Child Sexual Abuse ACT – Q&A

Règlement de l'UE sur les règles visant à prévenir et à combattre l'abus sexuel d'enfants

QUESTIONS/MESSAGES PRINCIPAUX

1. ***Qu'est-ce que la loi sur les abus sexuels sexuels d'enfants (CSA – Child Sexual Abuse Act) ?***

En mai 2022, la Commission européenne a déposé une proposition législative visant à prévenir et à combattre l'abus sexuel d'enfants en ligne. Les fournisseurs de services numériques tels que Meta et Google doivent prendre leurs responsabilités quant à ce qu'il se passe sur leurs plateformes afin de les rendre plus sûres pour les enfants. Ils doivent prendre des mesures afin que les images d'abus sexuel d'enfants sur leurs plateformes soient détectées et supprimées. C'est une arme nécessaire dans la lutte contre l'exploitation sexuelle en ligne.

2. ***À quel niveau, par qui et quand ce texte doit-il être voté ?***

Le Parlement européen et le Conseil européen étudient et commentent la proposition en profondeur. Leurs avis et ajustements seront connus d'ici le début du mois d'octobre. Si la proposition est adoptée, le Parlement européen, le Conseil européen et la Commission européenne poursuivront les négociations. S'ils parviennent à l'unanimité, la loi sera votée. La proposition est un règlement, qui rend les règles directement applicables dans tous les États membres de l'UE.

Il est important que cette loi soit adoptée avant que le règlement provisoire n'expire le 3 août 2024. Cette dérogation aux lois sur la protection de la vie privée permet à certains acteurs en ligne d'utiliser la technologie pour détecter les images d'abus sexuels sur leurs propres plateformes.

3. ***Que pense Child Focus de cette proposition ? Pourquoi est-ce si important ?***

Child Focus voit dans cette proposition une opportunité de mieux protéger les enfants en ligne. Année après année, nous constatons que le nombre de dossiers d'exploitation sexuelle augmente. Derrière chaque dossier se cache un enfant marqué à vie. L'organisation réclame depuis de nombreuses années un cadre européen qui responsabilise davantage les acteurs du numérique dans la protection des enfants et des jeunes en ligne. Nous devons utiliser les possibilités offertes par les technologies pour aider et protéger les enfants. Grâce à ce plan ambitieux, nous sommes convaincus que le nombre de cas d'abus sexuel d'enfants en ligne diminuera considérablement.

De plus, les enfants pourront exercer efficacement leurs différents droits : leur droit à la vie privée, leur droit à la protection contre l'exploitation sexuelle en ligne et leur droit à l'information.

4. ***De quelle manière, la Belgique est-elle confrontée aux images d'abus sexuel d'enfants?***

Child Focus dispose d'un point de contact civil (www.imagesdabus.be) où chacun peut signaler (de manière anonyme) des images d'enfants suspectes d'abus sexuel. Une dizaine d'employés de Child Focus analysent les images signalées. En 2022, Child Focus a reçu 1 832 signalements. La Belgique reçoit également des signalements de l'étranger concernant des victimes et des auteurs belges. En 2022, notre organisation mère, NCMEC a envoyé à Europol 50 299 signalements ayant un lien avec la Belgique (soit une augmentation de 319% par rapport à 2021). Mais tous les signalements n'ont pas pu faire l'objet d'une enquête efficace en raison d'un manque d'informations, d'où l'importance d'une approche européenne.

GÉNÉRAL

1. Pourquoi est-il important de s'attaquer à ce problème au niveau européen ?

Le monde numérique ne connaît pas de limites. Les victimes ont peu de contrôle sur leurs images et peu de garanties quant à leurs droits, car elles dépendent du pays où le service où la plateforme est enregistrée. Selon l'Internet Watch Foundation, basée au Royaume-Uni, 66 % de tous les contenus d'abus provenait de l'Union européenne en 2022. Cette législation offre une protection égale aux victimes dans toute l'UE, car toutes les entreprises fournissant des services dans l'UE doivent appliquer les mêmes règles.

2. Comment les enfants sont ils protégés en ligne ?

La proposition repose sur trois piliers qui, ensemble, s'attaquent à la racine du problème :

Prévention efficace →Signalement & détection → Centralisation

- **Prévention** : les fournisseurs de services numériques doivent prendre des mesures ciblées afin de prévenir les abus sexuels en ligne.
- **Obligation de signalement et de détection** : tous les cas d'abus sexuel en ligne doivent être signalés au Centre européen d'expertise. Si la plateforme numérique néglige ses obligations et prend des mesures insuffisantes, une ordonnance de détection s'ensuit. Une ordonnance de détection exige que l'entreprise déploie une technologie de scanning pour détecter l'abus.
- **Centre d'expertise européen coordonné au niveau central** : celuic-ci reçoit tous les signalements et les transmet à la police pour complément d'enquête. Le centre peut également aider la victime à retracer les images.

