

Faculté de droit et de criminologie

Nouvelles images, nouvelles pratiques : les images d'abus sexuels sur mineurs à l'ère de l'intelligence artificielle

NOM et Prénom de l'étudiant.e :
CHARLIER Faustine
Promotrice : Devresse, Marie-Sophie
Année académique 2025-2026
Master à finalité approfondie

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 107 à 114 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment <http://www.uclouvain.be/plagiat>.

Engagement d'intégrité – Travaux écrits et mémoires d'étudiant.e.s

Je reconnais avoir pris connaissance des règles d'or de l'honnêteté intellectuelle ainsi que des Lignes directrices sur l'usage responsable des outils d'intelligence artificielle de l'UCLouvain (disponibles sur le site www.uclouvain.be/drt - page "règlements") et je m'engage à respecter les valeurs d'intégrité et d'honnêteté qui fondent les règles et recommandations adoptées au sein de la communauté universitaire.

En particulier :

Engagement sur l'authenticité de mon mémoire/travail écrit

- Je déclare sur l'honneur que j'ai préparé et rédigé moi-même ce mémoire/travail écrit.

Reconnaissance du plagiat comme faute

- Je suis conscient·e que le plagiat consiste à réutiliser d'autres documents et sources, même partiellement, sans mentionner le nom de l'auteur ni/ou de la source. Reproduire littéralement des passages d'un autre document, éventuellement traduits, sans les placer entre guillemets, même si l'auteur et la source de cette œuvre sont mentionnés, constitue également un plagiat.
- Je reconnais que le plagiat constitue une faute grave qui entraîne l'application de la section 7 des articles 87 à 90 du Règlement général des études et des examens (RGEE).
- Je m'engage à ce que mon mémoire/travail ne constitue pas une reprise, même partielle, d'un autre document publié ou non, attribué à une personne ou anonyme.

Engagement à citer mes sources

- Je m'engage à attribuer à leur(s) auteur(s) toutes les idées, informations, données sur lesquelles je m'appuie. Je m'engage à référencer tous les emprunts intégrés au mémoire/travail (sous la forme de phrases, graphes, cartes, schémas, tableaux, etc.). Les références (par exemple, en note de bas de page) sont conformes aux exigences académiques et scientifiques (telles que présentées dans les cours de méthodologie, les séances de formation liées au Séminaire d'accompagnement des mémoires en Master et les guides de citation).

Engagement quant à l'usage d'outils d'intelligence artificielle (IA) générative

- Je m'engage à utiliser les outils d'IA générative, en particulier les générateurs de textes, de manière responsable, comme complément de mon apprentissage et sans chercher à contourner les exigences académiques.
- Je m'engage à respecter les Lignes directrices relatives à l'usage responsable de l'IA générative. Elles m'obligent notamment à référencer adéquatement les outils d'IA lorsque je reprends de manière littérale les contenus qu'ils ont générés. En revanche, certains usages de ces outils, par exemple comme assistant linguistique (pour corriger l'orthographe, la syntaxe ou le style), ne doivent pas être mentionnés.
- Je suis conscient·e que les contenus générés par ces outils d'IA ne reflètent pas nécessairement les faits/sources et je m'engage donc à toujours vérifier l'exactitude de ces contenus dans une démarche scientifique.
- Je m'engage à respecter toutes les consignes spécifiques pour le travail/mémoire, ainsi que les exigences de transparence et de documentation du processus ayant abouti au travail/mémoire, notamment en sauvegardant les conversations avec ces outils d'IA.
- Je m'engage à fournir, sur demande, des explications sur la manière dont j'ai utilisé ces outils.
- Je reconnais que le non-respect de ces exigences et de l'intégrité académique peut constituer un abus et être considéré comme une irrégularité au titre des articles 107 et suivants du RGEE et entraîner des sanctions telles que prévues aux articles 111 et suivants du RGEE.

Remerciements

Nous tenons, à travers les quelques lignes qui vont suivre, témoigner notre reconnaissance pour toutes les personnes, qui de très près ou de très loin, ont contribué à la réalisation de ce mémoire.

Nous aimerions tout d'abord remercier notre Promotrice, Madame Marie-Sophie Devresse pour l'intérêt qu'elle a porté à notre sujet, son accompagnement, sa patience et ses conseils. Le mémoire tel qu'il se présente aujourd'hui n'aurait jamais vu le jour sans son aide précieuse.

Nous remercions également toutes les personnes qui ont tenté de nous relire et de nous corriger, surtout nos phrases remplies d'implicites. Sans vous, ce mémoire n'aurait pas la forme qu'il a aujourd'hui.

Nous éprouvons une grande reconnaissance pour les personnes qui ont accepté de me rencontrer et d'échanger avec nous sur notre mémoire. Vos contributions ont été essentielles pour notre réflexion.

Les acquis que nous avons gagnés grâce à la formation de Criminologie nous accompagneront, sans aucun doute, dans notre futur professionnel. Pour cela, nous remercions l'équipe académique de l'École de Criminologie.

Ce mémoire clôture un parcours académique, parfois scabreux, mais rempli d'expérience enrichissante, des expériences qui n'auraient jamais été possibles sans le soutien inconditionnel de nos proches, parents et grands-parents.

Le meilleur pour la fin, nous tenons à dire merci à nos amis pour les rires, les pleurs et surtout pour l'apport du soutien émotionnel nécessaire dans un parcours académique.

Table des matières

Liste des abréviations.....	1
Introduction.....	2
Partie 1. Présentation de l'objet	3
1.1. Définition de l'objet de recherche.....	3
1.2. Objectifs de recherche.....	3
Partie 2. Méthodologie.....	4
2.1. Type de recherche	4
2.2. Types de données recueillies et terrain de recherche.....	4
2.3. . Méthode de recueil de données et personnes rencontrées en entretien.....	5
2.3.1. Le recueil des données	5
2.3.2. Les personnes rencontrées	6
2.4. Limitations de l'étude	7
2.5. Précisions quant à l'utilisation de l'IA dans un travail de recherche.....	9
Partie 3. L'abus sexuel sur mineurs : d'une image à l'autre.....	9
3.1. L'image à l'ère du numérique.....	9
3.2. Les images d'abus sexuels sur mineurs	11
3.2.1. Une problématique récente	11
3.2.2. Une définition en évolution	13
3.2.3. Des victimes : les mineurs	13
Partie 4. Le déploiement de l'intelligence artificielle.....	14
4.1. La toile de fond de l'intelligence artificielle.....	14
4.1.1. Aux fondements d'Internet et de la cybercriminalité	15
4.1.2. La naissance de l'intelligence artificielle.....	16
4.2. L'intelligence artificielle comme vecteur de nouvelles formes de criminalité..	18
4.2.1. Typologie des intelligences artificielles.....	18

4.2.2.	La criminalité numérique à l'ère de l'intelligence artificielle	20
4.2.3.	Une rencontre inquiétante : le cas des MASE	21
4.2.4.	L'émergence d'une nouvelle criminalité	24
4.2.5.	Des préjudices considérables	26
Partie 5. Un véritable marché sous-terrain.....		27
5.1.	Les plateformes : un lieu privilégié de distribution de MASE	28
5.1.1.	Le Clear Web et le Dark Web.....	28
5.1.2.	La face visible	29
5.1.3.	La face cachée.....	34
5.2.	La consommation.....	36
5.2.1	Un « accident » aux lourdes conséquences	36
5.2.2.	Les MASE : quand l'horreur devient rentable.....	38
5.3.	Les MASE sans frontières	39
Partie 6. État des lieux réglementaire		41
6.1.	Les instruments universels.....	41
6.2.	Les normes européennes	44
6.2.1.	Le cadre général des MASE dans l'espace européen	44
6.2.2.	Réguler l'espace numérique : une course contre la montre	45
6.3.	Les normes belges.....	48
6.4.	Des dispositions légales fragiles	49
6.4.1.	Chat Control 1.0 : beaucoup de bruit pour rien ?	49
6.4.2.	Les IA MASE : penser l'impensable	52
Partie 7. La réaction sociale aux phénomènes		53
7.1.	L'itinéraire des images d'abus sexuels sur mineurs	53
7.1.1.	Les techniques de détection	53
7.1.2.	La modération : une tentative de maîtriser les excès	57
7.2.	La prévention : une urgence de santé publique.....	58

7.2.1.	La prévention dans l'espace social	59
7.2.2.	La prévention auprès des auteurs d'infractions à caractère sexuel en ligne 60	
7.3.	L'IA et la santé mentale : symbiose ou antibiose ?.....	60
Conclusion		62
Bibliographie.....		63

Liste des abréviations

Afin de faciliter la lecture, nous avons élaboré une liste d'abréviations ayant pour but d'alléger le texte.

DSA = Digital service act – règlement sur les services numériques

IA = intelligence artificielle

IA MASE = images d'abus sexuels générées ou modifiées par IA

ICSE = International Child Sexual Exploitation

IWF = Internet Watch Foundation

LLM = large language model

MASE = matériel d'abus sexuels sur mineurs (images d'abus sexuels sur mineurs)

NCMEC = National Center for Missing and Exploited Children

P2P = peer-to-peer

RS = réseaux sociaux

TIC = technologie de l'information et de la communication

TOR = the onion router

Introduction

À travers le monde, neuf millions d'images d'abus sexuels sur mineurs (ci-après MASE) sont échangées chaque jour. Parmi, la quantité d'images disponible sur Internet, une partie de plus en plus importante est générée ou modifiée par intelligence artificielle. Une pratique qui touche des mineurs, individus considérés comme particulièrement vulnérables à l'ère du numérique. De nombreux réseaux sociaux sont concernés par ces partages d'images : Instagram, Tiktok, Facebook ou encore Whatsapp. À l'aube de l'année 2025, le chat bot Grok, l'intelligence artificielle développée par l'homme d'affaires Elon Musk a fait grand bruit pour sa capacité à créer du contenu pornographique ou à dénuder des individus. Ces pratiques, rapidement dénoncées par des internautes, ont illustré la facilité pour des individus à générer artificiellement des images pornographiques avec un nombre alarmant de celles-ci visant des mineurs. Face à cette situation inédite, de nombreuses inquiétudes et questions ont secoué la société civile et le monde académique. Dès lors, quelles sont les reconfigurations vécues par l'avènement de l'intelligence artificielle dans le domaine des abus sexuels sur mineurs ? Comment la Belgique doit-elle s'armer face à ce phénomène apparemment sans contrôle qui semble créer une criminalité nouvelle ? Une criminalité est laissée entre les mains de personnes expérimentées ou non, qui font une mauvaise utilisation des outils technologiques.

