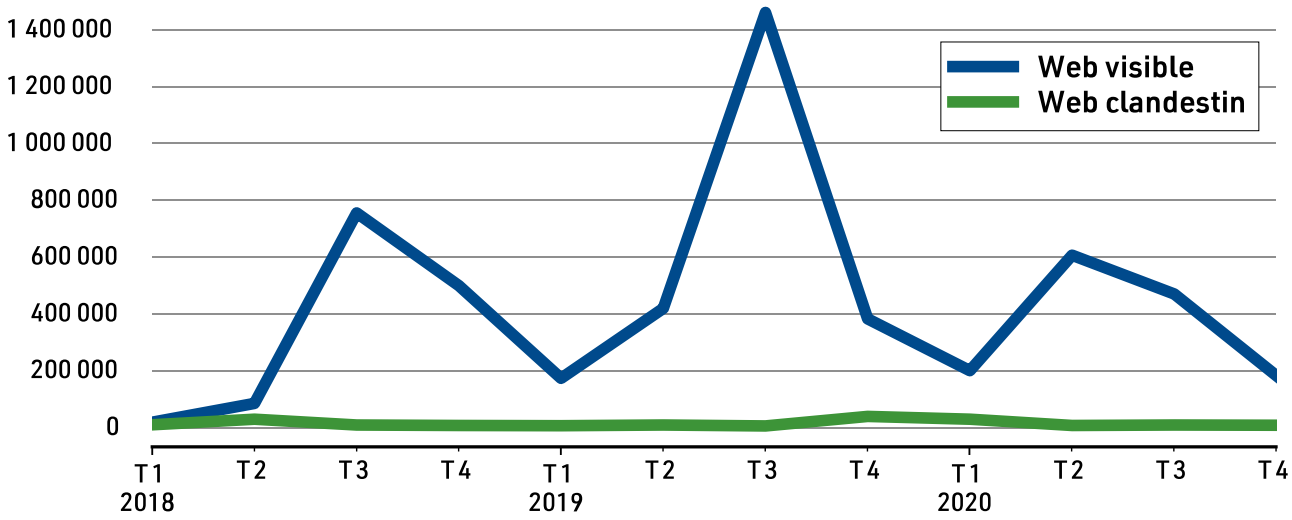


Photo de mannequin. Pour illustrer le texte.

Le **Tableau 2.2** montre que, dans les trois années de la période étudiée, les deux catégories d'images les plus fréquemment rencontrées par Projet Arachnid ont été les images d'enfants prépubères (n=3 403 748) et les images préjudiciables ou violentes (n=1 892 792).

Les images d'enfants post-pubères ne représentent qu'une petite fraction de l'ensemble des images vérifiées que Projet Arachnid a détectées (n=120 173).

Tableau 2.2

Détections d'images vérifiées, par catégorie d'images

Description	2018	2019	2020	Total
Images d'enfants prépubères	738 378	1 792 639	872 731	**3 403 748**
Images d'enfants post-pubères	27 996	51 432	40 745	**120 173**
Images préjudiciables ou violentes	644 829	650 245	597 718	**1 892 792**

La somme des totaux ne correspond pas forcément aux totaux du tableau 2.1, les images recatégorisées ayant été exclues.

Analyse

L'ampleur de l'accessibilité des images d'abus pédosexuels et des images préjudiciables ou violentes constatée par Projet Arachnid se mesure à la base par le nombre d'images détectées.

Comme nous l'avons mentionné précédemment, Projet Arachnid n'explore pas l'entièreté d'Internet. Inévitablement, donc, les chiffres présentés sous-estiment grossièrement l'accessibilité véritable de ces images sur Internet. En fait foi le grand nombre d'images (généralement hors de portée de Projet Arachnid) que les grandes plateformes technologiques signalent au NCMEC pour se conformer à leurs obligations.

Le Tableau 2.2 montre que la grande majorité des images d'abus pédosexuels vérifiées ne sont pas des images d'enfants post-pubères. Ce résultat ne correspond toutefois pas à la réalité en ce qui concerne les images d'adolescent.e.s sur Internet.

Les images de victimes plus jeunes ont toujours été et sont toujours traitées en priorité dans la plupart des interventions. Du point de vue des forces policières ou de la catégorisation des images, il est beaucoup plus facile de déterminer que des images d'abus pédosexuels répondent à une définition pénale lorsque les enfants qui y figurent sont en bas âge ou à l'état prépubère.

En revanche, lorsque les victimes sont à l'état post-pubère, les décisions de catégorisation comportent souvent beaucoup d'incertitudes. La nécessité d'obtenir des informations contextuelles supplémentaires sur ces images pour en arriver à une décision finale augmentera invariablement la complexité de la tâche et mobilisera plus de ressources. Par exemple, comment savoir, en se basant seulement sur des repères visuels, si une victime adolescente présentant tous les signes d'une maturité sexuelle complète est une personne mineure ou une personne adulte?

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 d'un pays à l'autre ont fini par induire un biais en faveur des victimes plus jeunes.

Par exemple, la Base de données internationale sur l'exploitation sexuelle des enfants (ICSE), un outil de renseignement géré par Interpol, a établi la catégorie Baseline. Il s'agit d'une catégorie générique dans laquelle sont classées les images qui seraient jugées illégales dans pratiquement tous les pays. Elle est présentée comme étant « une norme internationale permettant d'isoler les pires images d'abus pédosexuels ».

Selon un rapport d'Interpol et d'ECPAT (End Child Prostitution and Trafficking)[5] paru en 2018, les critères de la liste Baseline sont :

- que l'enfant sur l'image soit un vrai enfant (pas d'images créées artificiellement);
- qu'il s'agisse d'un enfant prépubère (il ne doit présenter aucun signe de puberté ou seulement les tout premiers signes et sembler âgé de moins de 12 ou 13 ans);
- que l'enfant soit impliqué dans une activité sexuelle ou un abus sexuel ou en soit témoin;
- que l'image mette en évidence les organes génitaux ou la région anale de l'enfant.

Il découle de cette réalité que les banques d'empreintes numériques d'images d'abus pédosexuels connues comportent un biais favorable aux victimes plus jeunes et aux images les plus extrêmes. Étant donné que la plupart des systèmes de détection d'images (y compris Projet Arachnid) utilisent ces banques d'empreintes numériques, les images découvertes par ces processus automatisés reflètent ce biais en faveur des images extrêmes de victimes plus jeunes.

5 INTERPOL (2018). *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: Technical Report.* https://www.ecpat.org/wp-content/uploads/2018/02/Technical-Report-TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL.pdf

À cela s'ajoute cela le fait que les victimes post-pubères sont souvent habitées par des sentiments de honte ou de peur vis-à-vis de la création, de la distribution et de l'exposition publique d'images des abus qu'ils ont subis ou de leurs moments de vulnérabilité. Au CCPE, les analystes de Cyberaide.ca rapportent que ces victimes, lorsqu'elles demandent de l'aide, veulent souvent éviter le déclenchement d'une intervention policière ou judiciaire parce qu'elles ont toujours peur de la personne qui a créé les images et qu'elles veulent éviter d'attirer davantage l'attention sur elles-mêmes.

Il ne fait donc aucun doute que les victimes adolescentes sont largement sous-représentées dans les images détectées par Projet Arachnid.

Le Web clandestin et la distribution des images d'abus pédosexuels

À la vue des détections effectuées par Projet Arachnid (**Tableau 2.2**), on constate que le nombre d'images hébergées directement sur le réseau Tor ou accessibles par celui-ci est relativement peu élevé par rapport au nombre d'images détectées sur le Web visible. Sans plus de détails, on pourrait conclure que le Web clandestin joue un rôle limité dans la distribution des images d'abus pédosexuels alors que c'est tout le contraire.

Plutôt que d'héberger des images d'abus pédosexuels et des images préjudiciables ou violentes, les réseaux du Web clandestin (comme Tor) servent souvent de véhicule pour diriger les internautes vers des endroits où trouver de telles images sur le Web visible. Des communautés entières, fortes de l'anonymat que leur procure le réseau Tor, se rassemblent dans des forums où leurs membres s'échangent des informations concernant les images d'abus pédosexuels et d'autres activités clandestines. On y discute souvent des endroits où trouver des images illégales et des moyens d'y accéder, de tutoriels et de manuels sur le conditionnement d'enfants et les abus pédosexuels, de chiffrement, de cybersécurité et de stratégies de destruction de preuves.

Il est important que les régulateurs et les FSÉ qui veulent appliquer des mesures proactives saisissent bien ce principe de vases communiquants entre le Web visible et le Web clandestin.

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 aux 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 deviennent 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.

Les distributeurs opteront souvent pour des services d'hébergement gratuits qui ne collectent guère de données sur leurs utilisateurs. Ils y déposeront des fichiers d'archive (chiffrés et protégés par mot de passe) pouvant contenir 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.

C'est ainsi que sont distribuées la majeure partie des images vérifiées que Projet Arachnid détecte. Comme nous l'avons souligné plus tôt, le champ d'action de Projet Arachnid sur le Web clandestin se limite au réseau Tor; sur les autres réseaux du Web clandestin, les modes de distribution peuvent différer.

Photo de mannequin. Pour illustrer le texte.

Images ciblées pour suppression

Durant les trois années de la période étudiée, Projet Arachnid a envoyé en moyenne 571 demandes de suppression de photos et de vidéos par jour. La forte augmentation du nombre d'images ciblées pour suppression à la fin de 2019 se rapporte à un service gratuit — ImageVenue.com — que des centaines de sites tiers utilisaient alors pour héberger des images d'abus pédosexuels.

Les noms de domaine de ces sites comportaient souvent des mots anglais associés à l'exploitation sexuelle des enfants, comme *teen*, *cuties* et *jailbait*. La découverte et l'exploration de ce groupe de sites par Projet Arachnid a entraîné une montée subite des détections liées à ImageVenue.com, le service où les images étaient hébergées.

Comme nous l'avons indiqué précédemment, le nombre d'images ciblées pour suppression par Projet Arachnid (**Tableau 3.1**) ne correspond pas au nombre réel d'images en circulation dans les faits puisqu'un même fichier d'archive en contient parfois des centaines.

Les données présentées dans le **Tableau 3.2** se rapportent aux FSÉ accusant au moins 5 000 images ou fichiers ayant donné lieu à 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 3.2**.

Les données de Projet Arachnid pour la période étudiée ici montrent que Free, qui administre le site d'hébergement de fichiers dl.free.fr, a hébergé au moins 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. Projet Arachnid a relevé un peu partout sur Internet des points d'accès à ces fichiers d'archive, portant à plus de 2,7 millions le nombre d'images détectées. On trouvera plus loin une étude de cas consacrée spécifiquement à Free.fr (voir p. 42).

Photo de mannequin. Pour illustrer le texte.

La grande majorité des FSÉ qui ont reçu des demandes de suppression venant de Projet Arachnid sont des fournisseurs d'hébergement d'images ou des services d'hébergement de fichiers. Comme on peut le voir au **Tableau 3.2**, les FSÉ suivants mobilisent le plus grand nombre d'images ciblées pour suppression :

- **ImageVenue.com :** Ce nom de domaine basé en République tchèque selon les coordonnées du titulaire exploite un service d'hébergement d'images, mais utilise les services d'hébergeurs externes pour accueillir des contenus générés par les utilisateurs (n=144 000).
- **Serverel :** Une société américaine qui offre un service d'hébergement sur ses propres serveurs (n=72 412).
- **CloudFlare :** Une société américaine qui offre des réseaux de diffusion de contenu (CDN) liés à plusieurs autres FSÉ bien connus du Projet Arachnid (n=49 183).
- **Incrediserve LTD :** Une société néerlandaise qui fournit des services d'hébergement (n=39 400).
- **Trichan :** Un réseau aujourd'hui disparu de forums apparemment centralisés qui permettait à ses utilisateurs d'héberger des images directement sur son site Web. Parmi les entreprises qui fournissaient des services d'hébergement à Trichan, plusieurs se retrouvent dans les relevés d'exploration de Projet Arachnid. Les chiffres indiqués dans le **Tableau 3.2** (n=34 157) sous-estiment largement le volume réel d'images offert sur ces forums au motif que l'absence chronique de réponse aux demandes de suppression a forcé l'adoption d'une nouvelle stratégie de suppression qui s'est répercutée sur la gestion des données.
- **NFOrce Entertainment B.V. :** Une société néerlandaise qui offre un service d'hébergement sur ses propres serveurs (n=23 211).

Le **Tableau 3.3** montre que, chez presque tous les FSÉ étudiés ici, la majeure partie des images signalées par Projet Arachnid sont des images d'enfants prépubères. La seule exception, comme le montre le **Tableau 3.4**, est Serverel, qui a surtout reçu des demandes de suppression pour des images d'enfants post-pubères (n=66 824).

Après analyse des demandes de suppression adressées à Serverel, il semblerait que cette irrégularité puisse s'expliquer par le fait que les sites Web qui utilisent les services de Serverel sont souvent des sites pornographiques éphémères qui hébergent des images d'enfants post-pubères avec de la pornographie adulte légale. Projet Arachnid a détecté ces images sur au moins 1 200 sites uniques qui utilisent les services d'hébergement de Serverel.

Tableau 3.1

Images ciblées pour suppression			
2018	2019	2020	Total
57 685	301 990	266 435	**626 110**

Les fichiers d'archive contenant plusieurs images sont enregistrés comme une seule et même entrée dans le tableau.