3. Pourquoi est-il important de voter cette proposition dans son intégralité?

La proposition cible tous les types de services, y compris les services de discussions en ligne public et cryptées. Il est essentiel de soumettre tous les services au même régime pour éviter le déplacement du problème. En effet, Child Focus constate que l'exploitation sexuelle en ligne se déplace des plateformes publiques vers des groupes privés. Les auteurs connaissent les plateformes où commettre leurs abus. En proposant une application spatiale, nous envoyons un message clair aux auteurs: ne cherchez pas d'échappatoire.

Comparez les rapports du réseau social Facebook, qui utilise une technologie de détection automatique, et Instagram, par exemple, qui s'appuie sur des signalements. Les chiffres ne mentent pas : Facebook 21 165 208 contre Instagram 5 007 902 ou WhatsApp 1 017 555. Ces chiffres devraient être divisés différemment en tenant compte de la popularité de ces différentes plateformes.

4. Quelle est la position des autres pays ?

Child Focus s'inquiète profondément du manque de soutien d'un certain nombre de pays au projet de loi, y compris celui du gouvernement belge. Le débat semble se réduire à une discussion technologique sur le cryptage et la protection de la vie privée, sans tenir compte des intérêts de l'enfant. Bien entendu, Child Focus se préoccupe de notre vie privée. Mais le projet de loi établit un bon équilibre entre la protection des enfants et la protection de la vie privée. D'ailleurs, selon un sondage récent de l'Eurobaromètre, 73% de la population belge soutien cette proposition.

5. ***Pourquoi y a-t-il une opposition ?***

Comme pour toute proposition, il y a des partisans et des opposants. Dans le cas présent, l'opposition vient de l'angle commercial et de la protection de la vie privée. Les géants du numérique devront prendre des mesures concrètes impliquant des dépenses financières. L'opposition vient également du côté des défenseurs de la vie privée, qui ont ouvert la voie au sein de l'UE depuis la directive sur la protection de la vie privée. Ils estiment que la proposition actuelle pourrait violer la vie privée en raison de la possibilité de détection des messages cryptés. Child Focus estime que la protection des enfants doit devenir une priorité absolue. Derrière chaque image d'abus sexuel se cache un enfant victime qui a lui aussi droit au respect de sa vie privée.

AUTRES RÉGLEMENTATIONS

1. ***Qu'est-ce qui existe déjà en Europe en termes de législation ?***

Ces dernières années, l'Union européenne n'a pas pris la plume :

- La Commission européenne fait de la lutte contre l'abus sexuel d'enfants une priorité. Le 24 juillet 2020, la stratégie de l'UE pour une lutte plus efficace contre l'abus sexuel d'enfants a été publiée, visant notamment à réviser la directive 2011/93/CE de 2011 (directive sur l'abus sexuel d'enfants).
- Règlement intérimaire du 14 juillet 2021 (2021/1232/UE) portant dérogation temporaire à certaines dispositions de la directive 2002/58/CE relatives à l'utilisation de technologies par des fournisseurs de services de communication interpersonnelle indépendant du numéro pour le traitement de données à caractère personnel et d'autres données en vue de lutter contre l'abus sexuel d'enfants en ligne.
- Le 5 juillet 2022, la loi sur les services numériques (Digital Services Act) est entrée en vigueur avec un large cadre pour réguler le marché numérique. Elle contient des règles relatives à la sécurité en ligne des enfants, telles que des mesures de lutte contre les contenus illégaux.
- La stratégie européenne pour un meilleur internet pour les enfants (BIK+) a été publiée le 11 mai 2022 et vise à garantir des expériences numériques sûres et l'autonomisation numérique des enfants.

La présente proposition découle de la stratégie UE 2020. Par rapport à d'autres textes législatifs, celle-ci impose aux fournisseurs de services numériques un cadre opérationnel assorti d'obligations de grande portée.