Notre sujet de recherche a pour but d'éclairer la question des images d'abus sexuels sur mineurs à l'ère de l'intelligence artificielle, ainsi que toutes les difficultés que ce phénomène implique. Pour explorer cette thématique, nous avons effectué une recherche qualitative inductive appuyée par trois entretiens exploratoires avec des acteurs de terrains dont des membres de la police, de Child focus et un criminologue de parquet. Dans un premier temps, ce travail envisage la complexité inhérente à la définition d' « images d'abus sexuels sur mineurs » pour comprendre le cadre dans lequel émergent ces contenus générés ou modifiés par l'intelligence artificielle. Ensuite, nous retraçons brièvement l'historique d'Internet et de la criminalité envers les mineurs pour délimiter un champ d'action dans lequel l'IA a pris place. Cette criminalité sera ensuite analysée afin de comprendre en quoi elle fonctionne comme un rouage d'un système économique. Une autre partie de ce mémoire sera conséquemment dédiée à l'examen des normes législatives impactant la définition et la gestion des MASE. Enfin, la dernière partie de ce travail abordera l'impact de ce phénomène sur les technologies mises en place pour tenter d'éradiquer les matériels d'abus sexuels sur mineurs.

Partie 1. Présentation de l'objet

1.1. Définition de l'objet de recherche

Comme beaucoup, nous avons peut-être déjà tous partagé ou connaissons quelqu'un qui a partagé des photos de son enfant ou d'un enfant qu'il connaissait sur les réseaux sociaux sans jamais se demander quelle vie aurait cette simple photo partagée en quelques secondes. Cette pratique apparemment sans incidence permet pourtant de nourrir un marché profondément remanié avec l'avènement de l'intelligence artificielle. Nous avons donc choisi d'envisager de manière inductive l'impact de l'IA sur les images d'abus sexuels sur mineurs. Le domaine touchant aux dynamiques de déviance sexuelle a toujours suscité un vif intérêt dans notre parcours académique et ce début le bachelier. Nous voulions également donner à cet objet un tournant actuel, raison pour laquelle nous avons décidé d'étudier l'impact d'une technologie sur cette question.

En parcourant la thèse de F. Fortin (2014) présentée dans le cadre du cours d'Introduction à la science forensique à l'Université Catholique de Louvain-la-Neuve par la professeure Bitzer Sonja, nous avons découvert que les problèmes liés à la distribution, la consommation, la détention d'images avaient connu un tournant majeur avec Internet. C'est donc naturellement que la question de l'impact de l'intelligence artificielle s'est installée au centre de notre réflexion.

Les images d'abus sexuels sur mineurs seront référencées à travers ce mémoire avec l'acronyme MASE, l'équivalent de « matériel d'abus sexuels sur enfants ». Nous avons choisi de nous référer à l'acronyme français dans un souci de cohérence avec les recherches francophones.

Pour un souci de neutralisation des données à caractère personnel et de neutralisation des sources scientifiques, nous opterons pour une écriture accordée au masculin.

1.2. Objectifs de recherche

Dans cette section, nous présenterons de manière synthétique les objectifs poursuivis. Nous voulons à travers ce travail soulever des questionnements relatifs à la conception de l'image à l'ère de l'intelligence artificielle. De ce fait, l'objectif principal de notre recherche est de découvrir comment l'avènement de l'intelligence artificielle a reconfiguré les images d'abus sexuels sur mineurs et leur traitement. Pour ce faire, nous avons exploré plusieurs thèmes de recherche, dont la croissance, l'accessibilité/la facilité, les images réelles vs les images non réelles, la consommation, la distribution, la détention... La volonté était de questionner et d'interroger ces thématiques au regard de l'IA. L'angle

choisi concerne donc en majorité les images, notre étude ne comprend que très peu d'informations sur les vidéos et les textes générés par IA.

Notre recherche tend à fournir un panorama francophone de notre problématique. À travers l'exploration de la littérature, nous avons constaté que très peu de documentations en langue française encadraient notre sujet, surtout concernant l'établissement d'un véritable enjeu économique.

Partie 2. Méthodologie

2.1. Type de recherche

Pour ce faire, notre recherche est construite sous la forme d'une analyse inductive dans une recherche qualitative en criminologie. Selon M. Blais et S. Martineau (2022), l'analyse inductive convient pour traiter les données portant « des objets de recherches à caractères exploratoires ». À travers cette analyse, il est question de passer du spécifique au général afin d'aboutir à une idée par un processus « de généralisation et non par une vérification d'un cadre théorique pré-établi » (*Ibid.* ; Rigaud et al., 2017). C'est pourquoi le choix de l'analyse inductive fait sens dans une recherche où il n'existe encore que très peu de recul sur l'objet (Coman et al., 2022). La complexité de notre question de recherche nous a conduit à choisir une approche qualitative avec la récolte d'entretiens semi-directifs à visée exploratoire. Nos choix ont été également guidés par la littérature et par la faisabilité des entretiens.

Dans nos réflexions de départ, nous avons cherché à comprendre comment évoluent l'image et son exploitation, notamment à travers l'arrivée de l'intelligence artificielle. En outre, nos réflexions sur la thématique des images d'abus sexuels sur mineurs générées ou modifiées par IA impliquent de se questionner sur l'éthique d'une telle technologie, sur son utilisation dans une portée criminelle et sa réorganisation l'IA réorganise quant à la production et la consommation des CSAM. Nous attendons de notre recherche de terrain qu'elle puisse nous informer de l'expérience professionnelle des personnes travaillant dans ce domaine et des difficultés rencontrées concernant les MASE à l'ère de l'IA. Pour percevoir au mieux ces potentielles transformations, nous avons choisi d'explorer le terrain de la police et des criminologues de parquet, de même que le terrain associatif, en particulier avec Child Focus.

2.2. Types de données recueillies et terrain de recherche

Pour la réalité de terrain des acteurs œuvrant dans le domaine des CSAM, nous avons choisi de recueillir des données qualitatives issues des expériences ou pratiques professionnelles dans les milieux judiciaire, associatif et policier.

Dans le milieu judiciaire, nous avons rencontré une personne travaillant comme criminologue de parquet, il nous semblait important également d'explorer le domaine policier pour mieux cerner la réalité de terrain des travailleurs confrontés directement à l'impact de l'intelligence artificielle. Dans ce cadre, nous avons eu l'occasion de rencontrer des personnes dont le terrain d'action se situe sur Internet. Enfin, pour le milieu associatif, nous avons choisi de contacter des représentants de Child Focus en raison de son domaine d'action qui est l'exploitation sexuelle d'enfant dont les images d'abus sexuels sur mineurs.

2.3. Méthode de recueil de données et personnes rencontrées en entretien

2.3.1. Le recueil des données

Dans cette recherche, les entretiens exploratoires sont entendus comme « [un] but, non de démontrer des hypothèses déjà bien établies par le chercheur, mais plutôt d'inventorier un champ social encore mal connu de lui, dans un but de découverte » (Bréchon, 2011, p.215). Ces derniers serviront à venir appuyer la récolte de données théoriques effectuée en amont et pendant la période de réalisation des entretiens. Les entretiens exploratoires donnent notamment l'opportunité de se familiariser avec le terrain et de construire la problématique de manière progressive. C'est pourquoi nous avons choisi ce type d'entretien pour notre sujet. En effet, la thématique des images d'abus sexuels sur mineurs est certes exploitée par la littérature, mais l'impact de l'IA sur ce phénomène n'est que très récent. L'objectif était d'explorer, découvrir et apprivoiser cette thématique à travers la littérature scientifique et la littérature grise (Marquet et al., 2022).

Pour traiter nos données, nous avons choisi de suivre la théorie développée par les sociologues S. Beaud et F. Weber (2002). Cette méthode indique qu'une transcription aménagée des entretiens combat les biais d'objectivité scientifique qui endommagent les nuances par rapport à une retranscription complète. Nous avons donc choisi la retranscription aménagée, car elle nous a permis de sélectionner les informations les plus pertinentes selon la problématique qui nous occupe. Elle permet aussi d'épurer le texte et ainsi de faciliter la lecture. Notons que ce processus doit s'effectuer en veillant à ne pas appauvrir le discours des personnes rencontrées.

Le phénomène que nous avons cherché à explorer au travers de nos entretiens se situe dans les pratiques policières, judiciaires et associatives. La police et la pratique judiciaire offrent un regard répressif sur la question. Les secteurs associatifs font de la prévention et envoient les signalements reçus à la police, pour débiter des investigations. Les organismes interviennent également dans la prise en charge des victimes. Par l'exploration de la littérature, nous avons estimé que ces trois angles nous donnaient l'opportunité de fournir un aperçu global et complet. Les acteurs qui dépendent de ces

organisations sont en contact direct avec notre phénomène. Une liste anonymisée des personnes rencontrées se trouve en annexe (Annexe B), mentionnant leurs rôles respectifs.

Pour réaliser nos entretiens exploratoires, nous avons contacté les acteurs qui nous semblaient pertinents pour approfondir la thématique des images d'abus sexuels sur mineurs. Afin de mener ces entretiens, nous avons construit des guides d'entretien sous forme de liste thématique. Les thèmes ont été choisis sur la base de la lecture et de l'exploration de la littérature. Ce type de guide donne l'opportunité à la discussion de se développer et de pouvoir s'adapter à la personne interrogée (Kalika et al., 2023). La rédaction des guides était adaptée en fonction des acteurs que nous allions rencontrer. Nous avons donc contacté une série d'acteurs de terrain par e-mail ou par formulaire Internet. Parmi la quinzaine de demandes d'entretien, nous avons pu en réaliser seulement trois. Nous tenons à préciser que, dans certains cas, même si nous n'avons pas pu obtenir l'accord pour un entretien, nous avons toutefois reçu des documents de la part de certaines associations. C'est le cas notamment pour *We protect global alliance*, association de protection de l'enfance face aux dangers de l'exploitation sexuelle en ligne.

Afin d'analyser nos entretiens exploratoires, nous avons opéré une écoute attentive de nos enregistrements. Grâce à cette écoute active et en nous aidant de la prise de notes réalisée durant les entretiens, nous avons pu identifier des extraits qui nous paraissaient pertinents pour venir appuyer la littérature choisie. Nous avons donc effectué des fiches synthétiques reprenant les extraits intéressants. Ces derniers ont été à nouveau épluchés pour n'en faire ressortir d'une dizaine. Ce type d'analyse, comme appuyée par Kaufmann, peut prendre vie dans les « situations intéressantes, informatives, épisodes intrigants, catégories de pensées indigènes, mais bien argumentées, éléments proches des hypothèses en cours d'élaboration » (Kaufmann & Singly, 1996, p. 81). Notre méthode d'analyse se trouve en Annexe (Annexe A). Ce processus s'est construit au fur et à mesure de l'élaboration de la partie théorique de notre mémoire. Nous avons grâce aux notes prises durant nos entretiens et à l'écoute active des enregistrements pu orienter notre recherche bibliographique sur le sujet. Les entretiens exploratoires ont fait émerger des thématiques pertinentes que nous avons ensuite articulées dans notre mémoire. S. Beaud et F. Weber (2003) estiment qu'une écoute active catalyse des pistes de recherches au cours de notre enquête de terrain (Sifer-Rivière, 2023).

