

Apple montre l'exemple ?

En 2020, le National Center for Missing and Exploited Children a recensé près de 21 millions de signalements liés à des contenus précriminels sur internet. Parmi ses multiples signalements, seulement 265 proviennent d'Apple, contre plus de 20 millions pour le réseau social Facebook. Pour faire face à ces contenus abusifs, Apple avait annoncé le 5 août 2021 intégrer à ses futurs appareils un système d'analyse nommé CSAM (Child Sexual Abuse Material), qui consiste à hacher et signaler les contenus précriminels présents dans l'iCloud de ses utilisateurs.

■ *Le système Child sexual abuse material*

Début août 2021, Apple avait révélé son nouveau système d'identification de contenu pédopornographique. La détection CSAM « hache » et filtre à l'aide de la technologie NeuralHash chaque contenu téléchargé sur l'iCloud. Chaque image est numérotée et classée selon qu'elle correspond ou non, à des données spécifiques fournies par le NCMEC à Apple. Si une image est repérée et présente plusieurs occurrences, elle est alors déplacée et un humain est chargé de vérifier il s'agit ou non de contenus interdits ou inappropriés. Si c'est le cas, il le signale au NCMEC, qui agit à son tour. En revanche, si la bibliothèque iCloud n'est pas activée, Apple n'a aucun moyen de vérifier et analyser les photos d'un utilisateur. Si l'iCloud est activé, Apple accède véritablement au contenu d'une image uniquement lorsque le « seuil » de correspondance des données est dépassé.



En plus de ce système de hachage, Apple avait annoncé développer de nouveaux outils pour les messages afin que les parents ou tuteurs d'un mineur puissent mettre en place un « contrôle parental ». Les parents reçoivent une notification si leur enfant envoie ou ouvre une photo à caractère sexuel. De son côté, le mineur est prévenu que le contenu est jugé inadapté et dangereux. Puis, s'il souhaite voir ou envoyer la photo, un autre écran l'informe qu'une notification sera envoyée à ses parents.

La détection CSAM faisant partie des systèmes d'exploitation des mobiles IOS 15 et iPadOS 15 devait être mise en place dès l'automne 2021 dans tous les États-Unis à partir de l'iPhone 6S et de la cinquième génération d'iPad.

■ Un système mal reçu par le grand public



Après l'annonce de la mise en place de ce système, des chercheurs informatiques américains et du monde entier se sont intéressés de près au projet.

Tandis que cette décision est perçue comme un véritable retournement de la part d'Apple, qui s'était jusqu'ici opposée aux autorités afin de défendre la vie privée de ses utilisateurs. Matthew Green, professeur à l'université Johns Hopkins et spécialiste en cryptographie, s'est exprimé sur Twitter quelques jours après la déclaration d'Apple. Selon lui, « ce type d'outil peut être très efficace pour détecter des contenus

pédopornographiques sur les téléphones ». Mais il n'a pas écarté l'idée des dérives possibles, « imaginez ce qu'un tel système pourrait permettre entre les mains d'un gouvernement autoritaire ». Ces craintes sont partagées par de nombreux chercheurs en cybersécurité, qui estiment eux aussi que cette technologie pourrait ouvrir la voie à une surveillance accrue des appareils personnels. Ils soutiennent malgré tous les efforts d'Apple dans la lutte contre les abus sexuels sur les enfants, mais redoutent que ce dispositif n'encourage certains gouvernements à réclamer un accès plus large aux données personnelles de leurs citoyens, au-delà des objectifs de base de l'entreprise.

Plusieurs experts internationaux en cybersécurité ont publié une étude de 46 pages, prouvant que selon eux, cette technologie de détection est non seulement inefficace, mais aussi « dangereuse ». Les chercheurs expliquent avoir entamé leurs travaux avant même l'annonce du projet en août. Leur inquiétude faisait déjà suite à des documents publiés l'année précédente par l'Union européenne, qui souhaite mettre en place un système similaire capable d'analyser des contenus liés aux abus sexuels sur mineurs, mais aussi au crime organisé et au terrorisme sur des appareils chiffrés. « L'extension des pouvoirs de surveillance de l'État franchit clairement une ligne rouge », a déclaré Ross Anderson, spécialiste en ingénierie de la sécurité et membre du groupe d'étude. Susan Landau, experte en cybersécurité et politiques publiques, a estimé que cette technologie permettrait « d'analyser un appareil personnel privé sans motif valable ». Elle a ajouté : « C'est extrêmement dangereux, tant pour les entreprises que pour la sécurité nationale, la sécurité publique et la vie privée. » Au-delà des enjeux de surveillance, les chercheurs affirment également que cette technologie est peu efficace pour identifier réellement les images d'abus sexuels sur mineurs. Quelques jours seulement après l'annonce d'Apple, certains internautes avaient déjà démontré qu'il était possible de contourner la détection en modifiant légèrement les images.