2. ***Que se passe-t-il si le règlement n'est pas voté ?***

Si le règlement n'est pas voté, il ne sera plus possible de détecter l'abus sexuel en ligne dans les discussions en ligne. Nous en avons déjà ressenti les effets à la fin de l'année 2020. À l'époque, notre organisation mère NCMEC, la Cybertipline américaine, a constaté une forte baisse de 58 % des signalements d'exploitation sexuelle en ligne, non lié à la diminution de cas, mais plutôt à un changement. META, l'entreprise qui a enregistré le plus grand nombre de signalements, ne détectait plus les signalements d'abus sexuels liés à des utilisateurs européens, car ils n'avaient pas de mandat légal.

3. ***Quelle est la différence entre le règlement européen et la législation américaine actuelle ?***

La proposition s'inspire largement de NCMEC, la Cybertipline américaine, où le signalement des images et des cas d'abus sexuel en ligne est exigé par la loi. NCMEC rassemble tous les signalements et les transfert à Europol. Elle va également plus loin : outre le signalement obligatoire à un centre

d'expertise européen, il existe également un devoir de détection des acteurs numériques qui négligent leurs responsabilités. Le centre d'expertise européen identifiera à cette fin une technologie de scanning.

4. ***Pourquoi la loi sur les services numériques (DSA, Digital Services Act), en tant que cadre législatif, est-elle insuffisante dans la lutte contre l'exploitation sexuelle en ligne ?***

Le 5 juillet 2022, la loi sur les services numériques (Digital Services Act, DSA) est entrée en vigueur avec un large cadre pour réguler le marché numérique. Elle contient des règles relatives à la sécurité en ligne des enfants. Cette loi forme une base quant à la responsabilisation des fournisseurs de services numériques, ce qui constitue déjà un pas important dans la bonne direction. Si les fournisseurs de services ne prennent pas de mesures pour empêcher les contenus illégaux d'être supprimés sur leurs serveurs, ils ne seront plus exonérés de leur responsabilité.

L'une de ces mesures est la mise en place de mécanismes de signalement clairs et adaptés aux enfants. Cette mesure est sans aucun doute importante pour les adolescents dont les images intimes sont diffusées sous de faux prétextes ou sans leur consentement. Le problème est que les victimes d'abus sexuel d'enfants sont à plus de 90 % des enfants pré-pubères. Dans la base de données d'Interpol, 40 % des 7 millions de dossiers concernent des jeunes enfants. Si nous voulons sauver et protéger ce groupe d'enfants, nous devons déployer une technologie de scanning.

5. ***Pourquoi ne pas se contenter de maintenir le règlement intérimaire, en autorisant la détection volontaire, comme le demandent certaines entreprises et certains experts ?***

Le règlement intérimaire n'a jamais eu pour objectif de devenir une loi structurelle, d'où sa nature temporaire. Il restreint un certain nombre de fournisseurs de services de communication interpersonnelle, laissant de côté de nouveaux acteurs. Surtout, la détection volontaire ne suffit pas à résoudre efficacement le problème des abus sexuels en ligne. Premièrement, la grande majorité des signalements proviennent d'une poignée de fournisseurs de services, alors qu'il est clairement établi que le problème ne se limite pas à une seule plateforme : 95 % des signalements aux États-Unis proviennent de META. Deuxièmement, les messages cryptés n'entrent pas dans le champ d'application, ce qui entraîne une forte sous-déclaration. Les chiffres ne mentent pas : Facebook 21 165 208 contre WhatsApp 1 017 555.

TECHNOLOGIE DE NUMÉRISATION & PROTECTION DE LA VIE PRIVÉE

1. ***Comment la technologie fonctionne-t-elle ?***

Il existe déjà sur le marché plusieurs types de technologies capables de détecter des images d'abus sexuels. Il est possible de combiner ces méthodes.

- Les plus courantes sont le hachage de fichiers (*file hashing,* par exemple SHA-1) et le hachage perceptuel (*perceptual hashing,* par exemple photo ADN), utilisés pour la détection **d'images d'abus sexuels connues** (+/- 15 ans). Un hachage est une empreinte numérique d'une image. La technologie de scanning est automatisée et compare les images sur le net avec des images connues d'abus sexuel sur la base d'un calcul numérique. La technologie n'est pas en mesure de reconnaître ou d'analyser les images. Ces technologies sont largement utilisées. Child Focus travaille également avec ce type de technologie dans le cadre d'Arachnid, le projet du Centre canadien pour la protection de l'enfance. Arachnid a déjà passé au crible 160 milliards d'images.