2.3.2. Les personnes rencontrées

Nos trois entretiens se sont déroulés d'abord avec des membres de la police, ensuite avec une personne désignée comme « conseiller politique » de Child focus, et enfin, un criminologue de parquet.

Tout d'abord, un entretien collectif a été réalisé avec la direction centrale de la lutte contre la criminalité grave et organisée de la police¹, plus précisément avec le secteur « child abuse ». Ont participé à cet entretien, le représentant de Child Abuse de la police fédérale, la personne qui lui succède à ce poste, un expert en computer crime unit et enfin, un expert en OSINT, opérant aussi sur le Dark web. Le rôle de l'OSINT « consiste au recueil et à l'analyse d'informations émanant de sources publiques » (*Le Renseignement de Sources Ouvertes : Qui et Pourquoi ?*, 2024). Ensuite, nous avons pu échanger avec une personne appelée « conseiller politique » au sein de l'organisme Child focus. Enfin, nous avons également rencontré un criminologue de parquet. Ces personnes sont concernées par des étapes différentes dans la trajectoire des MASE. La police fédérale a un rôle au niveau de l'enquête et de la détection. Child focus arrive plutôt au niveau du signalement et réapparaît au niveau de la prise en charge des victimes. Le parquet quant à lui intervient dans la poursuite judiciaire. Cette pluralité d'acteurs a, selon nous, permis d'aborder divers aspects de notre problématique.

Nous avons également rencontré une personne dans la police chargée des technologies de l'Information et de la Communication (TIC) policières. Cette rencontre nous a permis de recueillir des informations concernant les processus législatifs des CSAM, et nous a permis d'obtenir des contacts dans le domaine policier.

2.4. Limitations de l'étude

Au cours de la conception de ce mémoire, différentes difficultés et limites nous sont apparues. Cette partie vise à présenter succinctement et de manière réflexive les principaux obstacles rencontrés lors de nos recherches. Ensuite, il sera question d'évoquer les démarches qui ont été mises en place pour pallier ces contraintes externes.

L'adoption d'une méthode inductive pour l'analyse qualitative de contenu nous a amenés à réfléchir à la place de la posture de recherche adoptée dans ce travail. Tout d'abord, l'utilisation d'une méthode qualitative inductive nous engage à présenter uniquement un aspect exploratoire fondé sur un phénomène. Cependant, l'inductif ne permet pas toujours de baliser au mieux la recherche, entraînant le chercheur à se perdre dans le travail théorique (Coman et al., 2022). Au départ, notre recherche était orientée sur l'IA comme technique de détection et de production de CSAM et notamment sur la manière dont elle pouvait aider les acteurs de terrain. Dans ce but, nous avons préalablement rencontré des membres de la police qui, pour des raisons de sécurité, ne pouvaient pas nous dévoiler les techniques actuellement utilisées. En réaction à cet obstacle, nous avons élargi notre recherche pour nous diriger vers

¹Pour plus d'informations, nous renvoyons le lecteur sur le site Internet suivant : <https://www.police.be/5998/fr/propos/police-federale/police-judiciaire-federale/direction-centrale-de-la-lutte-contre-la>

une analyse axée également sur l'IA en tant que génératrice d'images, et pas uniquement sur la détection. L'approche abandonnée aurait également abouti à un mémoire orienté du côté de la science forensique ou à une analyse purement technique qui serait cependant intéressante à approfondir dans une prolongation de cette recherche. De ce fait, l'adoption d'une méthodologie qualitative nous permet de contourner cette difficulté inhérente à la composition floue du terrain étudié et à la nature nébuleuse de l'IA (Muchielli et al., 2009). Cette thématique suppose la compréhension de sujets qui sortent du domaine proche de la criminologie, surtout en ce qui concerne l'explication technique des différentes formes d'intelligence artificielle et de leurs spécificités d'utilisation. Ainsi, nous avons conscience qu'une de nos limites réside dans l'exploitation de la littérature scientifique propre à l'IA. Nous tenons également à rappeler que selon Donna Haraway, tous les savoirs sont situés dans un contexte social, économique, géographique et historique (Haraway, cité par Lépinard & Lieber, 2020). La réalisation de ce mémoire apparaît donc en plein milieu de l'expansion du phénomène. Cela implique un recul moindre sur la question et une applicabilité moindre de cette étude dans un moyen long terme.

Pour contacter des professionnels, nous avons dû parfois remplir des formulaires sur Internet, car nous n'avions pas de contact direct avec les personnes souhaitées. Cela implique que nous n'avons pas la certitude que l'e-mail a été lu. Notons que la première demande réalisée a porté ses fruits et nous avons pu rencontrer des membres de la police judiciaire. La police est souvent un milieu fermé qui s'ouvre peu aux extérieurs. Nous sommes donc conscients que leur disponibilité était peut-être orientée et motivée par un intérêt personnel. Concernant les autres intervenants, nous avons rencontré des problèmes de disponibilité. Par exemple, une association nous a expliqué n'avoir ni le temps ni les ressources humaines pour répondre à notre demande. La charge de travail que les acteurs de terrain subissent ne permet parfois pas de libérer du temps pour aider une étudiante dans le cadre d'une recherche académique. Cela pourrait expliquer pourquoi nous n'avons pas eu beaucoup de réponses positives de la part d'autres institutions. C'est pourquoi, selon nous, la principale faiblesse réside dans la quantité des entretiens exploratoires réalisés. L'absence d'un quota d'entretien satisfaisant entraîne également un souci d'exhaustivité que nous aurions voulu apporter à ce sujet. Ces entretiens sont essentiels pour l'exploration de notre objet de recherche, nous aurions voulu au minimum pouvoir nous appuyer sur cinq entretiens. Nous demandons aux lecteurs de prendre en considération que nous n'avons pas pu interroger tous les acteurs qui nous semblaient importants dans notre recherche malgré toutes les démarches de contact que nous avons entreprises. Par exemple, nous pensons qu'un organisme tel qu'Internet Watch Foundation (IWF) manque à notre recherche parce

qu'il a un point de vue plus international de la problématique. Ce dernier fournit cependant une série de rapports sur son site Internet, rapports que nous avons utilisés dans le cadre de notre recherche.

Notre position d'étudiante en criminologie constitue une limite méthodologique concernant les connaissances techniques suffisantes pour traiter de manière précise un outil aussi complexe que l'IA. Consciente de cette limite, nous avons restreint notre analyse aux IA principales. Cet obstacle s'est d'ailleurs retrouvé lors de l'exploration des techniques de détections.

2.5. Précisions quant à l'utilisation de l'IA dans un travail de recherche

Suite à la conjoncture actuelle de l'utilisation de l'IA dans les travaux universitaires, notre utilisation a respecté les trois principes prescrits par l'Uclouvain : responsabilité, authenticité et transparence. C'est précisément dans un enjeu de transparence que nous indiquons dans quel cadre l'IA a été utilisée durant la rédaction de ce mémoire. Nous avons eu recours à la vérification syntaxique et orthographique respectivement par l'intelligence artificielle et Antidote, outil orthographique.

Partie 3. L'abus sexuel sur mineurs : d'une image à l'autre

3.1. L'image à l'ère du numérique

Quelle définition donner à une image à l'ère dans laquelle les technologies repoussent les limites du possible ? Nous allons donc contextualiser l'image à travers son histoire pour comprendre comment sa définition a été influencée par divers événements, dont la photographie. La photo est en effet une étape importante dans la construction de la conception de l'image. Nous terminerons par envisager l'image dans son sens moderne, c'est-à-dire avec la reconfiguration que l'IA lui a apportée.

Dans la Grèce antique, l'image représente les pratiques sociales et religieuses de l'époque. À travers son histoire, elle sera comprise sous l'angle de la créativité et de la manifestation d'une nature divine. À ce sujet, Platon disait que les peintres faisaient des images d'images lorsqu'ils peignaient l'environnement qui les entourait (Bordron, 2025 ; Reverchon, 2020). Dans la littérature plus récente, J.-F. Bordron (2025) souligne que l'image s'inscrit dans une histoire qui débute aux empreintes et aux signes d'existence, autrement dit aux mains sur les murs dans les cavernes. Après, l'image sera envisagée sous l'angle de la perspective, donnant la naissance du point de vue rendant l'image possible au sens classique. Cette évolution nous montre que l'image prend des significations différentes en fonction de son contexte et de la manière dont elle a été créée. Il apparaît alors que sa

compréhension est ambiguë et qu'en l'absence d'une précision verbale accompagnant l'image, nous ne percevons pas toujours le sens et le contexte. Notons que l'image a pour but premier de représenter l'objet, si nous prenons en photo une chaise, elle ressemblera à une chaise. C'est pourquoi le sens d'une image est à considérer dans l'histoire dans laquelle elle a été créée et est toujours influencée par le contexte social dans lequel elle est produite (Faccioli, 2007 ; Schmoll, 2002).

L'apparition de la photographie a bouleversé la conception de l'image. La photo fige les pratiques techniques et esthétiques à un moment donné, nous faisant rentrer dans un nouveau régime de vérité. Dans ce dernier, les nouvelles technologies modifient le rapport au réel et imposent une nouvelle relation au monde. La photo est alors considérée comme une image numérique dont la création repose sur un cadrage, c'est-à-dire sélectionner des instants grâce à l'appareil photo pour capturer une image. La sélection d'un instant autrefois permis par l'appareil photo est désormais résumée à une indication donnée à une intelligence artificielle pour créer une image. La création d'images générées par l'intelligence artificielle débute par un « prompt », c'est-à-dire une instruction donnée à un algorithme pour obtenir une réponse ciblée. Ici, la réponse ciblée sera donc une image. Ensemble, la photographie et les images générées par IA amènent donc les artistes à s'innover en repoussant les limites de la création. L'IA démocratise le processus créatif en supprimant les difficultés inhérentes à la maîtrise des techniques artistiques. Cette démocratisation impacte la quantité de production des images explique J. – P. Terrenoire (1985), dans le monde actuel, « des images, par milliers, naissent, se répondent les unes les autres et meurent dans un flot puissant et généreux qui submerge tout sur son passage, laissant chacun ébahi, fasciné ou confondu » (p. 510). Cette citation nous permet d'introduire une problématique inhérente aux images générées par l'IA. Ces dernières sont de plus en plus nombreuses et Raphaël, F. (2007), nous fait remarquer que l'image se perd dans une multitude de copies (Guern, 2025). Ces constats théoriques sont malheureusement constatés dans la pratique rendant difficile l'intervention des autorités.