Tableau 3.2

Images ciblées pour suppression, par FSÉ *(Comprend uniquement les FSÉ accusant un minimum de 5 000 détections d'images ciblées pour suppression)*

Nom du FSÉ	Type de service	2018	2019	2020	Total
ImageVenue	Administrateur de contenu	6 214	76 579	61 099	**143 892**
Serverel	Hébergeur	826	9 121	62 465	**72 412**
CloudFlare	Réseau de diffusion de contenu	3 117	36 604	9 462	**49 183**
Incrediserve LTD	Hébergeur	15 861	19 353	4 186	**39 400**
Trichan	Administrateur de contenu	7 092	27 065	0	**34 157**
NFOrce Entertainment B.V.	Hébergeur	789	14 481	7 941	**23 211**
ImgOutlet.com	Administrateur de contenu	0	10 182	8 400	**18 582**
ImgView.net	Administrateur de contenu	96	6 509	4 035	**10 640**
FranTech Solutions	Hébergeur	54	688	8 987	**9 729**
ImgDew.com	Administrateur de contenu	0	5 618	3 574	**9 192**
Host Sailor	Hébergeur	117	6 845	1 778	**8 740**
ColoCrossing	Hébergeur	1 369	5 309	1 131	**7 809**
ALFA TELECOM s.r.o.	Hébergeur	501	6 909	62	**7 472**
DataWeb Global Group B.V.	Hébergeur	598	2 740	3 765	**7 103**
ImgMaze.com	Administrateur de contenu	0	4 541	2 300	**6 841**
Liteserver Holding B.V.	Hébergeur	2	4 125	2 639	**6 766**
ImageBam	Administrateur de contenu	42	2 363	3 934	**6 339**
OVHcloud	Hébergeur	3 104	1 873	1 304	**6 281**

Les données concernant le FSÉ Free ne figurent pas dans ce tableau.

Voir l'étude de cas en page 42 pour plus de détails.

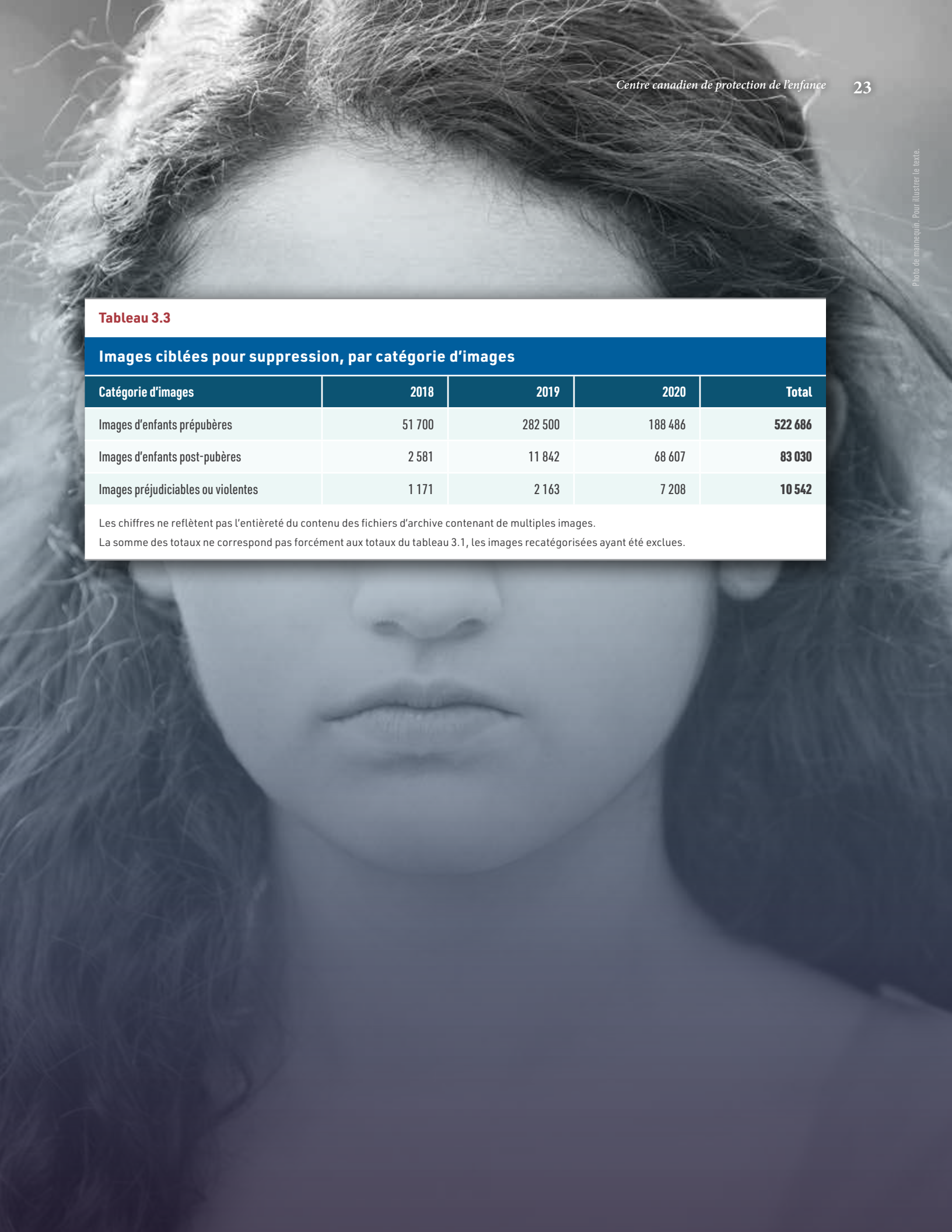


Photo de mannequin. Pour illustrer le texte.

Tableau 3.3

Images ciblées pour suppression, par catégorie d'images

Catégorie d'images	2018	2019	2020	Total
Images d'enfants prépubères	51 700	282 500	188 486	**522 686**
Images d'enfants post-pubères	2 581	11 842	68 607	**83 030**
Images préjudiciables ou violentes	1 171	2 163	7 208	**10 542**

Les chiffres ne reflètent pas l'entièreté du contenu des fichiers d'archive contenant de multiples images.

La somme des totaux ne correspond pas forcément aux totaux du tableau 3.1, les images recatégorisées ayant été exclues.

Tableau 3.4

Images ciblées pour suppression, par catégorie d'images et par FSÉ
(Comprend uniquement les FSÉ accusant un minimum de 5 000 détections d'images ciblées pour suppression)

Nom du FSÉ	Images d'enfants prépubères	Images d'enfants post-pubères	Images préjudiciables ou violentes
ImageVenue	142 449	236	550
CloudFlare	46 033	1273	446
Increditserve LTD	37 589	118	779
Trichan	32 215	49	624
NFOrce Entertainment B.V.	23 066	66	58
ImgOutlet.com	18 534	15	28
ImgView.net	10 549	30	32
ImgDew.com	9 139	22	28
Host Sailor	8 689	11	22
FranTech Solutions	7 893	24	1 753
ColoCrossing	7 573	7	57
ALFA TELECOM s.r.o.	7 406	51	13
ImgMaze.com	6 782	33	24
Liteserver Holding B.V.	6 748	0	17
ImageBam	6 189	10	105
OVHcloud	5 543	383	126
Serverel	4 529	66 824	3
DataWeb Global Group B.V.	2 583	4 151	25

Les données concernant le FSÉ Free ne figurent pas dans ce tableau.

Voir l'étude de cas en page 42 pour plus de détails.

Demandes de suppression

Dans les trois années de la période étudiée, Projet Arachnid a envoyé près de 3 500 demandes de suppression par jour. Le **Tableau 4.1** montre que, pour les trois années de la période étudiée, le nombre de demandes de suppression adressées aux FSÉ se chiffre à plus de 3,8 millions.

Projet Arachnid continue d'envoyer des demandes de suppression toutes les 24 heures jusqu'à ce que les images en cause ne soient plus détectées à l'adresse URL ciblée. De ce fait, le nombre de demandes de suppression adressées à un FSÉ est directement corrélé à la fois au nombre de photos et de vidéos ciblées pour suppression et à la durée pendant laquelle ces images sont accessibles.

La forte augmentation du nombre de demandes de suppression au début de 2019 est liée à une action concertée pour forcer la suppression de milliers d'images sur un réseau aujourd'hui disparu de forums en ligne consacrés à l'exploitation des enfants et connu sous le nom de Trichan. Cette initiative fait l'objet d'une étude de cas plus loin dans ce rapport (p. 44).

Le **Tableau 4.2** indique le nombre de demandes de suppressions envoyées par Projet Arachnid pour chaque catégorie d'images; les images d'enfants prépubères (n=2 986 280) cumulent le plus grand nombre de demandes. Toutefois, le nombre de demandes de suppression pour des images d'enfants post-pubères (n=737 718) est nettement plus élevé que ce à quoi on pourrait s'attendre compte tenu du nombre comparativement peu élevé de détections indiqué au **Tableau 2.2**. Il faut en déduire que les images d'enfants post-pubères génèrent beaucoup plus de demandes de suppression et, par conséquent, restent en ligne plus longtemps avant de devenir inaccessibles.

Le **Tableau 4.2** montre que les demandes de suppression pour des images catégorisées préjudiciables ou violentes ont fortement augmenté en 2020 (n=88 825). Cette augmentation coïncide avec la publication du Cadre du CCPE pour la protection et les droits de l'enfant (voir p. 9), qui a fait en sorte d'élargir les types d'images donnant lieu à des demandes de suppression.

Tableau 4.1

Demandes de suppression envoyées

2018	2019	2020	Total
502 162	1 699 017	1 633 698	**3 834 877**

Les chiffres font état des demandes de suppression initiales et subséquentes adressées aux FSÉ.

Tableau 4.2

Demandes de suppression envoyées, par catégorie d'images

Catégorie d'images	2018	2019	2020	Total
Images d'enfants prépubères	482 399	1 633 212	870 669	**2 986 280**
Images d'enfants post-pubères	9 934	40 000	687 784	**737 718**
Images préjudiciables ou violentes	6 589	12 512	69 724	**88 825**

La somme des totaux ne correspond pas forcément aux totaux du tableau 4.1 les images recatégorisées ayant été exclues.

Tableau 4.3

Demandes de suppression envoyées, par catégorie d'images et par FSÉ

(Comprend uniquement les FSÉ accusant un minimum de 5 000 détections d'images ciblées pour suppression)

Nom du FSÉ	Images d'enfants prépubères	Images d'enfants post-pubères	Images préjudiciables ou violentes
Trichan	733 927	776	7704
Increditserve LTD	381 498	641	4 696
NFOrce Entertainment B.V.	217 068	1 623	525
CloudFlare	170 923	9 646	1 158
ImageVenue	168 448	291	645
ColoCrossing	165 709	170	1 249
FranTech Solutions	94 707	877	15 047
Liteserver Holding B.V.	52 189	0	88
Serverel	44 662	637 631	3
ImgOutlet.com	34 830	34	41
OVHcloud	31 245	2 818	305
Host Sailor	24 768	42	23
ImgView.net	23 693	63	54
ImgDew.com	21 535	41	70
ALFA TELECOM s.r.o.	17 142	133	149
ImgMaze.com	16 257	65	61
ImageBam	6 565	10	105
DataWeb Global Group B.V.	3 778	11 017	26

Les données concernant le FSÉ Free ne figurent pas dans ce tableau.

Voir l'étude de cas en page 42 pour plus de détails.

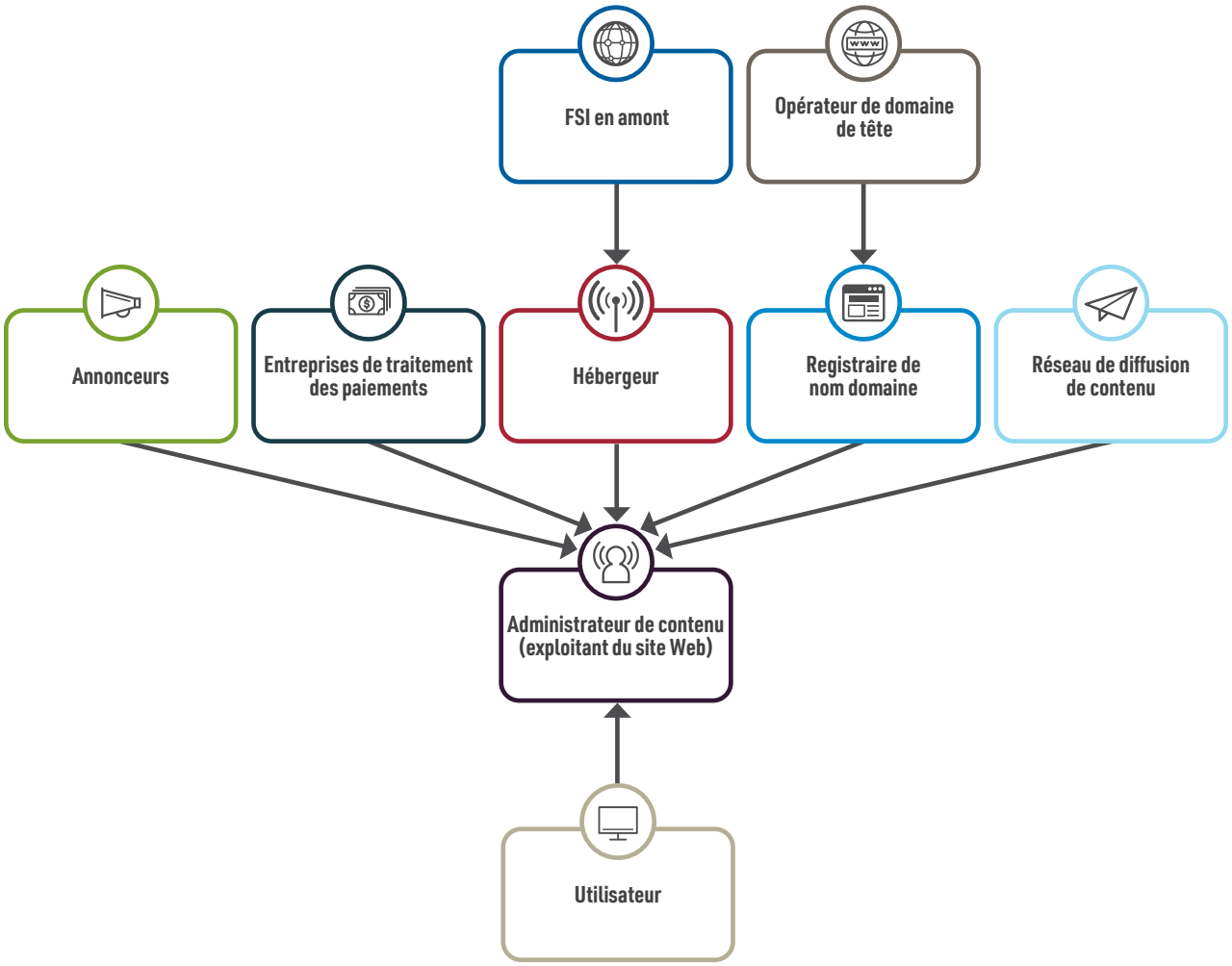
Analyse

Bien que ce rapport établisse des recoupements entre certains FSÉ et l'accessibilité des images d'abus pédosexuels et d'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.