- L'intelligence artificielle (+/- 5 ans) est relativement nouvelle sur le marché. Les classificateurs d'IA combinent différentes techniques pour détecter de **nouvelles images d'abus sexuels.** Cette technique de scanning est automatisée et ne permet pas de reconnaître ou d'analyser les images. Elle fonctionne sur le principe d'une arborescence : oui/non. Vous pouvez déterminer la fiabilité de la technologie. Plus elle est précise, plus la détection des images d'abus sexuel est faible. Une fiabilité de 99,9 % génère toujours une détection de 84 %. Avec une fiabilité élevée, la probabilité de faux positifs (une image légitime détectée à tort) et de faux négatifs (une image illégale non détectée) est plus faible.
- La sœur du classificateur d'IA est le classificateur de texte, qui détecte les modèles de **grooming** sur la base de 9 catégories.

2. ***Pourquoi la technologie de scanning est-elle nécessaire ?***

L'ampleur des abus sexuels en ligne atteint des proportions stupéfiantes. Internet est rempli de milliards d'images de victimes connues. Et des milliers de nouvelles images sont ajoutées chaque jour en un claquement de doigts. Prenons l'exemple d'une petite fille belge de 10 ans abusée par son père. Ses images ont déjà été retrouvées dans 190 000 fichiers de 12 900 criminels. La police, les organisations d'aide, les victimes et les citoyens travaillent jour et nuit pour nettoyer internet et protéger les victimes. Il s'agit de passer la serpillière en laissant couler le robinet, car toutes les mains jointes n'arrêtent pas l'eau qui coule. Nous avons besoin d'une technologie de scanning afin d'empêcher la recirculation d'images déjà connues, de détecter les images connues et les nouvelles images, et de faire la distinction entre les images dont la victime est connue et celles dont la victime est inconnue.

3. ***Quand la technologie de scanning peut-elle être déployée ?***

La technologie de scanning peut être utilisée à différents stades :

- La phase de téléchargement : empêcher les images d'abus sexuel de circuler sur internet.
- La phase de diffusion : rechercher des images sur le net.
- Sur le téléphone (*scanning-on-device*) : détecter des images avant le cryptage.

4. ***Toutes les images sont-elles scannées ?***

La meilleure comparaison que l'on puisse faire est celle avec un radar de vitesse. Toutes les voitures sont éligibles, mais seuls les conducteurs roulant au-dessus de la vitesse autorisée sont flashés.

5. ***D'autres images intimes, par exemple celles d'adultes, sont-elles également retenues par cette technologie de scanning ?***

Aucune technologie n'est parfaite. Il y a toujours un risque qu'une image soit injustement retenue ou qu'une image illégale ne soit pas retenue. Il est possible de réduire ce risque en augmentant la fiabilité. La technologie n'est pas capable de voir l'image comme vous et moi la voyons. Si une image est injustement retenue, elle sera à nouveau diffusée après vérification. Il s'agit d'un petit inconvénient pour un grand bénéfice social.

6. ***Cette technologie va-t-elle filtrer tout ce qui se trouve sur un appareil (client side scanning) ?***

Le CSS ou client side scanning est une application dans laquelle une technologie automatisée est intégrée à l'appareil, ce qui permet de détecter les images d'abus sexuel avant même le cryptage. La

technologie est automatisée et ne retient que les images qui correspondent à des images d'abus sexuel.

7. Cette technologie est-elle sûre ?

La technologie de scanning est suffisamment sûre et fiable pour permettre la détection d'images connues et nouvelles d'abus sexuel d'enfants, ainsi que des structures de grooming. Plus que pour d'autres types de matériel, comme les logiciels malveillants (*malware*) et le *spam*, de nombreux mécanismes de contrôle sont prévus, car les images d'abus sexuels contiennent des informations très sensibles. Toute technologie comporte un risque, mais en élaborant des politiques judicieuses, nous atténuons les risques.

8. Comment ce cadre contribue-t-il à la sécurité ?

Contrairement à ce qui se passe aujourd'hui, où ce sont les entreprises numériques elles-mêmes qui déploient la technologie de scanning sur une base volontaire, le règlement prévoit actuellement une utilisation fortement encadrée. La décision incombe à une autorité judiciaire lorsqu'il existe des preuves d'un "risque significatif d'utilisation du service à des fins d'abus sexuels en ligne sur des enfants", tels qu'une hausse de signalements par les utilisateurs. Plus qu'avant, l'utilisation de la technologie de scanning fera l'objet de contrôles. Les ordonnances de détection sont créées en coopération avec l'autorité de protection des données et le Centre de l'UE, sont limitées dans le temps, neutres sur le plan technologique et ciblées. En revanche, le règlement contribue beaucoup plus à une utilisation sûre de la technologie. Le centre européen surveille les technologies et, par l'intermédiaire d'un comité technique, peut les faire tester avant leur utilisation.