Mais ça augmente à une vitesse de flux. Au début, on pensait « est-ce que ça va devenir une certaine niche dans le domaine criminel ? » Mais on constate de plus en plus que l'IA, les images qui ont été générées sont devenues tellement populaires. Et ça augmente le volume des images réelles, on va dire... puisque la pédocriminelle il s'est recréé sa fantaisie explicite de maintenant et on constate qu'il y a des plateformes qui sont créées et consacrées uniquement aux images IA pédo, de plus en plus ça pollue, entre guillemets les images classiques et même les auteurs ne sont pas toujours au courant s'ils possèdent des images IA ou non IA. Il y a un mix énorme entre les deux

Personne travaillant à la police fédérale

Selon C. Leduc (2025), les images IA entraînent une incapacité à penser l'image au-delà de sa fonction de représentation. En effet, « les images produites par les grands générateurs ne seraient que des reproductions mécaniques des formes visuelles héritées manifestant une approche communicationnelle qui réduit l'art à une transmission d'information » (p.159). À ce propos, N.L. Le Guern (2025) rajoute que les images créées par IA ne sont pas des photographies (Leduc, 2025 ; Raphaël, 2007). Ainsi, la complexification du sens donné aux images et leur augmentation empêchent de saisir l'intention première du créateur de l'image. Avec l'émergence de l'IA, les images sont devenues la représentation d'un langage, le prompt, qui n'est plus la représentation analogique d'une réalité existante, mais un processus qui crée des réalités nouvelles. Par exemple, des IA dont Deep Dream créée en 2010, manipulent des images préexistantes, appelées alors des images « hybrides », car il s'agit de photos réelles modifiées par IA (Leduc, 2025). Ces indications nous permettent d'estimer qu'Internet sera de plus en plus submergé par des images sans signification et que nous sommes entrés dans une ère du visuel dans laquelle les outils numériques fournissent une nouvelle réalité simulée (Faccioli, 2007).

Les images sont donc influencées par des pratiques sociales attachées à un moment et à un contexte spécifiques dans l'histoire. Le contexte social modifie les significations et les usages. Cela nous amène à comprendre que l'image est un mode d'expression et de pensée propre qui traverse l'histoire (Metz, 1970).

3.2. Les images d'abus sexuels sur mineurs

À travers ce chapitre, nous discuterons de la problématique des MASE et de son émergence en tant que problème social dans l'actualité et dans les débats. Pour ce faire, nous allons décrire, puis illustrer l'enjeu des MASE à l'aide d'exemples tirés de l'actualité. Ensuite, nous nous concentrerons sur l'évolution terminologique des MASE, apparue pour protéger les victimes mineures, une protection qui nécessite une compréhension de leur statut.

3.2.1. Une problématique récente

Depuis les années 1960, les images d'abus sexuels sur mineurs sont considérées comme un problème social. Les mouvements féministes ont permis de conscientiser le problème en visibilisant et pointant dans les années 80 qu'il se déroule des abus sexuels sur les enfants, enjeu largement minimisé (Boussaguet, 2009). M. Salter dira que l'augmentation drastique de contenus d'enfants se situe dans les dix années folles, période durant laquelle la commercialisation et la production des images d'abus sexuels se sont mondialisées. Cette croissance est due notamment à l'accessibilité de la caméra, des échanges et de l'absence de

prescrits légaux créant des marges de manœuvre pour le marché noir des MASE. À cette époque, l'augmentation prend racine dans la légalisation de la pornographie propulsant les images d'abus sexuels sur mineurs du côté de la légalité. Avant 1990, les échanges s'opéraient au départ avec des papiers, des magazines ou encore des photos et rendaient la détection plus compliquée (Fondation pour l'enfance, 2024). L'agresseur profitait de crimes tels qu'un viol d'un mineur pour photographier ou réaliser des vidéos pour ensuite les partager par courrier, de personne à personne ou dans des magazines. Par exemple, des pays comme le Danemark ou la Suède, connus pour les problèmes de distribution de ces images, connaissent alors une augmentation de MASE. L'augmentation importante des MASE des années 90 a cependant été qualifiée comme une « panique morale », concept popularisé en 1987 par S. Cohen (2002, p. vii). Il est utilisé pour déclarer un phénomène infondé et accompagné d'une réaction exagérée prenant les événements avec peu de sérieux. C'est dans ce contexte que Jenkins sociologue septique par rapport à la crise des MASE, l'a malgré tout qualifié comme croissant et intolérable (Salter & Hanson, 2021). Ainsi, les luttes ont pris place dans une société empreinte de doutes et les scientifiques manquant de mots pour qualifier la crise qui occupe les images d'abus sexuels sur mineurs participaient à une banalisation de l'ampleur. M. Salter & T. Whitten (2022) pointe que l'expansion d'Internet au tournant du 21^e siècle a aggravé la quantité des images d'abus sexuels sur mineurs et a engendré de nouveaux problèmes. L'augmentation de la disponibilité de ces images et les échanges facilités par les nouvelles technologies dont la commercialisation d'Internet a participé à l'expansion de la criminalité (Westlake, 2019).

Pour illustrer les explications précédentes, nous allons présenter trois affaires qui ont traversé l'actualité. Dans les années 70 se déroule le cas de l'affaire Ionesco dans laquelle une mère a photographié sa fille pour la transformer en objet érotique. Les photos ont fait la une de dizaines de magazines sans que cela ne pose problème à l'époque (Drouelle, 2019 ; Le Monde, 2012). Plusieurs films et livres décrivent aussi la victimisation et l'exploitation des enfants, comme dans le livre *Lolita* de Nabokov et adapté au cinéma par Stanley Kubrick et qui dépeint le portrait d'une pédophile. Nous avons également l'affaire de Bastien Vivès accusé de promouvoir l'inceste et la pédophilie à travers ses œuvres. Cet artiste s'est présenté au festival de la Bande dessinée d'Angoulême en 2019 avec des œuvres montrant un jeune garçon avec un pénis disproportionné. Dès 2018, cette affaire a divisé les associations en faveur de la liberté d'expression et les personnes qui protègent les enfants (Bindé, 2022 ; Jaussent, 2022). Ces exemples tirés de l'art ou de la littérature montrent que la sexualisation visuelle ou littéraire d'abus sexuels sur mineurs a toujours été présente et traverse les époques (Holderness, 2024 ; Westlake, 2019).

3.2.2. Une définition en évolution

La définition et la problématique des MASE connaissent des évolutions constantes dans l'objectif de protéger les enfants victimes d'abus. Pour les protéger au mieux, les législateurs ont décidé qu'il était important de reconnaître l'illégalité de cette pratique. De ce fait, l'évolution de la définition du terme « pédopornographie » vers « images d'abus sexuel sur mineurs » prend racine dans une volonté de reconnaître les victimes. Nous sommes parfois réticents à nommer correctement les comportements alors que l'utilisation d'un mauvais vocabulaire minimise, banalise ou justifie ceux-ci (Bourcelet, 2024).

En Belgique, le Code pénal a récemment actualisé sa définition des images d'abus sexuels sur mineurs. En résumé, cela constitue un matériel visuel (images, vidéos ou photos) représentant un mineur dans des comportements sexuels explicites. Nous reviendrons plus précisément sur le libellé de l'article dans notre chapitre sur le cadre réglementaire. ²Bourcelet E. (2024), dans le journal du droit des jeunes, décrit le cadre entourant la terminologie des « images d'abus sexuels sur mineurs ». Ce terme apparu récemment est venu se substituer à l'appellation « pédopornographie ». En effet, cette dernière n'est plus considérée comme adéquate pour désigner ce type de violences sexuelles. La racine « pédo- » se réfère à l'enfance, tandis que « pornographie » se réfère à un contenu adulte licite. C'est pourquoi la littérature préfère les termes « images d'abus sexuels sur mineurs » ou encore « matériel représentant des violences sexuelles sur mineurs ». Par conséquent, nous utilisons dans ce travail le terme « images/matériel d'abus sexuels sur mineurs » ou l'acronyme MASE, déjà évoqué pour remplacer le mot « pédopornographie ». Dans la continuité de ses propos, E. Bourcelet (2024) attire notre attention sur le fait que le terme « abus », utilisé dans la nouvelle terminologie est également de plus en plus questionné. Il renverrait à un excès ou à un mauvais usage impliquant implicitement un certain seuil de tolérance. Or, nous l'avons déjà évoqué, l'utilisation d'une mauvaise terminologie banalise l'exploitation sexuelle des enfants (Dabrowska, 2025 ; Interpol, s. d.).

3.2.3. Des victimes : les mineurs

Dans ce point, nous évoquerons le statut des victimes et l'impact de ce dernier sur le consentement. Les victimes de ces images sont principalement des enfants, célèbres ou non, âgés au maximum de 18 ans (Internet Watch Foundation [IWF], 2024). Dans l'appellation « mineurs », nous englobons les jeunes de genre féminin et masculin. Tout ceci amène alors à la réflexion d'une potentielle incidence du genre sur la problématique. Selon une étude menée aux États-Unis par M. Salter et T. Whitten (2022), le genre de l'enfant dans ce type d'exploitation sexuelle n'a pas d'effet notable sur la consommation. Une étude qualitative

² C. pén., art. 417/43 ; Nouveau C. pén., art. 170.

menée par Benouamer et al. (2024) sur des participants belges consommateurs de matériel d'abus sexuels sur mineurs révèle qu'en effet le genre des victimes n'aurait pas d'impact significatif, car il n'apparaît pas que les auteurs des faits aient besoin de sélectionner leur contenu. Cela est dû notamment à la quantité massive d'images qu'ils peuvent trouver sur Internet. Il semblerait que se produise une légère prédominance du genre féminin. Benouamer et al. (2024) indiquent cependant que cette thématique n'est pas encore assez étudiée et qu'une seule recherche scientifique rejoint leur propos. Dans des recherches complémentaires, il serait intéressant d'examiner les patterns de victimisation selon le genre de la victime.