Les demandes de suppression envoyées par Projet Arachnid ciblent généralement un FSÉ précis sur la base 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 présent rapport se rapportent aux entités 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.

Figure 2.0



Pour mettre les choses en perspective, passons en revue la démarche qu'une personne doit généralement suivre pour mettre en ligne un site voué à la sexualisation des enfants :

1. La personne doit d'abord enregistrer un nom de domaine auprès d'un registraire de nom domaine. Ce dernier est autorisé par l'opérateur de domaine de tête à vendre des noms de domaines.
2. Après avoir enregistré un nom de domaine, la personne doit trouver un moyen de mettre son contenu en ligne et de le rendre accessible. Pour ce faire, elle retiendra les services d'un hébergeur. Certains hébergeurs possèdent ou louent des serveurs, d'autres louent de l'espace sur les serveurs d'autres sociétés, qui se répartissent parfois dans plusieurs pays. Ces FSÉ disposent généralement des moyens techniques et/ou légaux voulus pour fermer un site ou un serveur qui utilise leurs services; ils peuvent aussi imposer à leurs clients des conditions générales d'utilisation précises et légalement contraignantes.
3. La personne peut faire appel à un service de réseau de diffusion de contenu (CDN). Ce service permet d'accélérer l'accès au contenu d'un site en le copiant sur des serveurs répartis à différents endroits du globe de manière à réduire la distance que les données doivent parcourir. Du point de vue de la distribution d'images d'abus pédosexuels et d'images préjudiciables ou violentes, les réseaux CDN sont intéressants, car ils masquent habituellement l'identité de l'administrateur du site et des hébergeurs.
4. La personne peut aussi faire appel à un service de réseau privé virtuel (VPN) pour masquer son adresse IP d'origine à son hébergeur dans le cours de ses activités.
5. Pour monétiser le tout, la personne peut en outre faire appel à des services de paiement (dont les grands émetteurs de cartes de crédit) ou à d'autres systèmes de paiement en ligne. Elle peut aussi faire la promotion de son contenu afin d'en tirer des revenus publicitaires.

Les fournisseurs de services Internet en amont et les réseaux de niveau 1 forment l'épine dorsale du réseau Internet et ont la mainmise sur l'ensemble de l'écosystème numérique décrit précédemment. Même les plus grandes entreprises de technologie dépendent de ces entreprises pour rendre leurs plateformes accessibles à leurs utilisateurs dans le monde entier.

Photo de mannequin. Pour illustrer le texte.

Pics de détection d'images ciblées pour certains FSÉ

À la vue des données présentées ici, on constate que les interventions de Projet Arachnid auprès de certains FSÉ provoquent parfois des pics de détections. Comme nous l'avons indiqué précédemment, le nombre de détections fluctue, parfois de façon spectaculaire, selon le moment. Il est important de noter que le nombre de demandes de suppression qu'un hébergeur peut recevoir dépend souvent de la nature des activités de ses clients (c.-à-d., les administrateurs de contenu).

Le **Tableau 4.3** montre que deux FSÉ en particulier — ImageVenue.com et Serverel — ont reçu un grand nombre de demandes de suppression de la part de Projet Arachnid en 2019 et 2020. Ces pics de demandes sont dus en grande partie au fait que des réseaux de sites tiers distribuaient largement les images hébergées sur leurs serveurs.

Cette utilisation détournée des services d'hébergement de fichiers par des acteurs tiers illustre combien il est important que ces services fassent preuve de vigilance et mettent en place des outils pour bloquer la mise en ligne de contenus indésirables et se dotent de ressources de modération humaine suffisantes.

Le fait qu'un FSÉ accepte des contenus générés par ses utilisateurs et permette d'y accéder par l'entremise du Web clandestin peut aussi avoir un impact sur le nombre d'images détectées par Projet Arachnid chez ce FSÉ.

Certains FSÉ — dont quelques-uns sont mis en relief dans ce rapport — permettent à des utilisateurs anonymes de mettre des images en ligne sur leurs plateformes et d'y accéder depuis le réseau Tor. Lorsqu'un FSÉ omet de mettre en place des mesures de sécurité réseau pour bloquer ce genre de trafic suspect, les utilisateurs ont beau jeu d'utiliser son infrastructure pour distribuer des images d'abus pédosexuels, surtout s'ils n'ont pas de compte à ouvrir ou de frais à payer.

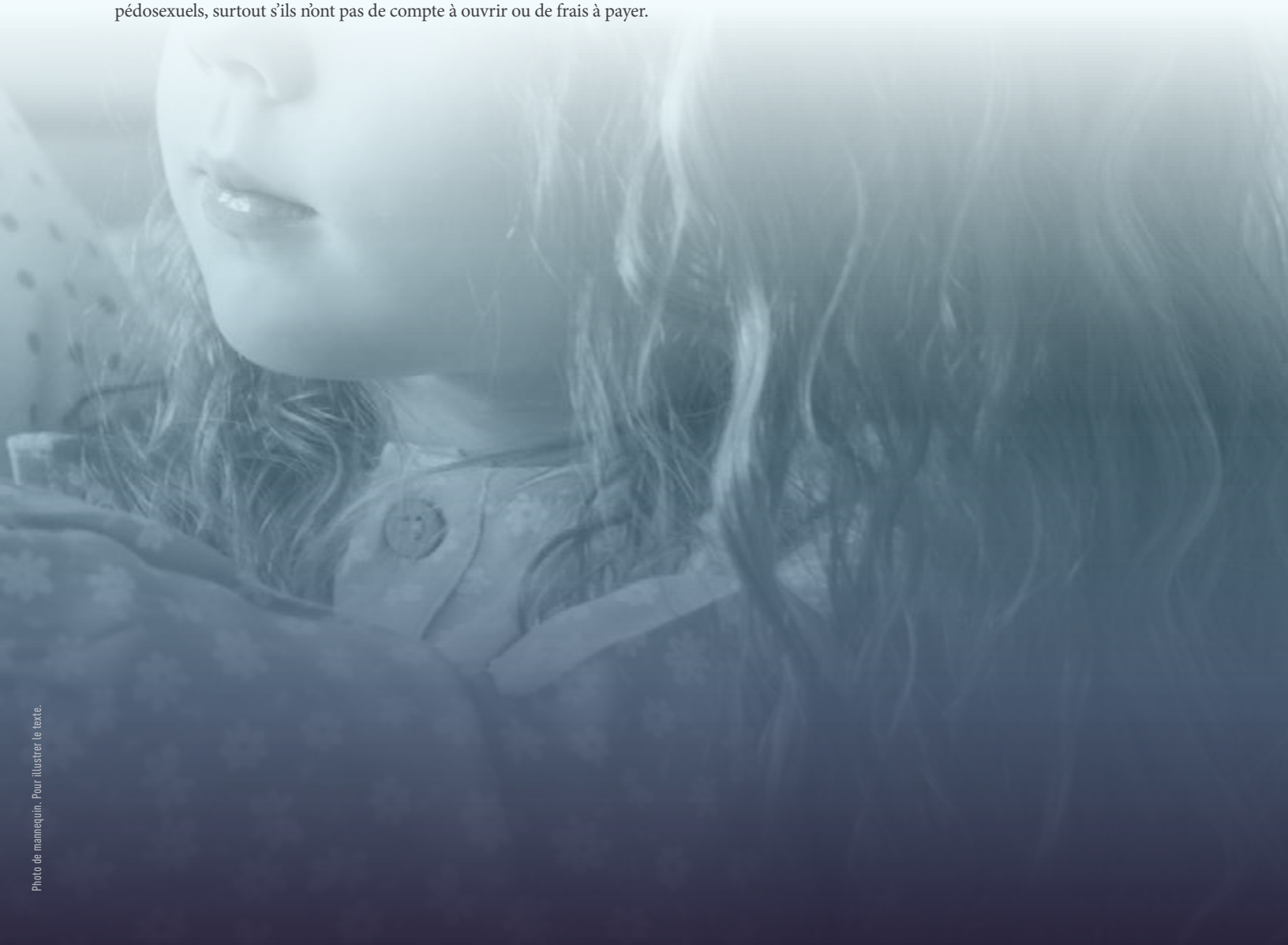


Photo de mannequin. Pour illustrer le texte.

Emplacement des serveurs des images ciblées pour suppression

La distribution des images d'abus pédosexuels et des images préjudiciables ou violentes est un problème mondial. La décentralisation des services Internet permet aux FSÉ d'avoir une présence physique et numérique à de nombreux endroits.

Pour déterminer l'emplacement des serveurs, Projet Arachnid utilise les données compilées par Maxmind inc., qui fait état d'un taux de précision de 99,8 % au niveau du pays[6].

Le **Tableau 5.1** montre que, dans les trois années de la période étudiée, Projet Arachnid a adressé près de 49 % de ses demandes de suppression à des FSÉ qui hébergeaient les images en question sur des serveurs situés aux Pays-Bas. Les États-Unis viennent au second rang (33 %), suivis du Canada (4,7 %).

Le **Tableau 5.2** présente, pour chaque pays, les trois FSÉ qui ont reçu le plus grand nombre de demandes de suppression. Certains de ces FSÉ utilisent leurs propres serveurs, d'autres louent de l'espace sur les serveurs d'autres entreprises.

Tableau 5.1

Demandes de suppression envoyées, selon l'emplacement du serveur hébergeur (15 premiers pays)

Géolocalisation (GeoIP)	2018	2019	2020	Total	Pourcentage
Pays-Bas	370 040	1 040 057	468 323	**1 878 420**	48,8 %
États-Unis	54 748	406 420	805 589	**1 266 757**	32,9 %
Canada	15 405	89 059	76 363	**180 827**	4,7 %
Russie	14 204	32 287	51 167	**97 658**	2,5 %
France	15 957	28 021	33 670	**77 648**	2,0 %
Seychelles	5 316	7 797	49 384	**62 497**	1,6 %
Ukraine	10 331	22 834	15 404	**48 569**	1,3 %
Lettonie	2	2 329	43 810	**46 141**	1,2 %
Belize	1 273	28 509	4 796	**34 578**	0,9 %
Hong Kong	0	3 984	21 447	**25 431**	0,7 %
Allemagne	771	4 683	9 890	**15 344**	0,4 %
Royaume-Uni	2 148	2 279	5 606	**10 033**	0,3 %
Afrique du Sud	11	4 126	5 415	**9 552**	0,2 %
Nouvelle-Zélande	332	2 443	5 368	**8 143**	0,2 %
Estonie	91	262	7 569	**7 922**	0,2 %

La géolocalisation des serveurs est basée sur des données fournies par Maxmind inc., un service de renseignement Internet.
Les pourcentages sont calculés sur l'ensemble des pays, y compris ceux qui ne figurent pas dans le tableau.

6 Pour plus d'informations sur le taux de précision de Maxmind inc., on consultera le www.maxmind.com/en/geoip2-country-database.

Tableau 5.2

Demandes de suppression selon l'emplacement du serveur (3 premiers FSÉ de chaque pays)

Pays (GeoIP)	Nom du FSÉ	Demandes de suppression
États-Unis	Serverel	616 911
États-Unis	CloudFlare	183 766
États-Unis	ColoCrossing	167 641
Royaume-Uni	JPG4.NET	3 081
Royaume-Uni	OVHcloud	1 816
Royaume-Uni	Trichan	655
Ukraine	TOV ITT	10 329
Ukraine	PE Brezhnev Daniil	9 130
Ukraine	ALFA TELECOM s.r.o.	5 996
Afrique du Sud	Zappie Host LLC	8 742
Afrique du Sud	Afrihost	810
Seychelles	IP Volume	33 957
Seychelles	Increditserve LTD	26 728
Seychelles	Novogara LTD	1 614
Russie	imgsrc.ru	17 999
Russie	ALFA TELECOM s.r.o.	11 118
Russie	VDSINA Hosting	5 972
Nouvelle-Zélande	Zappie Host LLC	8 047
Nouvelle-Zélande	Spark New Zealand	96
Pays-Bas	Trichan	717 722
Pays-Bas	Increditserve LTD	362 519
Pays-Bas	NFOrce Entertainment B.V.	218 907
Lettonie	Telia Latvija SIA	39 204
Lettonie	FastPic	3 130
Lettonie	Telenet Ltd	1 970
Hong Kong	Amarutu Technology Ltd	21 630
Hong Kong	Tele Asia	3 391
Hong Kong	I-Services Network Solution Limited	257
Allemagne	TerraTransit AG	4 616
Allemagne	Koddos/Amarutu Technology Ltd. 2	2 502
Allemagne	imgsrc.ru	1 970
France	Free.fr	25 551
France	OVHcloud	25 428
France	Dedibox SAS	19 428
Estonie	Xemu	7 124
Estonie	Estro Web Services Private Limited	312
Estonia	GmhostGrupp OU	192
Canada	ImageVenue	169 756
Canada	OVHcloud	6 949
Canada	Gayboystube	2 380
Belize	Trichan	21 603
Belize	TerraTransit AG	12 077
Belize	Koddos/Amarutu Technology Ltd. 2	855

La géolocalisation des serveurs est basée sur des données fournies par Maxmind inc., un service de renseignement Internet.