9. La vie privée des utilisateurs est-elle affectée de cette manière ?

Les dispositions sont le résultat d'un exercice d'équilibre entre l'intérêt de la vie privée et l'intérêt de la protection des enfants. Celles-ci fournissent de nombreuses garanties essentielles à la protection de la vie privée. Aujourd'hui, il existe déjà des technologies qui n'affectent pas la vie privée plus gravement qu'un simple antivirus ou un filtre anti-spam.

10. La technologie de scanning peut-elle être combinée avec le cryptage ?

Il existe trois options théoriques pour le scanning dans l'E2EE (*End-to-End Encryption*), chacune ayant ses avantages et ses inconvénients. La plus neutre est le *client side scanning*. Cette manière ne modifie pas la cybersécurité des environnements cryptés. Il s'agit d'une détection utilisée avant ou après le cryptage. De même, le CSS est utilisé pour le spam et les logiciels malveillants.

Il existe déjà aujourd'hui des techniques éprouvées qui peuvent davantage être testées et utilisées grâce au cadre précédent. Il s'agit également d'une incitation à développer les techniques de demain et à rester à l'avant-garde des nouvelles tendances.

11. Est-ce actuellement techniquement possible d'effectuer des analyses fiables ?

Il s'agit d'une technologie éprouvée, qui a été testée et est déjà déployée avec succès. Pour un déploiement/une commercialisation à grande échelle, les derniers obstacles doivent être levés. Plus la technologie est utilisée, mieux elle fonctionne et plus elle se rapproche de la perfection.

PARTIES IMPLIQUÉES

1. ***Quelles sont les parties concernées ?***

- Les prestataires de services électroniques de l'UE et des pays tiers fournissant des services dans l'UE
    - Analyse des risques trois mois après l'entrée en vigueur et mesures d'atténuation des risques.
    - Obligation de notification au centre de l'UE.
    - Des ordres de retrait lorsque les images d'abus sexuel ne sont pas mises hors ligne en temps utile.
    - Ordonnances de détection lorsque l'entreprise ne prend pas de mesures ou prend des mesures insuffisantes.
    - Point de contact central dans l'UE, y compris pour les entreprises de pays tiers offrant des services dans l'UE.
- Autorités de coordination au niveau de chaque État membre:
    - Pouvoirs d'enquête.
    - Assistance aux victimes dans le cadre de la détection d'images d'abus sexuels.
    - Pouvoirs d'exécution.
    - Coopération avec les autorités de coordination des autres États membres.
- Centre d'expertise de l'UE:
    - Base de données des indicateurs d'exploitation sexuelle en ligne (y compris des listes de hachages (*hashes*) d'images d'abus sexuels connus) .
    - Traitement des rapports des fournisseurs de services électroniques.
    - Cellule d'expertise.
    - Recherche proactive d'images d'abus sexuel des victimes.

2. **Quel est le rôle des réseaux sociaux ?**

Les réseaux sociaux doivent procéder à une analyse approfondie des risques liés à leurs services, élaborer des politiques de sécurité et prendre d'autres mesures pour prévenir les abus sexuels en ligne. Si elles ne le font pas ou si les mesures ne fonctionnent pas correctement, elles peuvent recourir à une ordonnance de détection pour résoudre le problème. Après la détection, ils peuvent prendre de nouvelles mesures pour réduire le risque.

3. ***Quel est le rôle de la police ?***

La police est à la fois rapporteur et destinataire des signalements. La police et d'autres organisations spécialisées signaleront les cas d'abus sexuel en ligne aux fournisseurs de services électroniques. La police, en tant qu'autorité compétente, recevra les signalements du centre européen et les analysera pour identifier les auteurs et les victimes. De nouvelles images peuvent être incluses dans la liste d'indicateurs du centre européen après ratification par les autorités compétentes, ce qui permet à la technologie de scanning de détecter la diffusion de nouvelles images.

4. ***La police ne sera-t-elle pas surchargée de signalements erronés ?***

Le centre européen filtrera tous les signalements manifestement infondés et les transmettra aux services de police compétents en fonction de la juridiction territoriale. La gestion centralisée permettra d'éviter les doubles emplois. Europol gardera également un œil sur les dossiers impliquant plusieurs districts de police.