Les victimes de ces abus sexuels n'ont pas consenti à l'utilisation de leur identité ou de la création d'un contenu sexuel avec leur visage dessus (Sablon, 2025). Les enfants sont alors incapables de consentir légalement à l'enregistrement ou la distribution de contenu sexuel ou toute autre relation sexuelle. La question de l'absence de consentement n'est pas libellée dans les éléments constitutifs de l'infraction lorsqu'il est entendu sous l'angle des MASE, mais le caractère punissable de l'infraction persiste même si la victime s'était livrée à un comportement sexuel réel ou simulé. Nous retrouvons trois seuils qui orientent le traitement de la question du consentement. Ce dernier est absent, et ce, de manière irréfutable si le mineur n'a pas atteint l'âge de 14 ans, si le partage des photos a été possible par un abus de confiance, si l'infraction a été rendue possible par autorité ou par influence sur la victime, si la diffusion est un fait des parents ou si les photos sont issues d'un acte de débauche ou de prostitution. À partir de 16 ans, le mineur est reconnu capable de donner un consentement libre quant à ses photos intimes. Enfin, il existe un régime spécifique pour les mineurs entre 14 et 16 ans qui disposent d'un consentement libre si la différence d'âge avec l'auteur des faits ne dépasse pas trois ans, si la victime et l'auteur sont mineurs et sont âgés de 14 ans accomplis. Il est alors possible de poursuivre l'auteur pour diffusion d'images d'abus sexuels sur mineurs si les photos rentrent dans le champ d'application de l'article (Bourcelet & Mathieu, 2025 ; Gangi et al., 2022 ; Holderness, 2024).

Partie 4. Le déploiement de l'intelligence artificielle

La toile de fond de l'intelligence artificielle

Les réseaux de neurones, principe de l'IA, et le connexionnisme³ ont une histoire intrinsèquement liée à celle de l'informatique. Pour comprendre l'installation de

³ « Le connexionnisme propose une conception de l'activité cognitive inspirée de ce que l'on sait du système nerveux. L'idée fondamentale est qu'un réseau connexionniste est constitué par un ensemble d'unités élémentaires, dont chacune possède un certain niveau d'activation ; ces unités sont connectées entre elles de sorte que les unités actives puissent activer ou inhiber d'autres unités. » (« Connexionnisme », s. d.)

l'intelligence artificielle dans nos quotidiens, nous allons maintenant examiner les fondements d'Internet. Envisager l'histoire de ce réseau nous donne l'opportunité de saisir la manière dont l'intelligence artificielle s'est implantée et comment elle a pu être détournée à des fins criminelles. (Saporta, 2023)

Aux fondements d'Internet et de la cybercriminalité

Dans la partie précédente, nous avons abordé la notion d'image et plus précisément, les images d'abus sexuels sur mineurs. Ici, nous envisagerons la naissance d'Internet et son fonctionnement. Cela nous permettra de comprendre pourquoi par sa nature Internet a permis le développement d'une nouvelle forme de criminalité.

C'est en 1969 avec le lancement du réseau ARPANET, ancêtre d'Internet (Robin, 2021), que nous pouvons comprendre comment les outils de calcul et de gestion administrative et financière ont aidé son implantation dans la vie des individus. La volonté de cet outil était de rationaliser, automatiser des tâches et des activités de travail. Ainsi, l'outil a servi à consulter des informations bibliographiques à distance dans le domaine médical et juridique. Cet usage premier n'est pas semblable à la conception actuelle d'Internet et a évolué pour devenir l'Internet que nous connaissons. D'un point de vue sociologique, ce dernier s'est articulé autour de trois promesses. L'avènement d'Internet visait à créer une société virtuelle avec des individus capables de s'auto-organiser en communauté. Ces individus partageant des intérêts communs ont eu l'opportunité de s'interconnecter grâce à l'apparition de la messagerie. D'une décentralisation des outils de l'information et de la communication est né le désir d'une société plus démocratique, une décentralisation qui a produit un amoindrissement des contraintes vécues concernant l'isolement social lié à la difficulté de rencontre des pairs. De plus, les risques de découvrir du matériel illicite ont évolué en rendant plus difficiles les interventions des autorités (Corriveau, 2010). Les criminels, les plus expérimentés, se sont emparés d'Internet quasi instantanément pour en exploiter les failles, les opportunités et ainsi le détourner de son usage premier. Des pratiques telles que le hacking c'est-à-dire le fait de pénétrer illégalement dans un système informatique (« hacking », s. d.), la diffusion des virus, du ransomware⁴ et du phishing⁵ sont apparues. Le cyberspace devient alors un terrain fertile pour les criminels par sa faible régulation et de l'absence quasi totale de contrôle (Mouheb, 2024 ; Beuscart et al., 2019). À partir de 1995, Internet a intégré des images, des sons ou encore des moteurs

⁴ Logiciel malveillant qui bloque des données pour menacer les victimes en vue d'une rançon. (*Qu'est-ce qu'un rançongiciel ?*, s. d.)

⁵ « Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de “mettre à jour” ou de “confirmer vos informations suite à un incident technique”, notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.) » (*Question | CNIL*, s. d.)

de recherche. Son développement s'est progressivement organisé autour du peer-to-peer, permettant le téléchargement et l'échange de fichiers entre utilisateurs. L'apport du dispositif peer-to-peer réside dès lors dans l'ampleur et l'internationalisation des échanges émanant directement de la nature du cyberspace. Dans ce contexte du peer-to-peer, il existe une prise de conscience sur l'aspect organisé et collaboratif du trafic de MASE présent sur le réseau. Internet a donc jeté les bases d'une nouvelle économie et de nouvelles relations marchandes et d'échange (Beuscart et al., 2019 ; Corriveau, 2010).

Pour comprendre les fondements de l'aspect collaboratif sur Internet, le concept de H. Becker sur la sous-culture de la déviance est mobilisé par P. Corriveau (2010). Ce concept est utilisé pour mieux saisir la dynamique des amateurs de MASE appelé des « groupes de nouvelles ». Ces groupes sont des communautés de discussions autour de leurs déviances sexuelles et d'échanges d'images entre utilisateurs. L'étude de Corriveau (2010) réalisée sur ces groupes montre que les consommations étaient autrefois plus isolées rendant plus difficile la création d'une communauté. Il apparaît qu'Internet offre un terrain de rencontre propice pour la mise en place des sous-cultures déviantes. De plus, le monde virtuel n'a pas de frontière géographique ce qui facilite les échanges entre les individus. Ces deux constats favorisent la reconnaissance réciproque des consommateurs de MASE. Les échanges de MASE sur Internet offrent donc la possibilité à des pédophiles auparavant isolés, de renforcer mutuellement leurs tendances déviantes. H. Mouheb (2024) précise en mentionnant qu'Internet a facilité l'apparition de pornographies et les images d'abus sexuels sur mineurs en ligne accessibles sur le Clear web et le Dark web. Ce constat est également appuyé par la thèse de F. Fortin (2014), montrant que l'apparition d'Internet a permis une voie d'accès à une multitude d'informations et a bouleversé le marché de la pornographie et de l'exploitation de l'enfant. Internet joue un rôle de facilitateur pour la consommation de contenu pornographique. Par sa nature, les pédocriminels ont accès 24 h sur 24, 7 jours sur 7 à des fichiers de bonne qualité et les technologies de l'information facilitent la distribution image d'abus sexuels sur mineurs (Corriveau, 2010 ; Westlake, 2019). Le phénomène des MASE a donc connu un bouleversement important avec l'arrivée d'Internet qui a offert la possibilité de l'anonymat, de complexifier les réseaux et d'augmenter les échanges (Corriveau, 2010). Nous appréhendons donc Internet comme un espace donnant la possibilité de s'organiser et d'échanger à des fins criminelles.

La naissance de l'intelligence artificielle

Dans cette section, nous envisageons les débuts de l'intelligence artificielle pour comprendre comment elle s'est rendue indispensable dans le quotidien d'une partie des individus. À cette fin, nous définirons et proposerons un historique de l'IA.

L'intelligence artificielle est définie par le Larousse comme « l'ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine » (« Intelligence Artificielle », s. d.). Le Parlement européen, quant à lui, la définit comme suit : « la possibilité pour une machine de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité » (Intelligence artificielle, 2020 ; Saporta, 2023). Ces deux définitions nous donnent une indication importante, l'IA est une machine qui reproduit des comportements humains. Nous pensons par exemple à l'IA Deepblue, ordinateur programmable, bien connu pour reproduire un jeu d'échecs (Pickover, 2021 ; Saporta, 2023). Au départ, le nom IA englobe un champ de recherche qui veut générer une science de l'esprit humain, en espérant produire des machines imitant son raisonnement. V. Beaudouin et J. Velkovska (2023) estiment que deux courants ont pris part à la naissance de l'IA. D'une part, entre 1946 et 1953, les conférences de Macys autour de la cybernétique avaient pour objectifs que des scientifiques échangent sur les fonctionnements de la pensée humaine. D'autre part, en 1956, John McCarthy a utilisé l'expression « *artificial intelligence* » dans un titre du Dartmouth Summer Research Project, pour désigner la simulation et la compréhension des processus cognitifs. Ces deux courants s'affrontent devant les prémices d'une réflexion sur la cognition humaine et non humaine. Nous donnons à l'IA des racines américaines et à la cybernétique des racines européennes. Ces domaines ne seront que très peu financés pendant de nombreuses années (Haiech, 2020).

Néanmoins, l'impulsion donnée par ces deux courants a favorisé l'émergence du concept de réseau de neurones. Celui-ci est défini comme un « ensemble organisé de neurones interconnectés permettant la résolution de problèmes complexes tels que la vision par ordinateur ou le traitement du langage naturel », également appelé deep learning (Police Fédérale - DJSOC FCCU, s. d.). Le mathématicien G. Saporta (2023), dans son étude sur l'histoire et les enjeux de l'IA, distingue trois types d'intelligence artificielle. Tout d'abord, l'IA symbolique qui est une modélisation du raisonnement humain avec des règles logiques ou probabilistes. Elle connaît son âge d'or dans les années 90 et reste très présente dans le milieu médical. Ensuite, l'IA numérique vise à prédire un comportement ou une réponse par des fonctions mathématiques et statistiques. À partir des années 2010, les réseaux de neurones connaissent un regain d'intérêt. Finalement, l'IA générative apparaît et elle produit du contenu sur demande à partir des données d'apprentissage. En 2022, un des plus connus réseaux de neurones et d'IA générative, Chatgpt, conçu par OpenIA connaît un succès fulgurant et démocratise l'accès à l'intelligence artificielle. Cette émergence possède des dangers importants poussant le champ scientifique à s'interroger sur l'éthique des nouvelles technologies. Il est important que l'IA respecte quelques principes autour de

son fonctionnement, par exemple la transparence, la justice et l'équité, la non-malfaisance, la responsabilité et la vie privée (Saporta, 2023 ; Beaudouin & Velkovska, 2023). Malgré ces exigences, nous constatons que l'IA est faillible et n'est pas stable ce qui la rend plus susceptible d'être victime de cyberattaques ou de créer elle-même des cyberattaques. Par exemple, des IA d'Open IA auraient mené de manière totalement autonome des cyberattaques (AFP, 2026). Cela nous démontre qu'il est encore nécessaire d'avoir une supervision humaine face à cette autonomie grandissante. Les humains travaillant derrière les IA sont appelés « les travailleurs du clic ». Ces personnes sont indispensables dans l'apprentissage par renforcement à rétroaction humaine (Saporta, 2023). Pourtant, l'intelligence artificielle s'autoalimente sur une large base de données, pour un jour potentiellement essayer de se passer d'interventions humaines. Le développement de l'intelligence artificielle n'est pas linéaire. Il a connu des périodes d'enthousiasme, de déception et de reculs. Cependant, de nos jours, même si l'IA a été démocratisée depuis peu de temps, il est difficile d'imaginer notre quotidien sans elle. Si cette dernière s'est implantée rapidement, elle a également connu un détournement rapide de la part des criminels (Mouheb, 2024).