Ce tableau n'indique pas nécessairement l'emplacement du siège d'un FSÉ; il indique plutôt le lieu physique où se trouvent ses serveurs.

Photo de mannequin. Pour illustrer le texte.

Analyse

L'examen des enjeux juridiques propres à l'espace numérique dépasse le cadre de ce rapport. Il est toutefois utile, d'un point de vue de politique publique, de savoir à quels endroits les images sont physiquement hébergées sur la planète – surtout quand les pays en question soumettent les FSÉ à des obligations de signalement.

L'un des obstacles souvent cités par les autorités judiciaires et policières est l'ambiguïté juridique qui entoure les sociétés Internet et leurs activités.

Le cas très médiatisé de la société MindGeek[MD] et de son site pornographique **Pornhub.com** illustre bien la difficulté de savoir si les lois d'un pays s'appliquent à une organisation.

MindGeek est bien implantée à Montréal, au Canada, où environ 1 000 employés travaillent dans ses bureaux. Et bien que MindGeek ait aussi des bureaux à Chypre, en Angleterre, en Roumanie et aux États-Unis, elle prétend avoir son siège au Luxembourg, où elle est légalement enregistrée[7].

Or, d'après les données de géolocalisation associées aux images détectées par Projet Arachnid, le contenu de Pornhub est principalement hébergé sur des serveurs aux États-Unis.

Dans le cas particulier de MindGeek, des arguments juridiques pourraient être avancés pour la forcer à respecter les lois du Canada, de Chypre, de l'Angleterre, de la Roumanie, des États-Unis et du Luxembourg ou de tous ces pays à la fois. Ce cas de figure montre à quel point il est important que les décideurs politiques définissent clairement les contours des lois se rapportant aux FSÉ. C'est une condition essentielle à la réglementation de l'espace numérique.

---

7 MindGeek (2 juin 2021). MindGeek. https://www.mindgeek.com/
Protection de la vie privée et de la réputation sur les plateformes telles Pornhub, Chambre des communes du Canada, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 43e législature, 2e session, réunion 19 (2021). https://www.noscommunes.ca/DocumentViewer/fr/43-2/ETHI/reunion-19/temoignages

Délais de suppression

On entend par *délai de suppression* le temps écoulé depuis l'envoi d'une demande de suppression jusqu'au moment où l'image en cause cesse d'être accessible. Du point de vue de la victime, ce délai est d'une importance capitale.

Pour donner un sens aux résultats présentés ici, 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.

Le **Tableau 6.1** montre que, dans les trois années de la période étudiée, 50 % des images ciblées n'étaient plus accessibles le jour suivant l'envoi de la demande de suppression. Le délai de suppression est de 24 heures pour le percentile médian (50^{e}), mais il est de 42 jours au-delà du 90^{e} percentile. Il faut comprendre ici que 10 % des images ciblées pour suppression dans les trois années de la période étudiée ont été retirées d'Internet plus de sept semaines après l'envoi de la demande de suppression. Cela pose un problème majeur.

Les délais sensiblement plus longs observés en 2018 (**Tableau 6.1**) seraient attribuables à quelques facteurs. À l'époque, Projet Arachnid n'en était qu'à ses débuts, et l'on ne prenait pas la pleine mesure des nombreux obstacles à la suppression des images d'abus pédosexuels et des stratégies à mettre en place. En outre, une partie des demandes de suppression envoyées par Projet Arachnid transitaient au début par des instances régionales. L'élimination progressive des intermédiaires en 2019 a permis d'améliorer considérablement les choses.

Il convient toutefois de noter que même si les délais de suppression sont grandement réduits depuis 2018, ils se sont récemment allongés au-delà du 90^{e} percentile, passant de 26 jours en 2019 à 38 jours en 2020 (**Tableau 6.1**).

Cette augmentation des délais de suppression s'explique en partie par une augmentation du nombre d'images d'enfants post-pubères ciblées pour suppression en 2020 (**Tableau 3.3**), les délais de suppression étant généralement plus longs pour cette catégorie d'images que pour les images d'enfants prépubères et les images préjudiciables ou violentes (**Tableau 6.2**).

Dans l'ensemble, le délai de suppression (90^{e} percentile) pour les images d'enfants prépubères est de 40 jours, comparativement à 56 jours pour les images d'enfants post-pubères et à 37 jours pour les images préjudiciables ou violentes (Tableau 6.2).

Le **Tableau 6.3** fait état de grandes différences entre les FSÉ au chapitre des délais de suppression. Certains FSÉ hébergent des volumes importants d'images d'abus pédosexuels et ne répondent généralement pas aux demandes de suppression. Trichan répondait rarement aux demandes de suppression, allongeant par le fait même les délais de suppression (90^{e} percentile = 138 jours). Cependant, lorsque ses principaux hébergeurs ont commencé à retirer leurs services, les délais de suppression ont considérablement raccourci puisque les images en cause sont vite devenues inaccessibles.

Le **Tableau 6.3** montre qu'il y a aussi des FSÉ qui réagissent beaucoup plus rapidement aux demandes de suppression. Dans certains cas, cela s'explique par la mise en place d'un mécanisme interne pour automatiser le traitement des demandes de suppression envoyées par Projet Arachnid afin de réduire les délais de suppression.

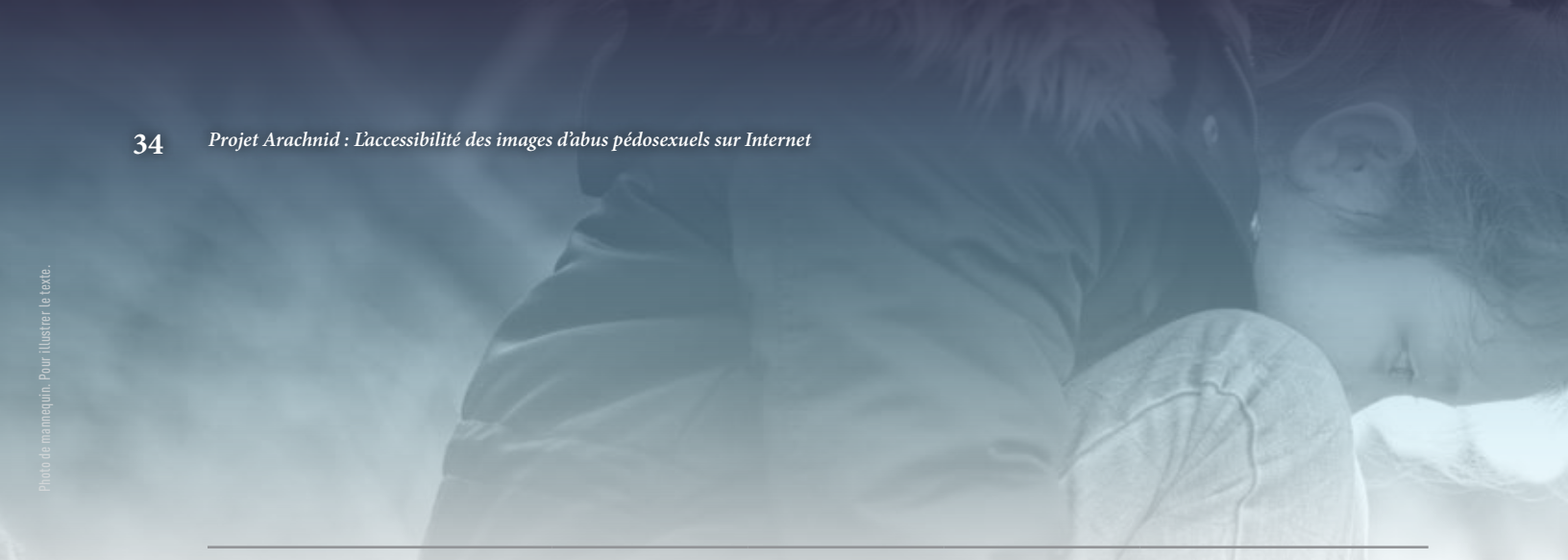


Photo de mannequin. Pour illustrer le texte.

Tableau 6.1

Délais de suppression (toutes les images ciblées pour suppression)

	2018	2019	2020	Toutes années confondues
50e percentile (médiane)	5 jours	1 jour	1 jour	1 jour
90e percentile	161 jours	26 jours	38 jours	42 jours

Durée de maintien en ligne des images durant la période étudiée entre l'envoi d'une demande de suppression et le 31 décembre 2020.
Une image est considérée comme supprimée lorsqu'elle n'est plus accessible à l'adresse URL ciblée.

Tableau 6.2

Délais de suppression, par catégorie d'images

Catégorie d'images	50e (médiane)	90e percentile
Images d'enfants prépubères	1 jour	40 jours
Images d'enfants post-pubères	2 jours	56 jours
Images préjudiciables ou violentes	1 jour	37 jours

Durée de maintien en ligne des images durant la période étudiée entre l'envoi d'une demande de suppression et le 31 décembre 2020.
Une image est considérée comme supprimée lorsqu'elle n'est plus accessible à l'adresse URL ciblée.

Tableau 6.3

Délais de suppression, par FSÉ

Nom du FSÉ	50e (médiane)	90e percentile
Trichan	1 jour	138 jours
ColoCrossing	27 jours	127 jours
NFOrce Entertainment B.V.	8 jours	70 jours
Serverel	6 jours	60 jours
Increditserve LTD	3 jours	53 jours
Liteserver Holding B.V.	1 jour	43 jours
FranTech Solutions	13 jours	40 jours
CloudFlare	1 jour	27 jours
OVHcloud	3 jours	23 jours
Host Sailor	1 jour	15 jours
ImgView.net	2 jours	6 jours
ImgMaze.com	2 jours	6 jours
ImgDew.com	2 jours	6 jours
ImgOutlet.com	2 jours	4 jours
ALFA TELECOM s.r.o.	1 jour	4 jours
DataWeb Global Group B.V.	1 jour	2 jours
ImageVenue	1 jour	1 jour
ImageBam	1 jour	1 jour

Durée de maintien en ligne des images durant la période étudiée entre l'envoi d'une demande de suppression et le 31 décembre 2020.
Une image est considérée comme supprimée lorsqu'elle n'est plus accessible à l'adresse URL ciblée.

Analyse

Par ses rapports avec les survivant.e.s, le CCPE a appris que l'existence et le maintien en ligne d'images de leurs abus ajoutent une dimension supplémentaire à leur traumatisme et les affectent dans toutes les sphères de leur vie. Pour les survivant.e.s, le simple fait de savoir que ces images existent et que des gens de partout dans le monde tirent du plaisir de leur souffrance suscite une gamme d'émotions dont la peur, la honte et un sentiment profond d'impuissance. C'est essentiellement pourquoi il est si capital d'obtenir rapidement la suppression de ces images préjudiciables.

Le délai médian de suppression des images ciblées par Projet Arachnid est de 24 heures. Cette réalité doit toutefois être située dans le contexte global du problème. Prise isolément, cette statistique est encourageante, car elle donne à penser que Projet Arachnid arrive à obtenir la suppression d'une part importante des images ciblées dans des délais relativement rapides. Or, elle occulte l'un des principaux aspects de la problématique. 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. Ils n'ont pas à subir de conséquences pour leur inaction en matière de prévention. Les forts taux de récidive d'images rapportés plus loin témoignent crument de cette réalité.

Les FSÉ devraient mettre tout en œuvre pour empêcher d'emblée que de telles images puissent être mises en ligne sur leurs plateformes. À défaut, le recours à des technologies de détection proactive peut aider à en accélérer la suppression ou à bloquer les images connues.

Cela dit, ce rapport veut attirer tout particulièrement l'attention sur les délais de suppression beaucoup plus longs qui se situent au-delà du 90^{e} percentile. Plus les délais de suppression sont longs, plus le préjudice subi par les victimes figurant dans les images est grand.

Le tableau ci-dessous illustre l'éventail des réponses et des comportements de l'industrie vis-à-vis des demandes de suppression adressées par le CCPE. Il convient de noter que certains FSÉ peuvent adopter une approche proactive pour détecter les images d'abus pédosexuels, mais se montrer très réfractaires aux demandes de suppression. Les catégories suivantes ne s'excluent donc pas mutuellement.

Proactivité :	Entreprises qui cherchent activement à détecter les images d'abus pédosexuels et à en empêcher la publication sur leurs serveurs. Il s'agit généralement de grandes entreprises de technologie, mais parfois aussi d'entreprises de plus petite taille.
Réactivité :	Petites et grandes entreprises qui réagissent favorablement aux demandes de suppression, mais qui ne cherchent pas activement à empêcher la publication d'images d'abus pédosexuels sur leurs serveurs. Le temps de réaction varie d'une entreprise à l'autre.
Résistance :	Entreprises qui contestent ou qui rejettent les demandes de suppression soit parce qu'elles ne sont pas convaincues que l'image montre un enfant, soit parce qu'elles refusent de reconnaître le caractère illégal de la photo ou de la vidéo.
Récalcitrance :	Entreprises qui ignorent les demandes de suppression ou qui refusent simplement de supprimer des images clairement associées à des abus pédosexuels.
Complicité :	Entreprises qui permettent sciemment la publication d'images d'abus pédosexuels sur leurs serveurs et qui cherchent parfois à protéger leurs clients qui se livrent à des activités illégales.

Les tendances qui ressortent des données recueillies par Projet Arachnid sont souvent indicatrices d'un changement de comportement chez un FSÉ. La diminution des délais de suppression est un bon indicateur pour déceler les FSÉ qui ont peut-être adopté des stratégies proactives de réduction des préjudices.