En plus d'être vivement critiqué par les spécialistes en cybersécurité du monde entier, Apple s'est rapidement trouvé au cœur d'une polémique, car le système fut jugé comme ne correspondant pas aux valeurs d'Apple par le grand public. En 2016, Apple était allé en justice avec le FBI, car l'entreprise a refusé l'accès à l'iPhone d'un suspect terroriste après une fusillade à San Bernardino, en Californie, maintenant sa réputation de lutte pour les droits de ses clients.

Sources :

- <https://www.developpez.com/actu/317447/Apple-envisage-un-systeme-de-detection-d-images-d-abus-d-enfants-dans-la-galerie-de-photos-des-utilisateurs-mais-les-chercheurs-en-securite-craignent-une-surveillance-de-masse-des-iPhone/>
- <https://www.kaspersky.fr/blog/what-is-apple-csam-detection/17541/>

■ Et aujourd'hui ?

L'Union européenne a repris le projet peu de temps après, dans le but d'imposer au géant de la tech de scanner automatiquement les contenus stockés et échangés sur les serveurs des plateformes numériques, afin de détecter les contenus pédopornographiques. Même si les associations de défense de la vie privée étaient parvenues à faire reculer l'Union européenne sur cette question, l'idée n'a pas été totalement abandonnée.

Comme le rapporte Euractiv, les discussions se sont poursuivies et le Conseil de l'Union européenne est finalement parvenu à un accord sur la méthode à adopter. Initialement, le projet visait à obliger les entreprises technologiques à intégrer des outils de détection automatique de contenus pédopornographiques sur les appareils et services cloud. Dans sa nouvelle version, le texte ne leur impose plus cette obligation. Néanmoins, cette possibilité demeure ouverte et chaque entreprise pourra choisir de mettre en place ce système si elle estime cela nécessaire.



Le texte doit encore être examiné par le Parlement européen, mais cette avancée constitue déjà une étape importante qui pourrait aboutir à l'adoption d'une législation à l'échelle européenne dans les prochains mois. Peter Hummelgaard, ministre danois de la Justice, considère déjà ce projet comme une mesure nécessaire dans la lutte contre les crimes sexuels visant les mineurs.

Source : <https://www.macg.co/services/2025/11/lue-pourrait-pousser-apple-reprendre-son-projet-de-surveillance-des-contenus-pedopornographiques-305281>

■ Que mettent en place Meta et Google ?

Depuis 2016, Meta organise des hackathons avec des ONG afin de développer des solutions pour renforcer la sécurité des enfants en ligne.

En 2020, Meta a participé au lancement de Project Protect, une initiative collaborative destinée à mieux protéger les mineurs sur Internet. L'entreprise analyse également les contenus abusifs dans le but de comprendre leur diffusion et de développer de nouveaux outils de prévention, notamment pour limiter les recherches de contenus pédopornographiques.



Voici les mesures principales mises en place sur Facebook et Instagram :

- Limitation des interactions entre adultes suspects et comptes d'adolescents.
- Suppression des recommandations de profils de mineurs.
- Blocage des commentaires et demandes de contact de comptes jugés suspects.
- Déploiement des alertes AMBER pour aider à retrouver des enfants disparus.

Meta rappelle également que ses politiques interdisent strictement tout contenu exploitant des mineurs. Le portail Take It Down, développé avec le NCMEC, permet aux victimes mineures de demander la suppression de contenus intimes diffusés en ligne.

■ Peu de résultats

Dans son dernier rapport annuel publié le 23 avril 2025, Internet Watch Foundation (IWF) alerte sur la forte augmentation des sites vendant des contenus pédopornographiques. Leur nombre a doublé en 1 an, passant de 7 028 en 2024 à 15 031 en 2025. Selon l'organisation britannique, ces plateformes permettent aux précriminels de générer facilement des revenus grâce à des contenus mettant en scène des mineurs de tous âges, dans les formes les plus graves d'abus sexuels.

L'IWF souligne également la hausse inquiétante de la sextorsion, qui consiste à menacer de diffuser des images intimes en échange d'argent. Les signalements liés à cette pratique ont augmenté de 127 % entre 2024 et 2025. Les adolescents de 14 à 17 ans sont les principales victimes, même si certains cas concernent des enfants beaucoup plus jeunes.

En France, le nouvel Office des mineurs (Ofmin), dirigé par Gabrielle Hazan depuis septembre, est chargé de lutter contre les violences faites aux enfants. La France figure parmi les pays hébergeant le plus de contenus précriminels au monde, derrière les États-Unis, la Russie et les Pays-Bas. Les signalements ont aussi explosé ces dernières années. Environ 3 200 en 2013 contre plus de 318 000 en 2023.

Gabrielle Hazan déplore également le manque de moyens face à l'ampleur du phénomène, indiquant que moins de 1 % des signalements reçus peuvent actuellement être traités.

Discussion

La question de la lutte contre les contenus pédopornographiques demeure donc au cœur du débat dans le monde entier. Faut-il privilégier la lutte contre la pédocriminalité, quitte à renforcer les mécanismes de surveillance numérique, ou préserver avant tout le respect de la vie privée et le chiffrement des communications ? Si, en 2021, une majorité semblait clairement favorable à la protection de la vie privée, le contexte actuel montre la détresse de la situation.

Rédigé par Marie-Charlotte Hugon