L'intelligence artificielle comme vecteur de nouvelles formes de criminalité

Typologie des intelligences artificielles

Le mot « intelligence artificielle » englobe plusieurs technologies différentes, le Machine Learning composé du Deep Learning et du Neural network, éléments importants pour la compréhension des IA génératives. Les IA posent de réelles questions sur le futur : arriverons-nous encore à distinguer la réalité de la fiction ? (Police Fédérale - DJSOC FCCU, s. d.) Pour répondre à cette question, nous voulons comprendre le contexte des émergences des IA génératives et comment l'arrivée d'une telle technologie a rebattu les cartes de la diffusion des MASE.

La firme IBM définit le concept de Machine Learning, comme l'« IA axée sur les algorithmes capables “d'apprendre” les schémas de données d'entraînement pour faire des inférences précises sur de nouvelles données. » (Bergmann, s.d.) L'IBM affirme également que toutes les IA ne sont pas des machine learning, mais toutes les machine learning sont des IA. Les IA génératives comprises à l'intérieur de ce groupe sont par exemple, les Grands modèles linguistiques, la génération d'images par l'IA, l'IA multimodale, la génération augmentée par récupération, la génération de code par l'IA et enfin, les agents d'IA. Parmi les sous-catégories de la Machine Learning, le Deep Learning ou « apprentissage profond », système neuronal en couche, est largement l'IA la plus utilisée (Police Fédérale - DJSOC FCCU, s. d.). Une autre sous-catégorie est le neural network, la fondation des algorithmes

de deep learning. Nous nommons « IA générative d'image », les IA qui, au moyen de prompts, c'est-à-dire des « instructions envoyées à un algorithme d'intelligence artificielle spécialisé dans la génération » (« Prompt, Prompte », s. d.) engendrent des images qui s'avèrent de plus en plus réalistes. (Bergmann, s.d. ; François & Aubernon, 2024 ; IBM Data & AI Team, s. d.)

Revenons aux intelligences génératives. Nous avons vu qu'elles ne se limitent donc pas aux IA génératives d'images, mais concernent aussi ChatGPT ou encore Gemini qui sont des Grands modèles de Langage (LLM) avec lesquels l'utilisateur peut entretenir une conversation. Ces technologies ont été créées pour générer un texte, parfois prédictif, c'est-à-dire qui propose une écriture de mots, aux utilisateurs (Davidson et al., 2026 ; Stryker, s.d. a). Au sein des IA génératives énumérées ci-dessus, nous trouvons des modèles de diffusion utilisés pour générer des images entraînées par le deep learning⁶. Les AI sont entraînées sur des bases de données qui contiennent parfois des contenus illégaux ou encore des MASE comme cela a été le cas pour l'IA *Stability AI* (Bracket Foundation, 2024 ; Hotz, 2026). Stable Diffusion, Midjourney, Imagen ou encore DALL-e sont des modèles de diffusions connus pour générer ce genre d'images. Dans la catégorie des modèles de diffusion, il existe également le Fine tuning model, traduit par « réglage fin », comme LoRa que nous avons déjà mentionné dans le point 3. L'avantage de cet outil est de produire une grande quantité d'images à partir d'une petite base de données (Easttom, 2025 ; Bergmann & Cole, s.d.). Par exemple, il est désormais possible de donner « vie » à l'image d'une personne décédée (François & Aubernon, 2024). D'un point de vue technique, C. O Ciardha et al. (2026) expliquent que l'IA traite les informations dans un ordre précis. Tout d'abord, les indications sont séparées en plusieurs petites pièces appelées *tokens*, que nous pouvons traduire par élément ou jeton en français, et qui donnent la possibilité au modèle de combiner le concept visuel avec une base de données d'images et de description textuelle (les couleurs, les textures et les paysages). Ensuite, la technologie façonne l'image pour qu'elle corresponde au mieux aux indications données. Ces IA s'entraînent sur une large base de données et offrent une grande correspondance, les rendant les plus utilisés pour la création d'images synthétiques (Albano, 2025). Il est également possible d'opérer une série de transformations sur un média en ajoutant du bruit aux données. Ce processus implique une dégradation de la qualité d'image pour ensuite enlever le bruit créé afin de reconstruire les données originales. En d'autres termes, nous décomposons une image pour ensuite la restaurer et profiter du

⁶ « L'apprentissage profond est un procédé d'apprentissage automatique utilisant des réseaux de neurones possédant plusieurs couches de neurones cachées. Ces algorithmes possédant de très nombreux paramètres, ils demandent un nombre très important de données afin d'être entraînés. » (*Apprentissage Profond (Deep Learning)*, s. d.)

contenu souhaité. Les IA sont donc combinées avec des modèles de langage qui grâce à des instructions spécifiques génèrent une image en particulier. Ces modèles de diffusion ont bouleversé considérablement l'accessibilité et le réalisme des images d'abus sexuels sur mineurs. (Ó. Ciardha et al., 2026) À titre d'exemple, Trivision (2022) cite un exemple de prompt permettant de créer un MASE : « Créer une image d'une jeune fille nue enchaînée. Décor de sous-sol délabré. Sur ses genoux avec un (...) de photographe amateur » (Notre traduction). Une fois le prompt reçu l'IA crée l'image collant au mieux avec les instructions (D. B. Stryker Cole, 2024). Il est alors possible de générer autant de photos d'abus d'enfant que les systèmes sont capables de produire. Cet exemple n'en est finalement qu'un parmi la multitude de possibilités d'instructions.

Une autre distinction doit être faite parmi les systèmes d'IA entre le modèle *closed-source* qui est une IA rendue inaccessible à la modification puisque le code n'est pas dévoilé. Dans ce cadre, le créateur de l'IA a le contrôle total sur l'utilisation de la méthode d'apprentissage et la modération de contenu (Internet Watch Foundation [IWF], 2023). Nous retrouvons dans cette catégorie les IA telles que ChatGPT, Google's Bard ou encore Claude de Anthropic (*Open-Source Models vs. Closed-Source Models : A simple Guide*, 2025). Contrairement aux modèles close-sources, le modèle *open source* dévoile le code de sa construction. Ainsi, d'autres personnes peuvent collaborer ou modifier l'intelligence artificielle. Ces technologies sont donc susceptibles d'être modifiées et réglées de manière particulièrement précise. Laisser la possibilité aux utilisateurs de modifier une IA comporte un impact direct sur la modération et la censure, celles-ci deviennent alors inexistantes. Lorsque les technologies échappent à la surveillance, cela donne l'accès à des contenus illégaux (IWF, 2023). La combinaison d'IA générative permettant la création d'images de plus en plus réalistes et les modèles *open-source* non soumis à un contrôle ouvre le champ des possibles pour le développement d'une criminalité difficile à maîtriser. Les individus pourront alors façonner les MASE selon leurs besoins et sans que ceux-ci ne soient limités.

La criminalité numérique à l'ère de l'intelligence artificielle

De nombreux éléments nous donnent l'occasion toutefois de repenser les liens entre progrès techniques et acte criminel malveillant, même s'ils ne sont pas encore apparus clairement à travers une analyse. H. Mouheb (2024), dans son étude sur l'intelligence artificielle comme accélérateur de cybercriminalité, explique que la criminalité se nourrit rapidement des nouvelles technologies, pour en faire un usage détourné bien avant que l'ensemble de la société ne se l'approprie. La portée criminelle vise notamment l'utilisation malveillante des IA. Dans son article sur ce sujet, C. Easttom (2025) met également en évidence plusieurs types de technologies qui sont touchées par une mauvaise utilisation.

Parmi la multitude de mauvaises utilisations possibles, certaines sont appelées Jailbreaking, détournant les garanties et les garde-fous des intelligences artificielles et fournissant du contenu interdit. Pour ce faire, les auteurs utilisent de prompts spécifiques afin de contourner les protocoles de sécurité. (Easttom, 2025; Ó. Ciardha et al., 2026) Les technologies telles que ChatGPT, sont des ressources en grande majorité accessible et qui ne nécessitent pas de compétences particulières pour les utiliser, donnant l'opportunité à n'importe qui de se lancer dans la cybercriminalité. L'intelligence artificielle est alors utilisée comme agent facilitateur pour commettre des crimes par suppression des barrières technologiques. Les criminels cherchent à affiner leurs modes opératoires grâce à l'IA, surtout dans le domaine des cyber escroqueries. Pour ce faire, les cybercriminels opèrent une optimisation des résultats des IA afin d'augmenter la réussite de leur crime. H. Mouheb (2024) donne l'exemple des deepfake pour illustrer le concept de sophistication de l'intelligence artificielle, les sons, les images et les vidéos sont plus réalistes. Les MASE sont alors de plus en plus vraisemblables et la distinction entre réalité et fiction devient plus difficile.

La commission des infractions ne passe pas seulement par le *jailbreak*, il existe des modèles de diffusion qui, par leur manque de sécurité, fournissent un accès à la création de médias illégaux. Même si la modification des images dans un but criminel a débuté avant les modèles de diffusion, par exemple avec des technologies échangeant les visages appelés « face swap », elle a connu un tournant significatif (Bitouk et al., 2008). Ces derniers ont offert la possibilité aux individus sans expertise de produire des contenus nuisibles. Il est donc devenu plus facile pour les auteurs d'infractions de manipuler les outils selon leurs propres besoins. Ainsi, les machines d'apprentissage sont devenues un moyen pour augmenter la production criminelle. Les criminels ne s'arrêtent pas à ces manipulations et implantent aussi les IA avec des logiciels malveillants pour permettre au logiciel d'être plus performant créant une plus grande menace en termes de cybercriminalité (Ó. Ciardha et al., 2026).

Une rencontre inquiétante : le cas des MASE

Comme nous l'avons évoqué plus haut, l'émergence de l'IA conduit à une augmentation de l'accessibilité et de l'optimisation de la qualité des images générées. Que se déroule-t-il alors lorsqu'une technologie presque sans limites rencontre des criminels, expérimentés ou non, en recherche d'images d'enfant ? Nous allons évaluer comment ces deux éléments peuvent faire ressortir une utilisation détournée problématique. C'est pourquoi dans cette partie nous portons notre attention sur l'impact des IA dans le domaine des IA MASE représentant une utilisation détournée des outils technologiques.