Délais de suppression des images d'enfants post-pubères

Un coup d'œil au **Tableau 6.2** permet de constater que les délais de suppression sont beaucoup plus longs pour les images d'enfants post-pubères que pour les images d'enfants prépubères.

Ici, la longueur des délais peut s'expliquer de diverses manières :

- les images d'abus pédosexuels sont jugées moins graves lorsqu'elles mettent en scène des enfants post-pubères et reçoivent donc un degré de priorité moins élevé;
- les FSÉ n'estiment pas que les images en question constituent des images d'abus pédosexuels;
- les FSÉ s'attardent aux repères visuels observables sur les images sans égard au contexte potentiellement illégal dans lequel elles ont été produites et tardent donc à les supprimer.

On peut citer ici, à titre d'exemple, une situation vécue par le CCPE :

Dans un long échange de courriels, un FSÉ contestait la catégorisation de certaines images. Ces images d'une fille nue avaient été examinées par des analystes du CCPE, qui les avaient reliées à une victime connue âgée de 15 ans.

Le représentant du FSÉ remettait en question l'âge attribué à la victime sous prétexte que d'autres informations trouvées en ligne indiquaient qu'elle était adulte. Il a fallu lui faire remarquer que la victime était devenue adulte entre le moment où les images avaient été prises, quelques années plus tôt, et le moment où les demandes de suppression ont été envoyées.

Les images ont toutes fini par être supprimées, bien que l'une d'entre elles l'ait été au bout de neuf jours. Cet exemple démontre l'absurdité des situations que l'on peut rencontrer dans ce domaine. Dans un contexte où l'arriéré d'images suspectes à examiner est considérable, comme nous l'avons mentionné précédemment, ces interactions ponctuelles avec les FSÉ pèsent constamment sur des ressources limitées et entraînent des délais de suppression préjudiciables aux victimes et aux survivant.e.s.

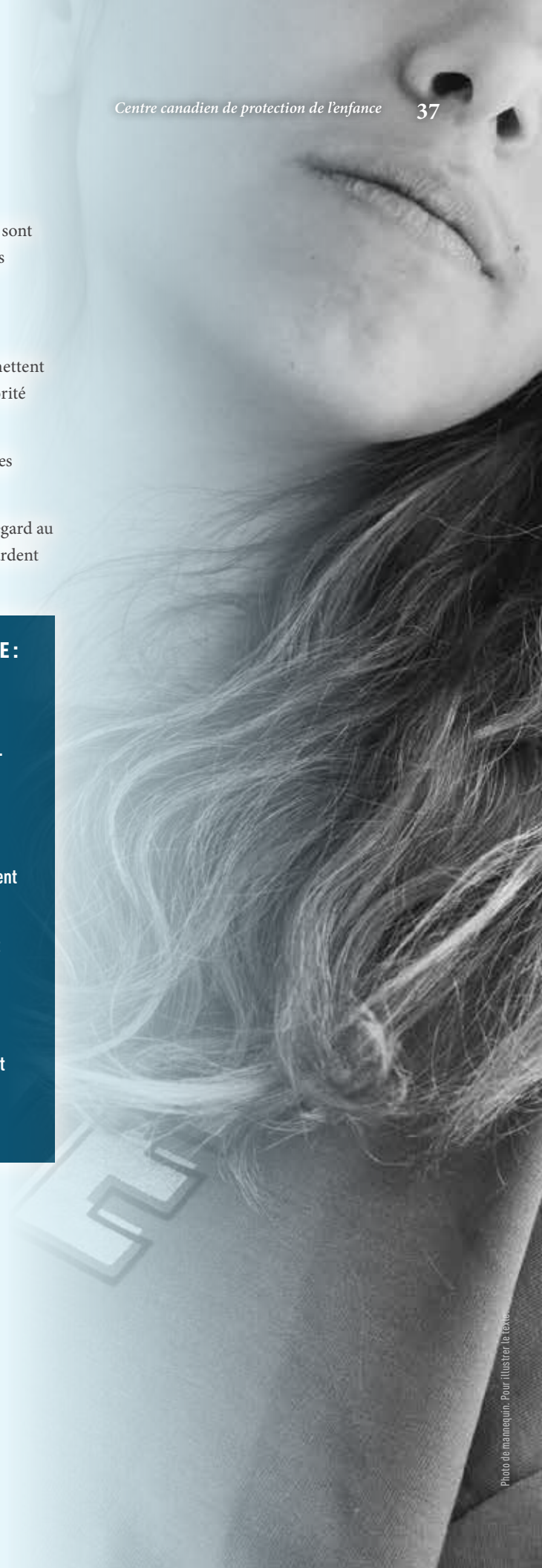


Photo de mannequin. Pour illustrer le texte

Récidive d'images

À la différence des délais de suppression, qui mesurent la réactivité des FSÉ aux demandes de suppression, le taux de récidive d'images offre un éclairage sur l'adoption (ou la non-adoption) de stratégies préventives par les FSÉ.

Nous avons relevé la récidive d'au moins une photo ou vidéo précédemment ciblée pour suppression sur les serveurs de 41 % des 761 FSÉ ayant reçu au moins une demande de suppression venant de Projet Arachnid dans les trois années de la période étudiée.

Le **Tableau 7.1** montre que, dans ces trois années, 48 % des images ciblées pour suppression avaient déjà été détectées sur les plateformes du même FSÉ. On y constate aussi que les taux de récidive d'images ont généralement augmenté durant la même période. Le Tableau 7.1 montre que ces taux ont plus que doublé, passant de 20,7 % en 2018 à 54,9 % en 2020.

Il est important de noter que les taux de récidive d'images calculés ici ne sont pas nécessairement comparables d'un FSÉ à l'autre, car ils sont influencés par de nombreux facteurs. Par exemple, sur un site dont la clientèle se compose essentiellement de producteurs d'images d'abus pédosexuels, les images mises en ligne seront souvent inédites, mais il y a d'autres sites où les utilisateurs republient sans cesse les mêmes images. Dans le premier cas, ce site présentera un taux de récidive peu élevé puisque les images que Projet Arachnid y détectera seront vraisemblablement de nouvelles images.

Par conséquent, un site établi qui a reçu de nombreuses demandes de suppression ces dernières années présentera un taux de récidive plus élevé qu'un nouveau site ayant exactement le même contenu parce que les demandes de suppression que Projet Arachnid enverra au nouveau site porteront sur des images qui n'y auront encore jamais été détectées.

Le **Tableau 7.2** montre que les taux de récidive sont nettement plus élevés pour les images d'enfants post-pubères (73,1 %) que pour les images d'enfants prépubères (46 %) et les images préjudiciables ou violentes (18 %). Ces résultats donnent à penser que les FSÉ avaient plutôt tendance à retarder sensiblement (ou même à ignorer) les demandes de suppression portant sur des images d'enfants post-pubères et/ou l'ajout des empreintes numériques de ces images à leurs listes de blocage, à supposer qu'ils en tenaient une.

Tableau 7.1

Taux de récidive pour l'ensemble des images ayant fait l'objet d'une demande de suppression

	Images récidivistes	Toutes images confondues	Taux de récidive
2018	11 258	54 448	20,7 %
2019	103 987	211 470	49,2 %
2020	100 464	183 152	54,9 %
All years	215 709	449 070	48,0 %

Toutes années confondues.

Les récidives sont établies sur la base de la correspondance d'empreintes numériques SHA-1.

Model in image and intended as illustrative.

Tableau 7.2

Taux de récidive, par catégorie d'images

Catégorie d'images	2018	2019	2020	Toutes années confondues
Images d'enfants prépubères	21,7 %	49,4 %	50,1 %	46,0 %
Images d'enfants post-pubères	23,8 %	64,0 %	77,4 %	73,1 %
Images préjudiciables ou violentes	7,2 %	14,1 %	21,1 %	18,0 %

Les récidives sont établies sur la base de la correspondance d'empreintes numériques SHA-1.

Il faut savoir aussi que les FSÉ, même s'ils hébergent physiquement les images sur leurs serveurs, n'y ont pas pour autant toujours accès. Par exemple, si le client d'un hébergeur offre un service de chiffrement, l'hébergeur ne sera pas nécessairement en mesure de voir son contenu ou d'y accéder. Dans un tel cas, la détection proactive des images par l'hébergeur ne serait pas une option.

Le **Tableau 7.3** montre que des FSÉ comme le tchèque ALFA Telecom s.r.o. et les néerlandais Serverel, ImageVenue et LiteServer Holding B.V. présentent des taux de récidive supérieurs à 86 %. Dans les faits, cela signifie que ces FSÉ ont continué d'héberger des images que Projet Arachnid leur avait maintes fois signalées.

Tableau 7.3

Taux de récidive pour toutes les images ayant fait l'objet d'une demande de suppression, par FSÉ

Nom du FSÉ	Taux de récidive, toutes années confondues
ALFA TELECOM s.r.o.	93,6 %
Serverel	93,5 %
ImageVenue	87,5 %
Liteserver Holding B.V.	86,4 %
Host Sailor	68,6 %
FranTech Solutions	65,3 %
CloudFlare	48,6 %
ColoCrossing	35,5 %
Increditserve LTD	34,0 %
Trichan	26,2 %
OVHcloud	11,4 %
DataWeb Global Group B.V.	11,4 %
NFOrce Entertainment B.V.	5,9 %
ImgDew.com	5,8 %
ImgView.net	5,3 %
ImgOutlet.com	4,9 %
ImgMaze.com	4,5 %
ImageBam	3,2 %

Les récidives sont établies sur la base de la correspondance d'empreintes numériques SHA-1.

Analyse

La comparaison d'empreintes numériques est la principale méthode de détection automatique d'images illicites, mais ce ne sont pas tous les FSÉ qui l'utilisent. Lorsqu'un utilisateur dépose des images sur le serveur d'un FSÉ, les empreintes numériques de celles-ci sont systématiquement croisées avec des banques d'empreintes d'images d'abus pédosexuels et d'images préjudiciables ou violentes précédemment détectées. En cas de correspondance, les images sont soit bloquées, soit supprimées. Cette méthode s'avère très efficace pour freiner la distribution d'images connues, mais elle ne peut empêcher la mise en ligne d'images nouvelles.

Déployée correctement et en l'absence d'un système de chiffrement, la comparaison d'empreintes numériques permet aux administrateurs de contenu de réduire les chances que des images précédemment supprimées réapparaissent sur leurs serveurs.

Hélas, beaucoup de FSÉ ne semblent pas utiliser cette méthode élémentaire puisque Projet Arachnid a détecté (par correspondance d'empreintes numériques SHA-1) au moins un cas de réapparition d'image chez presque 41 % d'entre eux.

Comme mentionné plus haut, même si le contenu est physiquement hébergé sur leurs serveurs, les FSÉ ne sont pas nécessairement capables pour autant de détecter des images dans les espaces de leurs clients ni d'y accéder directement. Pour cette raison, certains hébergeurs ont indiqué au CCPE être d'avis que la détection proactive était techniquement impossible et qu'ils ne pouvaient donc rien pour empêcher des images de réapparaître sur leurs serveurs.

Bien qu'il puisse y avoir des contraintes techniques comme celles décrites précédemment, le CCPE est d'avis que rien n'empêche les FSÉ d'obliger par contrat leurs clients à prendre des mesures pour respecter les lois. Ils pourraient par exemple exiger de leurs clients qu'ils utilisent certaines technologies de détection d'images, bloquer les transferts de fichiers à partir du Web clandestin, maintenir une certaine capacité de modération humaine et supprimer les images dans un délai déterminé à partir de leur détection ou de leur signalement.

Ces solutions pratiques seront expliquées plus en détail plus loin, dans les recommandations.

Photo de mannequin. Pour illustrer le texte.

Correspondances d'images : SHA-1 vs PhotoDNA

L'établissement d'une correspondance SHA-1 repose sur une empreinte numérique unique. Le fichier numérique de l'image, jusqu'au niveau binaire, doit correspondre exactement à une autre image. Toute modification de l'image ou de ses métadonnées aura pour effet de changer son empreinte numérique SHA-1, empêchant ainsi toute correspondance avec la version antérieure de l'image. Par exemple, les opérations suivantes sur une image auraient pour effet de modifier son empreinte numérique :

- **changement de couleur;**
- **redimensionnement;**
- **enregistrement dans un format de fichier différent;**
- **modification des métadonnées (données Exif);**
- **suppression ou addition d'un pixel;**
- **prise d'une capture d'écran de l'image.**

Dans les faits, de nombreuses images détectées par Projet Arachnid sont des versions légèrement modifiées d'images précédemment vérifiées; or, ces différences sont généralement imperceptibles à l'œil humain. Bien qu'il s'agisse visuellement des mêmes images, leurs empreintes numériques uniques différeront pour les raisons expliquées plus haut.

Pour établir des correspondances entre des images non identiques, il est possible d'utiliser une technologie de correspondance approximative, comme l'algorithme PhotoDNA de Microsoft, bien connu dans le milieu. Bien que Projet Arachnid utilise PhotoDNA, les taux de récidive rapportés ici sont basés sur la correspondance exacte d'empreintes numériques SHA-1 et ne tiennent pas compte de l'existence de variantes semblables en apparence des mêmes images. Par le fait même, il y a lieu de croire que les taux de récidive présentés ici sont très en deçà de la réalité.

Récidive d'images d'enfants post-pubères

Comme le montre le Tableau 8.2, les images d'enfants post-pubères présentent des taux de récidive nettement plus élevés que les images d'enfants prépubères et les images préjudiciables ou violentes.

Cette situation pourrait être attribuable à certains des mêmes facteurs mentionnés plus haut comme raisons possibles des longs délais de suppression pour cette catégorie d'images. Soulignons par ailleurs qu'en plus des mesures préventives qu'un FSÉ peut prendre, les taux de récidive d'images dépendent aussi de la nature du contenu mis en ligne par les utilisateurs d'un FSÉ. Par exemple, une collection d'images nouvelles présenterait des taux de récidive relativement peu élevés comparativement à une collection d'images largement diffusée.

À la différence des images d'enfants prépubères, des images d'enfants post-pubères sont souvent détectées à travers des images d'adultes ou encore sur des sites grand public qui acceptent de la pornographie adulte (p. ex. Twitter). On pourrait supposer que les personnes qui envoient ces images sur Internet estiment que l'âge apparent du sujet est suffisamment incertain pour leur fournir une défense plausible dans le cas où ils auraient à répondre de leurs actes. Cela dénote peut-être aussi une méconnaissance de la définition d'une image d'abus pédosexuels et des conséquences associées à la distribution de telles images.

Mis ensemble, ces facteurs peuvent amener les administrateurs de contenu et les utilisateurs à penser qu'il est relativement peu risqué de mettre et de remettre en ligne des images d'enfants post-pubères.

Il découle de ce qui précède qu'en l'absence d'informations permettant de croire que les personnes figurant sur certaines images sont mineures, les administrateurs de sites Web peuvent décider d'ignorer les demandes de suppression des images d'enfants post-pubères qui leur sont signalées et de ne pas ajouter ces images à leurs listes de blocage.

Cette attitude à l'égard des images d'enfants post-pubères explique peut-être en partie les taux de récidive d'images plus élevés pour cette catégorie.

ÉTUDE DE CAS

L'opérateur de télécommunications français Free : La plus grande source d'images d'abus pédosexuels détectées par Projet Arachnid

Dans les trois années de la période étudiée (2018-2020), Projet Arachnid a adressé des demandes de suppression à plus de 760 FSÉ. Les données recueillies dans ce contexte montrent clairement que certains FSÉ contribuent, directement ou indirectement, de façon plus importante que d'autres à la distribution des images d'abus pédosexuels et des images préjudiciables ou violentes sur Internet.

Les données de Projet Arachnid concernant les détections d'images ciblées pour suppression révèlent en outre qu'un volume très important d'images d'abus pédosexuels et d'images préjudiciables ou violentes est mis à disposition sur les serveurs d'un FSÉ en particulier : le géant français des télécommunications Free, propriété du groupe Iliad de Paris.

Pour les trois années de la période étudiée, Projet Arachnid a détecté plus de 18 000 fichiers d'archive contenant collectivement près de 1,1 million de photos et de vidéos assimilables en apparence à des images d'abus pédosexuels ou à des images préjudiciables ou violentes. Ces fichiers étaient (ou, dans certains cas, sont toujours) hébergés directement sur le service public d'hébergement de fichiers de Free.

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 des sites Tor. 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 se chiffre à plus de 2,7 millions d'images détectées.

Polémique passée autour du service d'hébergement de Free

Ce service d'hébergement de fichiers, logé à l'adresse dl.free.fr, a essuyé des critiques en octobre 2007. La ministre française de la Culture de l'époque l'avait alors pointé du doigt, estimant que ses opérateurs ne prenaient pas de mesures adéquates pour lutter contre la distribution illégale d'œuvres protégées par le droit d'auteur.

Dans une déclaration officielle, la ministre avait manifesté sa réticence face aux nouvelles caractéristiques de ce service, qui « permet aux internautes de télécharger anonymement et massivement des contenus pirates sur dl.free.fr[8] » .

Elle a aussi demandé au directeur général d'Iliad de l'époque que la « maîtrise technique incontestée » de Free soit mise à profit pour faire respecter la loi, soit en limitant l'accès à son service d'hébergement de fichiers, soit en le supprimant purement et simplement.

Dans sa déclaration, la ministre avait aussi rappelé les détails d'une récente décision de justice qui avait contraint Free à bloquer l'accès à 14 « newsgroups binaires », un type de forum décentralisé souvent utilisé pour faciliter le partage de fichiers entre utilisateurs. On se souviendra qu'à l'époque, plusieurs associations de défense des droits d'auteurs avaient manifesté leurs inquiétudes vis-à-vis du service d'hébergement. Le gouvernement français était allé jusqu'à menacer Free de voir sa demande de licence 3G refusée à cause de son service d'hébergement de fichiers.

8 Ministère de la Culture. (2007, October 12). *Christine Albanel demande à Free de lutter plus activement contre le piratage.* http://www2.culture.gouv.fr/culture/actualites/ communiq/albanel/free07.html

Description du service d'hébergement

On trouve dans les archives du Web des captures de la page d'accueil du site d'hébergement gratuit de Free datant d'aussi loin que début 2006, époque à laquelle le service avait été lancé à titre expérimental[9].

Ce service semble avoir la cote auprès des internautes qui veulent distribuer anonymement de gros volumes d'images. Il est recommandé dans des forums du Web clandestin pour la distribution d'images d'abus pédosexuels.

On peut avancer quelques raisons pour expliquer la popularité de ce service :

- L'utilisateur n'a pas à ouvrir de compte, ni à s'inscrire, ni à indiquer ses coordonnées ou à débourser de frais pour mettre un fichier en ligne, créer un lien de téléchargement et partager ce lien avec n'importe qui, n'importe où.
- L'interface est minimaliste, mais la limite de taille des fichiers est très généreuse, ce qui permet de mettre en ligne et de distribuer de grandes collections d'images.
- L'utilisateur peut protéger un fichier d'archive par mot de passe, de sorte que seules les personnes en possession du mot de passe puissent accéder au contenu. On peut souvent se procurer ces liens et ces mots de passe sur le Web clandestin.

Il est intéressant de noter que la page d'accueil du service d'envoi de fichiers de Free n'a pas changé d'apparence depuis 2008[10]. Elle utilise d'ailleurs encore l'obsolète protocole de transfert hypertexte non sécurisé (HTTP), tandis que le site principal de Free, lui, utilise le protocole de transfert hypertexte sécurisé (HTTPS).

De plus, en date du 18 mai 2021, le lien « Signaler un contenu illicite » présenté en page d'accueil déclenche une erreur 404, signalant que la page en question n'existe pas.

Tout cela donne à penser que Free ne s'occupe guère de ce service depuis quelques années.

Le service d'hébergement de fichiers de Free et la distribution d'images d'abus pédosexuels

Les internautes qui veulent distribuer des images d'abus pédosexuels et des images préjudiciables ou violentes utilisent le service d'hébergement de Free pour stocker anonymement des fichiers sur Internet et en diffuser par la suite les liens de téléchargement direct sur des forums en ligne.

Les relevés d'exploration de Projet Arachnid montrent que des liens menant à dl.free.fr sont fréquemment détectés dans des forums de discussion du réseau Tor, où un nombre inconnu d'utilisateurs anonymes peuvent se procurer les liens directs pour télécharger les fichiers correspondants ainsi que les mots de passe pour les ouvrir et accéder à leur contenu.

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 pourraient très bien réapparaître sur Internet à une date ultérieure.

Communications avec des représentants de Free

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 fait l'objet de demandes de suppression durant les trois années de la période étudiée étaient toujours publiquement accessibles.

---

9 Free. (2006). *Conditions d'utilisation du nouveau service experimental* ***http://dl.free.fr***. https://web.archive.org/web/20060126211229/http://dl.free.fr/

10 Free. (2008). *Service d'envoi de fichiers http://dl.free.fr* https://web.archive.org/web/20081106103820/http://www.dl.free.fr/

ÉTUDE DE CAS

Projet Arachnid s'attaque aux forums à images Trichan

Parmi les grands hébergeurs d'images d'abus pédosexuels avec lesquels Projet Arachnid a eu affaire, il y a un groupe de forums à images connu sous le nom de Trichan. Hébergés en grande partie aux Pays-Bas, ces forums aujourd'hui disparus étaient principalement consacrés à l'exploitation sexuelle d'enfants et existaient depuis au moins sept ans.

Cette brève étude de cas sur la façon dont le CCPE a utilisé Projet Arachnid pour perturber la distribution d'images d'abus pédosexuels donne un aperçu des démarches qu'il faut entreprendre et des obstacles qu'il faut surmonter pour faire enlever d'Internet des images d'abus pédosexuels et des images préjudiciables ou violentes d'enfants.

Premier contact

En mars 2019, Projet Arachnid a vu le nombre d'images détectées sur les forums Trichan monter en flèche. La situation était telle que les informaticiens du CCPE ont dû modifier le robot d'exploration d'Arachnid pour gérer toutes ces détections.

Aussitôt que le système a commencé à envoyer des demandes de suppression, il est devenu évident que l'opérateur de Trichan n'était pas disposé à agir. Les nombreux courriels envoyés aux adresses indiquées sur les sites n'y changeaient rien : la grande majorité des images signalées étaient maintenues en ligne. Les demandes de suppression ont fini par générer des avis de non-livraison.

Malgré tout, Projet Arachnid a continué de compiler des données sur les images d'abus pédosexuels détectées sur ces forums. Les analystes du CCPE ont alors entrepris d'examiner ces images. Sur la base d'un échantillon de 51 917 images, ils ont établi que le contenu des forums se composait à près de 34 % d'images d'abus pédosexuels et que le reste était possiblement constitué d'images d'abus pédosexuels et d'images préjudiciables ou violentes.

Fort de ces données et compte tenu du fait que l'administrateur de Trichan ignorait essentiellement les demandes de suppression que lui adressait Projet Arachnid, le CCPE s'est adressé aux FSÉ en amont dans l'espoir de faire bouger les choses.

Ces derniers ont d'abord opposé une forte résistance, allant parfois jusqu'à suggérer au CCPE d'adresser plutôt ses demandes de suppression à la centrale de signalement des Pays-Bas. Après de nombreux allers-retours avec les FSÉ en amont, certains ont pris des mesures pour bloquer le routage des adresses IP de Trichan.

Dans les semaines qui ont suivi, Trichan a changé plusieurs fois d'hébergeur. À chaque occasion, le CCPE informait le nouvel hébergeur – données à l'appui – de la nature du contenu hébergé sur Trichan.

Déploiement de techniques d'évasion

Les forums de Trichan ont finalement disparu d'Internet pendant une période d'environ trois mois. Mais ils ont refait surface, et l'on a pu rapidement constater qu'ils utilisaient à présent une nouvelle technique pour échapper à la détection automatisée des images d'abus pédosexuels.

Cette technique, dont le résultat était imperceptible à l'œil humain, consistait à injecter du « bruit » dans les images par décalage aléatoire de pixels, de sorte que des versions modifiées de ces images s'affichaient à l'écran du visiteur à chaque nouvel appel de fichier. Dès lors, il devenait plus difficile pour Projet Arachnid de croiser ces empreintes avec celles d'images précédemment signalées.

Néanmoins, grâce à l'utilisation de technologies de comparaison approximative d'images comme l'algorithme PhotoDNA de Microsoft, Projet Arachnid a pu continuer de détecter les images d'abus pédosexuels et d'envoyer des demandes de suppression.

Ces deux images paraissent identiques à l'œil humain, mais elles ont des empreintes numériques complètement différentes. Les taches rouges représentent des ensembles de pixels qui ont été légèrement décalés d'une image à l'autre.

Une fois de plus, le CCPE est intervenu auprès du nouvel hébergeur, et les forums Trichan ont été mis hors ligne peu après. Apparemment confronté à l'impossibilité de trouver un hébergeur tolérant, l'administrateur de Trichan a fini par capituler. Dans une annonce publiée en page d'accueil, l'un des modérateurs de Trichan a déploré les efforts acharnés qui étaient déployés pour faire disparaître leurs images et annoncé du même souffle la fermeture définitive du site :

> « Après sept merveilleuses années, nous aurions bien aimé continuer encore sept années de plus, mais les antis s'acharnent sur nous avec un zèle sans précédent, et après avoir dû fermer deux douzaines de fois et servi quotidiennement plus de 100 000 frères dans le monde entier, nous n'avons plus les moyens financiers de continuer. » [traduction libre].

Sur une période d'environ deux ans et demi, Projet Arachnid a détecté plus de 1,5 million d'images vérifiées sur Trichan.

Analyse

Cette étude de cas illustre concrètement le dur combat des organismes qui luttent pour obtenir la suppression des images d'abus pédosexuels. Elle présage aussi les nombreux obstacles qui se dresseront inévitablement devant les gouvernements qui voudront réglementer la diffusion de ce type de contenu sur Internet.

Comme le rapporte une étude récente[11] consacrée à cette histoire, la continuité des activités des forums Trichan a été rendue possible par une chaîne de FSÉ, dont certains ignoraient l'existence des images d'abus pédosexuels tandis que d'autres ne semblaient guère se préoccuper du fait que leurs clients mettaient de telles images à la disposition du public.

La résistance de certains FSÉ à sévir, malgré les preuves qui leur sont présentées, contre leurs clients distribuent massivement des images d'abus pédosexuels est un problème auquel les décideurs politiques doivent s'attaquer.

Dans le cas de Trichan, le CCPE a finalement réussi à obtenir la suppression des images en s'adressant aux fournisseurs de services en amont. Comme le notent Salter et Richardson (2021), cette intervention montre qu'il s'avère efficace de miser sur les relations de pouvoir entre les FSÉ et d'agir de concert avec les nœuds influents du réseau numérique global.

Les données collectées par Projet Arachnid permettent au CCPE de dresser un portrait d'ensemble des relations entre les FSÉ en aval et en amont et de montrer comment l'action et l'inaction de ces acteurs contribuent directement à la présence d'images d'abus pédosexuels et d'images préjudiciables ou violentes sur Internet.

Les auteurs de cette étude soulignent que « les fournisseurs de transit et d'autres services stratégiques concluent constamment des accords commerciaux avec des fournisseurs de services et des clients impliqués dans la distribution d'images d'abus pédosexuels[12]. » Et en dépit du rôle central de ces accords commerciaux dans la distribution d'images d'abus pédosexuels sur Internet, Salter et Richardson notent que les FSÉ ne sont pas tenus par la loi de refuser de servir des clients qui se livrent à ces activités abusives et potentiellement illégales.