Dans la première partie de notre mémoire relative à la typologie des intelligences artificielles, nous avons envisagé les modèles *open* et *closed source* de manière assez brève sans évoquer volontairement l'utilisation détournée de ceux-ci. Pour compléter ces informations, l'*Internet Watch Foundation* (IWF) met en exergue les inconvénients des modèles open source. En effet, ce dernier permet à n'importe qui de modifier une image et, par conséquent, de détourner les garde-fous mis en place pour éviter de générer des MASE. À l'inverse, dans le cas des modèles *closed*, les utilisateurs rencontrent des difficultés à générer des MASE à cause de restrictions de prompt ou de données manquantes. Ces deux éléments bloquent l'accès pour une création libre d'images (Fondation pour l'enfance, 2024 ; IWF, 2023). Nous ajoutons par rapport à ce qui a été dit précédemment qu'il existe des cloud-based model qui sont des systèmes avec des accès via Internet et non par l'ordinateur des utilisateurs. Le cloud entraîne une absence de traçabilité et une meilleure anonymisation rendant l'identification des auteurs plus complexe. Cela représente des avantages profitables aux amateurs de MASE, des avantages qui sont retrouvés dans les IA téléchargeables, c'est-à-dire qu'une fois que celles-ci sont téléchargées sur l'ordinateur, les criminels peuvent les faire fonctionner sans connexion. Ce procédé permet aux pédocriminels d'échapper à la détection (IWF, 2023 ; IWF, 2026 ; Ó. Ciardha et al., 2026). En résumé, les IA MASE sont souvent générées par des modèles open source, les outils de prédilection des pédocriminels, car ils peuvent les modifier à leur convenance.

Malgré cette grande accessibilité, les rapports de l'*Internet Watch Foundation* offrent un regard et une analyse sur les problèmes des IA MASE (des images, des vidéos, des conversations créées avec l'assistance d'IA générative). Les principales IA génératives utilisées pour générer des MASE sont les larges modèles de langage, les applications qui nudifient, et les textes-vers-images, des IA qui créent du contenu visuel à partir d'une description en langage naturel. Il est intéressant de constater que ce document nous indique que les images générées par IA ne sont pas la plus grande partie des signalements qu'ils reçoivent (IWF, 2026). Ce constat est partagé par Child focus et la personne interviewée nous indique :

Donc là dans nos chiffres oui c'est vrai, on a quelques-uns, mais c'est pas énormément [...] L'IA peut être utilisé dans d'autres moyens pour exploiter les jeunes, mais peut-être on ne l'a pas encore ou pas tellement des dossiers concernant du contenu qui a été créé.

Personne travaillant chez Child Focus

En dépit de ces observations, le danger réside bel et bien dans une augmentation rapide observée depuis quelques années et qui devrait se faire ressentir dans la pratique rapidement (IWF, 2026). Plus précisément, les MASE sont notamment créés en analysant

des photos réelles d'enfants pour ensuite les modifier en les mettant dans des positions sexualisantes (Ende, 2025). Concrètement, les MASE d'enfants réels servent quelques fois de contenu pour entraîner les IA et enrichir les bases de données (IWF, 2026). En effet, l'IA crée et génère des contenus réalistes qui permettent souvent de cacher des abus et d'éviter les contre-indications légales en rendant l'identification des victimes toujours plus compliquée. Les personnes chargées de la détection n'arrivent plus à savoir si les images sont réelles, modifiées ou totalement générées (Ende, 2025 ; Boutier, 2026). Par exemple, nous trouvons le Fine tuning, traduit par « réglage fin », utilisé sur des images d'enfants pour leur donner des âges, des positions ou des contenus explicites particuliers. Les auteurs utilisent les failles techniques des technologies à leur avantage pour contourner les mesures de sécurité (Easttom, 2025 ; Stryker, 2024).

Dans les premières générations d'intelligence artificielle générative, nous retrouvons les Generative adversarial Networks, appelé GANs basé sur deux neural network : un générateur d'images et un discriminateur pour discerner le vrai du faux (European Parliamentary Research Service & Negreiro, 2025). Ces modèles étaient connus pour générer des images synthétiques hyperréalistes. Ils sont encore utilisés pour créer des données synthétiques qui déterminent le taux de réalisme des contenus. Les techniques composées du GANs sont utilisées pour l'échange de visage ou pour modifier des images existantes comme la nudification des photos prises par caméra. Ce processus a été devancé par les modèles de diffusions désormais favorisés pour générer des contenus complètement synthétiques (Ó. Ciardha et al., 2026 ; Hotz, 2026). Selon O. Ciardha et al. (2026), les contenus visuels concernés sont du matériel sexuel explicite créé ou modifié en utilisant des techniques comme les modèles de diffusion ou les GANs. Les IA MASE se distinguent en ce qu'elles sont générées synthétiquement ou modifiées, contrairement aux MASE classiques qui découlent souvent de l'abus d'un enfant. En réalité, il persiste encore une distinction qui peut être faite parmi les MASE, c'est-à-dire celles qui sont complètement générées et celles qui sont manipulées. Cela montre une différence entre le matériel d'abus totalement et partiellement synthétique. Par exemple, les Deep fake sont des contenus partiellement synthétiques dans lesquels l'intelligence artificielle est utilisée pour modifier une image ou une vidéo déjà existante.

Ces explications nous permettent de définir les IA MASE visés par cette recherche, comme une image hyper réaliste d'une exploitation sexuelle pour mineur, complètement ou partiellement manipulée à partir de photos ou vidéos existantes. Ils sont souvent aussi considérés comme non réels (Hotz, 2026). Ces IA MASE apparaissent donc dans quatre situations distinctes. Premièrement, les images d'enfants sont prises pour entraîner des IA

telles que des modèles de diffusion comme *Stability AI*. Deuxièmement, les photos des réseaux sociaux (ci-après RS) sont prises pour générer des photos, notamment les *Deepnudes*. Troisièmement, les criminels prennent une photo d'enfant nu existante et la modifient à nouveau et finalement, l'IA est utilisée pour rajeunir une photo d'un adulte. Toutes ces situations produisent des IA MASE qui circulent sur la sphère du Web (Bracket Foundation, 2024).

L'émergence d'une nouvelle criminalité

Par l'évènement des intelligences artificielles génératives, des photos d'individus sont dénudées ou encore modifiées dans un but sexuel. Ces contenus peuvent être considérés comme des « deepfakes » dont la racine du nom provient de « deep learning » (Easttom, 2025). Ce terme est traduit parfois par « hypertrucages » en français, et renvoie à un procédé permettant de générer complètement ou partiellement une image. Cette technique, à visée criminelle, touche principalement les enfants et les femmes. Grâce à cette technologie, il est désormais possible de créer très facilement une vidéo ou une photo d'un mineur dans un contexte sexualisant. Cette technique soulève un questionnement important : le matériel généré avec cette technologie semble réel, mais a été manipulé par l'IA (Dakota Szyf et al., 2023 ; Ó. Ciardha et al., 2026 ; Rougaïbi, 2024). Désormais, les criminels utilisent une technologie générative *open source* afin de produire des images dévastatrices. L'IA générative est construite à partir d'une base de données et les données sont partagées afin de façonner les modèles. Au sein des technologies de deepfakes, nous retrouvons les deepnudes. Le verbe « deepnuding » fait référence au fait de nudifier la photo d'une personne grâce à l'intelligence artificielle. Si ce déshabillage n'est pas nouveau, l'IA rend la manipulation plus facile. Par exemple, une autre technologie de *deepfake* est *DreamBooth* qui est une technique d'apprentissage profond et crée du contenu personnalisé en incorporant des caractéristiques spécifiques telles que des objets, des individus, ou des styles. (Bergmann & Stryker, 2024 ; Easttom, 2025). Nous retrouvons, dans la catégorie des *deepfakes*, *DeepFace* un outil en Python *open source* qui est une technologie de programmation avec une lisibilité du code (*Python : Définition et Guide Complet*, s. d.). Elle crée des photos et des vidéos de manière rapide avec peu de connaissances sur l'apprentissage profond. Il est possible de trouver des tutoriels sur Internet rendant cette technique facile d'utilisation. D'autres outils sont également créés spécifiquement pour produire des images de grande qualité, comme *StyleGAN*, qui génère des images réalistes de haute résolution. Cette technologie est basée sur le « *style-based* » qui convertit un code latent en un espace latent rendant les images plus raffinées et plus détaillées (Easttom, 2025). Dans la continuité de ce que nous avons exposé dans ce paragraphe, nous avons vu cette

année l'émergence de Grok, IA développée par l'homme d'affaires Elon Musk (Davidson et al., 2026). Cet outil s'est fait connaître de manière fulgurante pour sa capacité à enlever les vêtements au départ d'une image d'une personne initialement habillée. Rapidement, les internautes se sont emparés de cette technologie pour l'appliquer à un panel varié de situations et de cibles. Nous en avons eu une démonstration lors de l'incident tragique du Crans-Montana, dans lequel des femmes bien souvent mineures ont été dénudées par le biais de cette technologie ⁷(IWF, 2026 ; Jaussent, 2026). Dénuder une photo était auparavant possible grâce à des compétences spécifiques en Photoshop. Cet exemple nous montre qu'il est désormais facile de nudifier une photo sans connaissance particulière (Grossman et al., 2025). La modification d'une image à des fins sexuelles n'est pas la seule utilisation criminelle possible qui touche les MASE. La photo générée par IA est utilisée pour attirer les utilisateurs et faire la promotion de messageries cryptées ou de sites Internet dans lesquelles il est possible de trouver des MASE. Ce modus operandi est propre au Clear Web. Par exemple, le réseau social X, anciennement Twitter, est connu pour véhiculer ce type de contenu. Cela représente le modus operandi propre au Clear web. La mauvaise utilisation des IA génératives comprend également les grands modèles de langage (LLM) qui sont aussi utilisés pour l'exploitation sexuelle d'enfants. Les pédocriminels les utilisent parfois pour mieux aborder les enfants et adapter leur comportement. Les LLM servent aussi à générer des MASE ou encore à créer des avatars pour se mêler aux enfants présents sur Internet (IWF, 2023 ; IWF, 2026 ; Lykousas & Patsakis, 2025).