11 M. Salter et L. Richardson (2021). « The Trichan takedown: Lessons in the governance and regulation of child sexual abuse material », *Policy & Internet*, vol. 13, nº 2. Publication en ligne anticipée. https://doi.org/10.1002/poi3.256

12 M. Salter et L. Richardson (2021). « The Trichan takedown: Lessons in the governance and regulation of child sexual abuse material », *Policy & Internet*, vol. 13, nº 2. Publication en ligne anticipée. https://doi.org/10.1002/poi3.256

RECOMMANDATIONS

L'analyse présentée ici fait ressortir plusieurs enjeux majeurs qui méritent une attention particulière et une action immédiate de la part des FSÉ et des décideurs politiques.

Les résultats montrent aussi que l'on ne peut tout simplement pas compter sur les FSÉ pour investir volontairement des ressources adéquates dans la modération de contenu et faire primer la sécurité des enfants et leur droit à la vie privée.

Cette approche ne fonctionne pas, comme on peut en juger aussi par la disparité des obligations de signalement d'un pays à l'autre, l'hétérogénéité des mesures de modération appliquées par les sociétés et le déluge de victimes et de survivant.e.s qui peinent à obtenir la suppression de leurs images d'abus.

Dans le contexte de ses activités de suppression d'images, le CCPE a réuni par l'entremise de ses enquêtes auprès des survivant.e.s, des signalements venant du public et des activités de Projet Arachnid beaucoup d'informations qui mettent en évidence les faiblesses d'environnements réglementaires totalement inadéquats. Cette connaissance du terrain place notre organisation dans une situation idéale pour recommander des mesures réglementaires qui permettront d'obtenir les meilleurs résultats possibles pour les enfants.

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 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 sur Internet.

Photo de mannequin. Pour illustrer le texte.

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

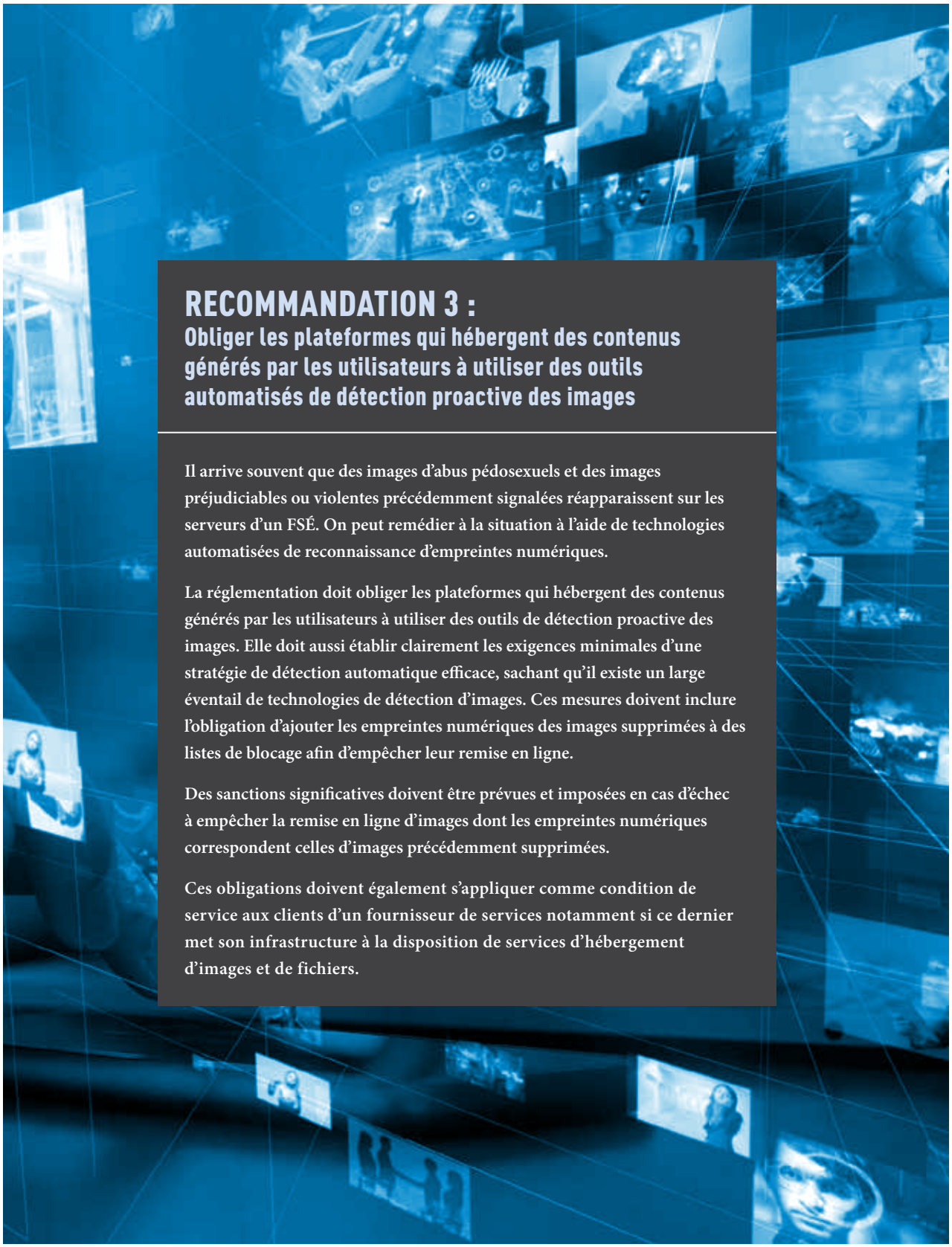
Internet transcende les frontières et il n'existe guère de mesures réglementaires ou législatives concertées pour encadrer les activités des sociétés Internet. Au lieu de cela, l'espace numérique s'articule autour d'une multitude d'accords complexes et interdépendants entre toutes sortes d'entités qui 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 :

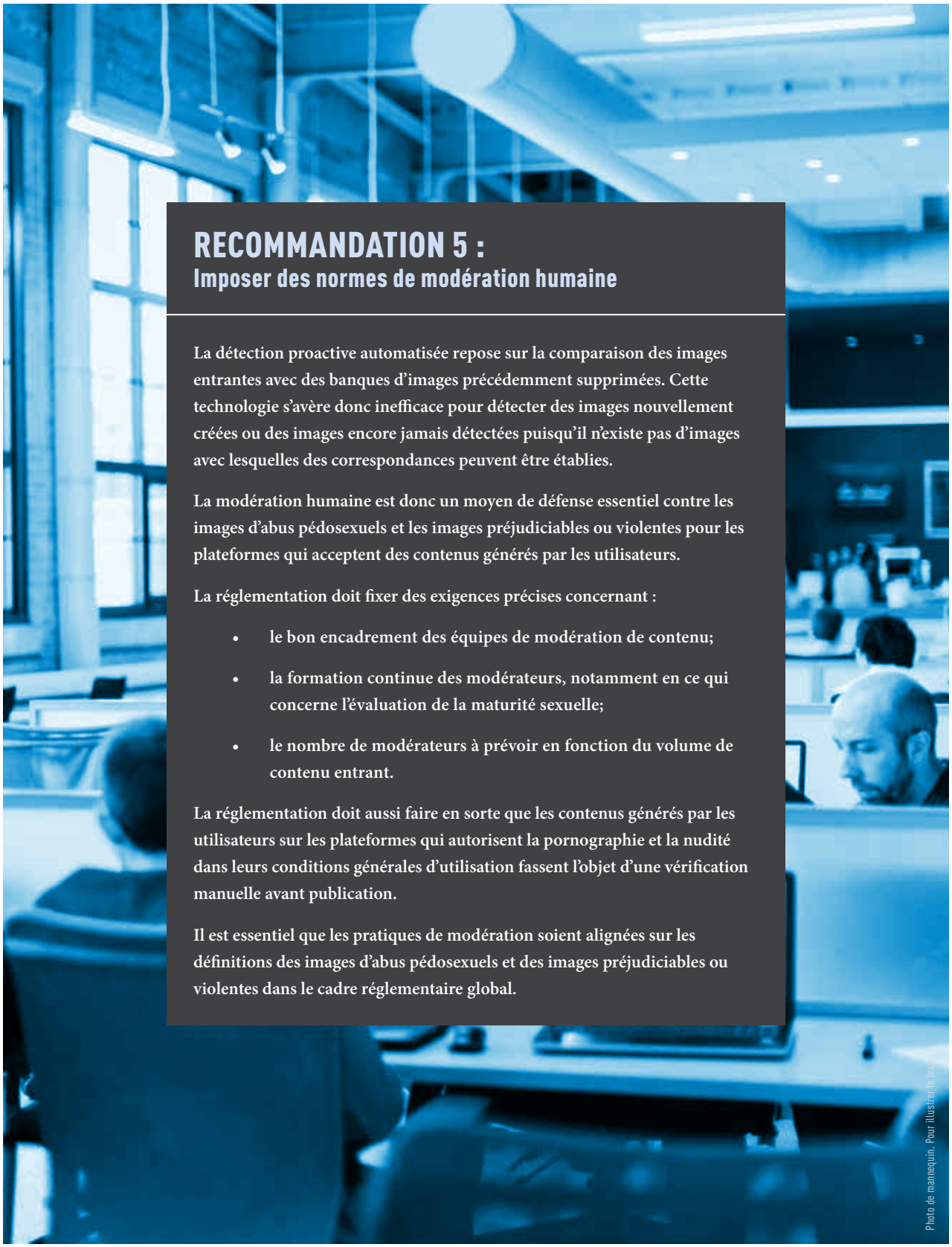
Établir des normes quant aux contenus qui, sans nécessairement être illégaux, restent préjudiciables ou violents à l'égard de personnes mineures

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.

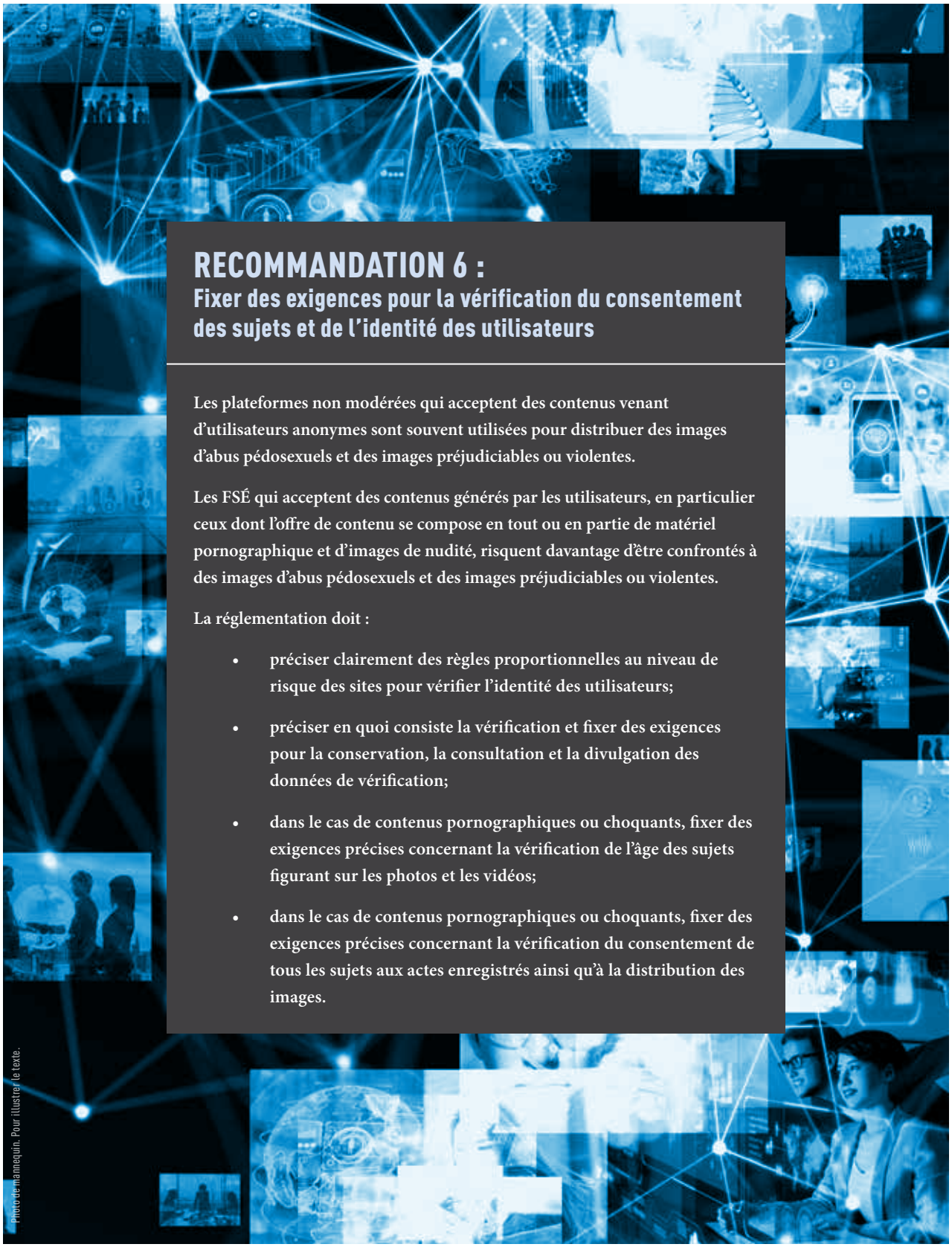
La réglementation doit fixer des exigences précises concernant :

- 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.

Photo de mannequin. Pour illustrer le texte.



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.

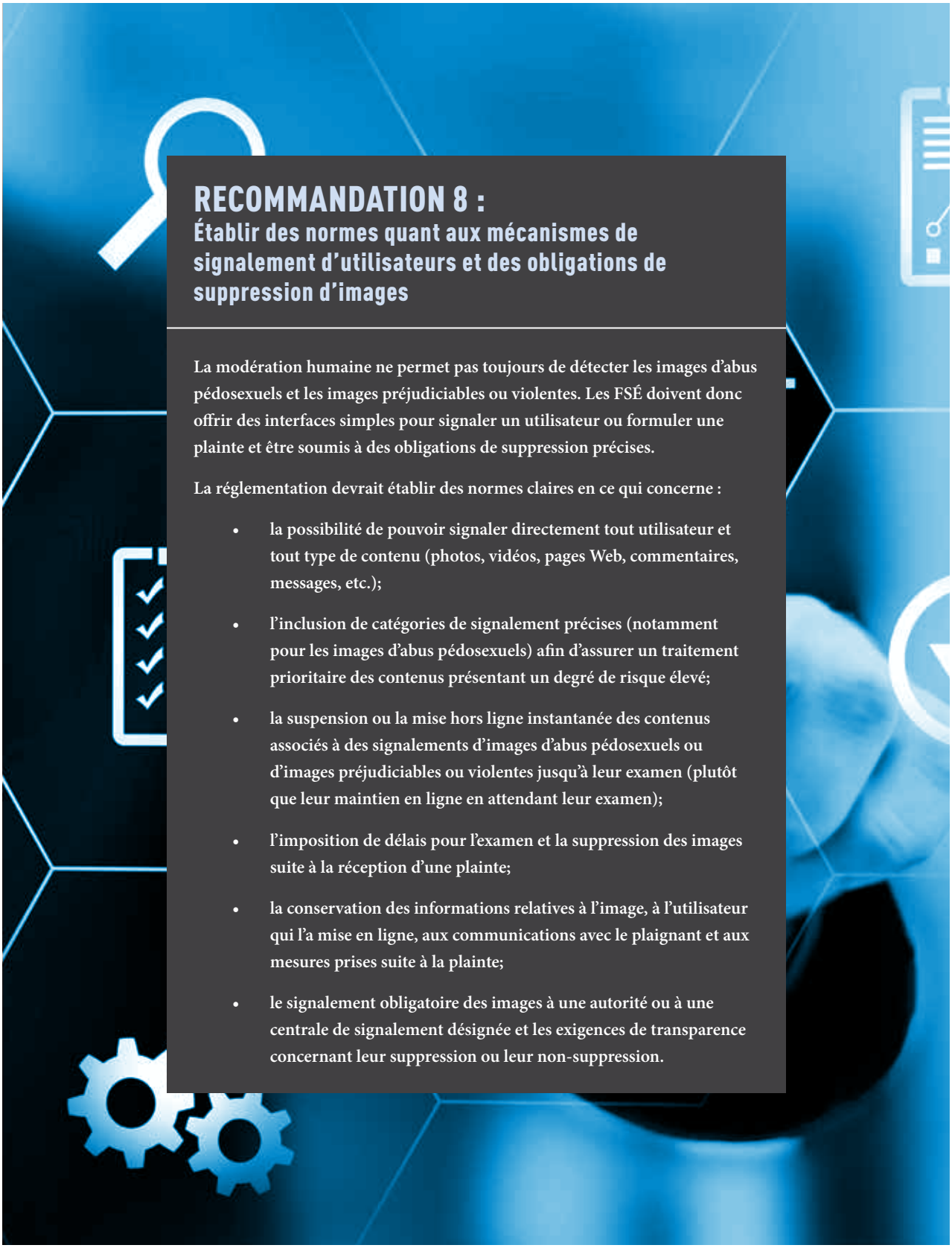
Photo de mannequin. Pour illustrer le texte.

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 présent 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 récidive 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.

Ce 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.

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

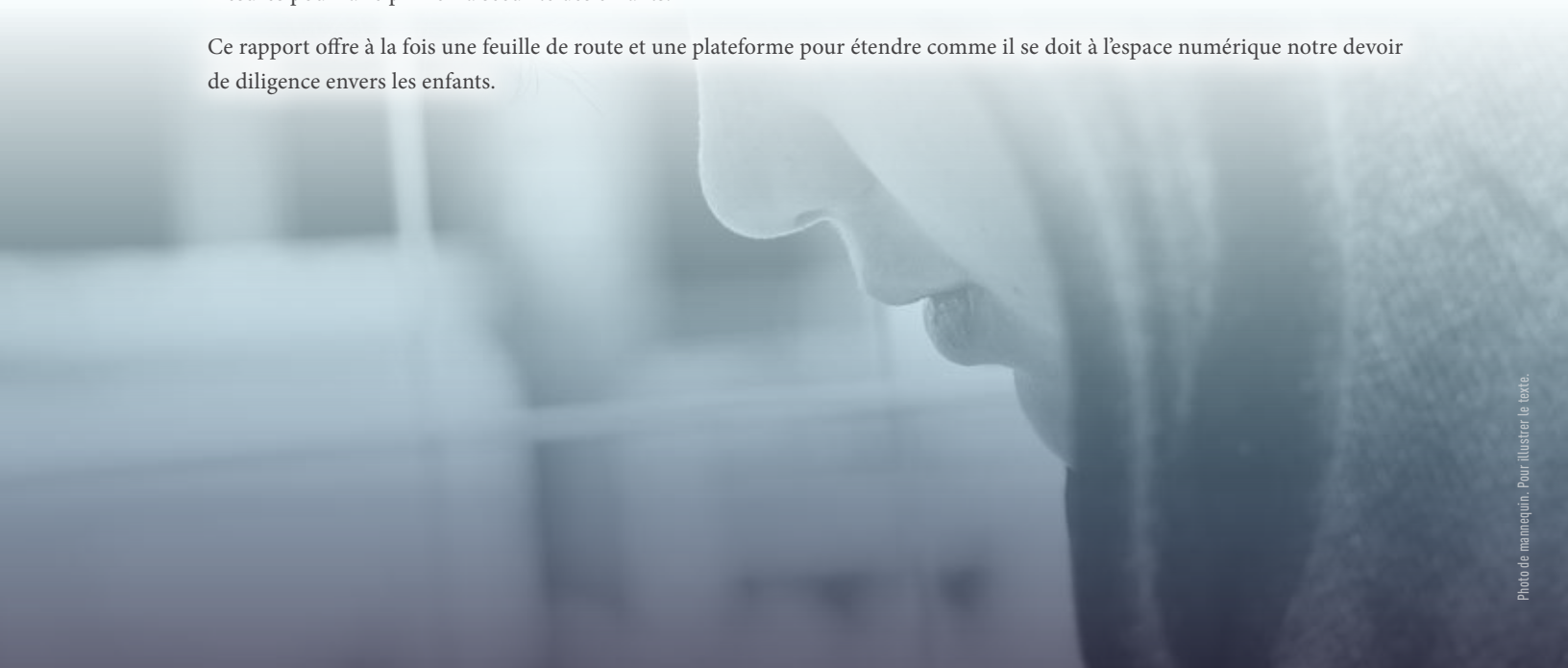


Photo de mannequin. Pour illustrer le texte.

Photo de mannequin. Pour illustrer le texte.

ANNEXE

Glossaire

Administrateur de contenu

Se dit d'un site Web ou d'un service Web. Exception faite des grands FSÉ, la plupart des administrateurs de contenu ne sont ni propriétaires ni gestionnaires des serveurs qu'ils utilisent. Les sites Web qui hébergent des fichiers individuels entrent généralement dans cette catégorie.

Contenu

Se dit de tout type d'image.

Demande de suppression

Avis envoyé à un FSÉ par le Projet Arachnid pour l'informer de la présence sur ses serveurs d'images d'abus pédosexuels ou d'images préjudiciables ou violentes d'enfants et lui demander de les supprimer.

Détection

Se dit de la découverte ou de l'« observation » d'une image sur Internet par Projet Arachnid. L'accessibilité d'une image se mesure à son nombre de détections. Une même image hébergée à un endroit mais incorporée dans plusieurs pages Web donnera lieu à une détection pour chaque occurrence relevée par Projet Arachnid.

Données Exif

De l'anglais Exchangeable Image File Format. Norme d'échange de données utilisée en photographie numérique pour la capture de métadonnées (date de création, rapport hauteur/largeur, résolution, endroit où l'image a été prise, etc.).

Empreinte numérique

Valeur unique (ou signature) représentant un fichier informatique. Les empreintes numériques sont produites par un algorithme de hachage.

Enfant

Personne âgée de moins de 18 ans.

Fournisseur de services électroniques (FSÉ)

Terme générique désignant toute entité qui fournit un service dans l'espace numérique (réseaux de diffusion de contenu, hébergeurs, fournisseurs de services en nuage, administrateurs de contenu ou de sites Web, fournisseurs de services Internet, etc.).

Hébergeur

Entreprise qui fournit les technologies et les services nécessaires pour diffuser un site ou une page Web sur Internet. Un site Web est hébergé (ou conservé) sur les serveurs de l'hébergeur.

Image

Se dit de tous les types de contenus traités par Projet Arachnid. Il s'agit généralement de photos, de vidéos ou de fichiers d'archive (qui contiennent des photos ou des vidéos).

Images d'enfants post-pubères

Cette catégorie renvoie à des images d'abus pédosexuels susceptibles de répondre à une définition pénale d'une image d'abus pédosexuels. Les victimes représentées sur ces images sont à l'état post-prépubère et leur âge est connu. Cette catégorie comprend également des images d'enfants aux derniers stades de la puberté.

Images d'enfants prépubères

Cette catégorie renvoie à des images d'abus pédosexuels susceptibles de répondre à une définition pénale d'une image d'abus pédosexuels. Les victimes représentées sur ces images sont à l'état prépubère ou au début de la puberté.

Image examinée

Se dit d'une image qui a été examinée par un analyste. Les images examinées ne constituent pas nécessairement des images d'abus pédosexuels ou des images préjudiciables ou violentes.

Images préjudiciables ou violentes

Catégorie d'images regroupant des images d'enfants qui ne semblent pas répondre aux définitions pénales utilisées dans plusieurs pays, mais qui pourraient néanmoins violer les conditions générales d'utilisation d'un FSÉ. Ces images peuvent aussi porter atteinte à la vie privée ou à la sécurité d'un enfant ou être associées à des images d'abus pédosexuels. Pour une description plus détaillée de cette catégorie d'images, voir le cadre du CCPE (p. 10).

Image suspecte

Se dit de toute image dont on peut raisonnablement penser qu'elle constitue une image d'abus pédosexuels, mais qui n'a pas encore été examinée.

Image vérifiée

Terme utilisé pour désigner une image qu'un analyste, après examen et évaluation, catégorise comme étant soit une image d'abus pédosexuels, soit une image préjudiciable ou violente.

Personne mineure

Personne âgée de moins de 18 ans.

PhotoDNA

Technologie de comparaison d'images servant à détecter des correspondances entre des versions modifiées d'une même image ou d'images présentant des caractéristiques similaires. On parle parfois de « correspondances floues » ou de « hachage perceptuel ». Cette technologie a été développée par Microsoft en partenariat avec le Collège Dartmouth.

Réseau de diffusion de contenu

Réseau de serveurs distribués géographiquement qui permet de réduire les temps de chargement du contenu des pages Web en réduisant la distance physique entre le serveur et l'utilisateur. Ce type de réseau ne révèle généralement pas l'identité de l'hébergeur des sites qui utilisent ses services.

Réseau privé virtuel (VPN)

Réseau privé permettant d'établir une connexion sécurisée (ou tunnel) entre deux points dans un réseau existant comme Internet ou un réseau étendu (WAN). Plusieurs FSÉ offrent des services commerciaux de réseau privé virtuel à leurs utilisateurs.

SHA-1

De l'anglais Secure Hashing Algorithm (algorithme de hachage sécurisé). Valeur de hachage cryptographique attribuée à une image traitée par Projet Arachnid pour lui donner une signature numérique unique établie par un algorithme informatique.

The Onion Router (Tor)

Réseau ouvert qui permet à ses utilisateurs de naviguer anonymement sur le Web. Tor est généralement considéré comme un sous-ensemble de ce que l'on appelle communément le Web clandestin (dark web).

URL

Abréviation de « Universal Resource Locator » (localisateur uniforme de ressource). Une adresse URL conduit directement l'internaute à une page Web ou à une image sur Internet.

Web clandestin

Terme générique désignant l'ensemble des réseaux auxquels on ne peut accéder au moyen d'un navigateur Web traditionnel. Ces réseaux, dont Tor fait partie, chiffrent généralement le trafic Internet et offrent une navigation anonyme.

Web visible

Partie publiquement accessible du Web dont les pages sont en grande partie indexées par les moteurs de recherche.

Liste des acronymes

CCPE : Centre canadien de protection de l'enfance

ECPAT : End Child Prostitution and Trafficking

Exif : Exchangeable Image File Format

FSÉ : Fournisseur de services électroniques

HTTP : hypertext transfer protocol (protocole de transfert hypertexte)

HTTPS : hypertext transport protocol secure (protocole de transfert hypertexte sécurisé)

Interpol : Organisation internationale de police criminelle

NCMEC : National Center for Missing & Exploited Children (États-Unis)

RPV : Réseau privé virtuel

SHA-1: Secure Hash Algorithm 1

Tor : The Onion Router

URL : Uniform Resource Locator (localisateur uniforme de ressource)

Photo de mannequin. Pour illustrer le texte.


Photo de mannequin. Pour illustrer le texte.
CENTRE CANADIEN de PROTECTION DE L'ENFANCE MC
Aider les familles. Protéger les enfants.
protegeonsnosenfants.ca
@ProtegerEnfant
Centre canadien de protection de l'enfance