Par ailleurs, les analystes de l'IWF sont inquiétés par ce qu'ils appellent les « Agentic AI » qui peut être traduit par « agentique IA ». Ces systèmes sont capables de poursuivre un objectif précis avec une intervention humaine limitée (Stryker, s.d. b ; « Qu'est-Ce Que L'"IA Agentique" ? Comprendre Son Histoire Pour Dépasser L'effet De Mode », 2026). Selon l'IWF, cela impactera davantage la propagation des MASE en ligne. Nous sommes dans un monde où les contenus générés par certaines intelligences artificielles sont visuellement très convaincants et indissociables de vrais contenus non manipulés (Easttom, 2025). Les associations telles que IWF, les intervenants de terrain ou encore les chercheurs pointent un danger d'aggravation de phénomène des MASE (IWF, 2026). Au départ de l'aperçu que nous venons de proposer, nous imaginons mieux comment IA et MASE se rencontrent et engendrent des problématiques importantes. Il est impossible de « définir jusqu'où la société sera capable d'aller avec l'IA générative en bien comme en mal, dans une semaine, dans un mois, dans un an » (Fondation de l'enfance, 2024). Ce dont nous

⁷ Notons que depuis quelques mois, suite à une interdiction européenne, Grok ne peut plus dénuder les photos (Datta, 2026).

sommes certain, est bel est bien le caractère inquiétant des IA génératives qui sont souvent nommées « arme », notamment pour commettre la cyberpédocriminalité (Béchu, 2025). Pour aller plus loin, le point suivant envisage comment ce phénomène impacte les victimes.

Des préjudices considérables

Précédemment, nous avons constaté que plusieurs situations sont à l'origine des IA MASE : la nudification de photo, la prise de photo d'un réseau social, le rajeunissement d'une photo d'un adulte et des photos prises durant la perpétration d'actes sexuels réels. Derrière chaque production d'un matériel d'abus sexuels sur mineurs se cache un processus de victimisation sans fin touchant profondément les victimes. Internet et les IA MASE ont créé une criminalité nouvelle où la violence change de nature. Le contenu une fois mis en ligne devient immaitrisable et génère des traumatismes chez l'enfant. Dans cette section, nous allons spécifier les principaux dommages possibles à la suite de la création, la consommation, l'échange ou la détention de MASE.

Les crimes liés aux MASE sont considérés comme des infractions entraînant une revictimisation continue et une prolongation du préjudice. Les préjudices ne se contentent pas d'apparaître lorsqu'un matériel a été créé, mais interviennent aussi lors de son échange et sa détention. Ils concernent aussi l'exploitation d'une image initiale pour créer de nouveaux scénarios (Bourcelet, 2024). La création de contenu via l'IA peut victimiser ou revictimiser un enfant réel par l'utilisation de ses images pour entraîner l'intelligence artificielle. Selon A. Trivision (2024), les MASE attisent également l'appétit sexuel des consommateurs. Donc, l'impact sur l'enfant est constant, c'est-à-dire qu'une fois que le contenu a été partagé sur les plateformes, l'image y reste indéfiniment et peut être repartagée perpétuellement. Ce processus s'effectue notamment au moyen des *deepfakes* dont nous avons précédemment expliqué le mécanisme (Bourcelet, 2024 ; Bourcelet & Mathieu, 2025 ; Ende, 2025 ; Trivision, 2024). Le préjudice subi à cause des IA MASE peut également dépasser la victimisation et revictimisation. Les images synthétiques normalisent la violence sexuelle à l'égard des enfants. Selon l'IWF, l'IA permet une certaine normalisation des comportements déviants, et plus précisément par l'utilisation de *chatbots*. Les *chatbots* sont des outils conversationnels qui peuvent fournir des informations sur comment commettre un abus sexuel ou simuler des conversations sexuelles avec des enfants. Les préjudices ne s'arrêtent donc pas à ce que nous avons exposé ci-dessus. Ils concernent également la croissance de l'exploitation sexuelle d'enfant au départ d'une normalisation des abus grâce à l'IA (IWF, 2024, ; IWF, 2026 ; Ó. Ciardha et al., 2026).

Malheureusement, la victimisation et la banalisation d'un comportement déviant ne sont pas les seuls préjudices possibles. C. Ciardha et al. (2026) mettent en évidence sept

préjudices dus aux IA MASE : la représentation de vrais enfants, la coercition, le grooming, traduit par pédopédiage qui consiste à piéger un enfant en ligne, souvent par le biais de manipulation (Dakota Szyf et al., 2023) et l'extorsion sexuelle, la normalisation et la désensibilisation, la porte d'entrée vers la délinquance, la création du contenu par les jeunes pour exploiter les pairs, la protection inégale et la difficulté de détection et finalement, le profit généré par la production. Force est de constater que l'impact sur les enfants est tel que ceux-ci se sentent traumatisés et trahis. Ce traumatisme est aussi mesurable socialement, lorsque ce genre d'images apparaît sur Internet, cela entache leur réputation. Même si dans certains cas, l'enfant n'a pas été abusé physiquement, ces comportements délictueux sont considérés comme étant contre le droit des enfants et affectent leur santé mentale (Ende, 2025.). Les conséquences de ce type de contenu ne se limitent donc pas à la potentielle victime, mais engendrent également des effets négatifs sur la société toute entière (M. Ngo et al., 2022 ; Bourcelet & Mathieu, 2025.).

Nos observations et nos conclusions se rallient aux auteurs qui déclarent que l'intelligence artificielle est un agent facilitateur pour commettre un crime, parfois déjà existant, mais sous une autre forme (Mouheb, 2024 ; Police Fédérale - DJSOC FCCU, s. d.). Ainsi, dans le point suivant, nous envisagerons le marché de ces images sur les plateformes afin de comprendre l'organisation d'un commerce qui semble bien rodé.

Partie 5. Un véritable marché sous-terrain

« Quand une société réifie ses enfants en les transformant en groupe de consommateurs, quand elle les déshumanise en les convertissant en un produit jetable, elle n'a plus qu'à les accuser des maux qu'elle a elle-même engendrés. »

(Banks, 2011, cité par Bonnet, 2021, p.113)

À travers ce chapitre, nous voulons montrer l'organisation du marché des MASE. Pour ce faire, cette partie envisagera la question du rôle des plateformes permettant l'échange des MASE, et la reconfiguration imposée par l'avènement de l'IA. Nous allons également aborder le Clear web et les darknets, endroits rendant l'échange des MASE et des IA MASE possibles. La création d'une économie autour de l'exploitation sexuelle des enfants pose de réelles questions sur la manière dont circulent les MASE sur Internet. Une monétisation s'installe autour des enfants, il devient de plus en plus difficile de la contrôler et de l'arrêter (Mandloi, 2025). Nos réflexions seront accompagnées, lorsque cela est pertinent, d'extraits d'entretiens que nous avons réalisés.

Les plateformes : un lieu privilégié de distribution de MASE

Le Clear Web et le Dark Web

Dans la toile du web, nous trouvons plusieurs « couches » : d'abord le Clear web ou le web de surface reprend les sites accessibles de tous. Ensuite, les darknets, apparus dans les années 90, sont des réseaux anonymisés, en dehors des référencements et des moteurs de recherches. Ils sont alors inaccessibles à partir d'une recherche classique. Ces réseaux servent parfois à dissimuler des pratiques illégales. Le Darkweb, seulement accessible via les Darknets, renvoie souvent à des pratiques illégales et un Internet caché. Enfin, le Deep web/Deep net concerne les sites non indexés par les moteurs de recherche comme l'accès aux applications bancaires. Le Deepnet regroupe des pages accessibles librement sur Internet, mais qui n'apparaissent pas sur les moteurs de recherche (Robin, 2021 ; *Darknet, Dark Web, Clear Web ou Deep Web ?*, 2022).

Internet héberge des réseaux peer-to-peer (P2P) qui permettent à des utilisateurs de collaborer, de se connecter et d'échanger des fichiers. Le P2P est gratuit et accessible publiquement. Ces réseaux sont plus anonymes que d'autres réseaux de communication et ne nécessitent parfois même pas de contact direct avec la personne pour échanger du contenu. À titre d'exemple, ARPANET dont nous avons discuté plus tôt serait un réseau P2P (Musiani, 2020 ; Lee et al., 2020).

Au départ, les MASE s'avéraient difficiles à produire et à s'échanger, mais grâce aux évolutions des technologies, la plupart des échanges de ce contenu repose désormais sur les réseaux de communications et sur le P2P. En 2024, la Fondation pour l'enfance nous alertait déjà de la facilité déconcertante avec laquelle il était possible de trouver du contenu pédocriminel sur le Clear web. Les moyens de communication concernés ne sont pas toujours les plus connus comme Instagram ou Tiktok, mais concernent de petites applications moins connues telles que Gnutella, un site dédié au partage de fichiers. En 2026, L'IWF, dans son rapport sur les IA MASE, pointe que ces contenus se trouvent sur le Clear web et sur le Dark web. Ainsi, les IA MASE ne sont pas présentes seulement sur le Dark web, elles le sont aussi sur les RS, sur les sites d'échange de contenus ou sur les plateformes à abonnement (Fondation pour l'enfance, 2024 ; Holderness, 2024 ; IWF, 2026).

L'illégalité de ce commerce amène les criminels à prendre des mesures de sécurité importantes notamment l'utilisation de réseaux prévus à cet effet. Le moyen le plus courant pour se cacher est d'effectuer le trafic sur le Dark Web, le réseau le plus courant pour y accéder est The onion router (TOR). Ce ne sont pas les seuls moyens pour anonymiser les utilisateurs, il existe des P2P comme BitTorrent ou encore les communications chiffrées de

bout en bout, car elles procurent des garanties de sécurités pour héberger paisiblement des échanges de MASE. Les pédocriminels utilisent ces réseaux parce qu'ils y trouvent un avantage. Nous allons tenter de comprendre ce qu'offre concrètement le Clear Web et le Dark Web pour les consommateurs de MASE (Lykousas & Patsakis, 2025 ; Robin, 2021).

La face visible

Sur le Clear web se déroule ce que N. Lykousas & C. Patsakis (2025) appellent le multi level marketing. Celui-ci se déploie donc à la vue de tous sur le Clear web qui se voit employer comme moyen d'accès à des plateformes et des contenus. Selon l'auteur, ce processus se déroule en plusieurs étapes. Les criminels offrent du contenu gratuit, tout en réservant du contenu plus explicite pour des personnes privilégiées. Ces personnes accèdent à ce contenu soit en payant, soit en parrainant d'autres personnes via des liens, parfois trouvables en commentaire YouTube. Elles débloquent alors du contenu d'une valeur pouvant aller jusqu'à une centaine d'euros. En pratique, les sites Internet utilisés possèdent une courte durée de vie pour éviter d'être fermés par les autorités. Ils sont composés de noms de domaine qui sont la plupart du temps des combinaisons aléatoires qui leur confèrent une certaine sécurité. Pour garantir l'anonymat, les utilisateurs ont recours à de faux comptes ou à des comptes piratés pour diffuser les contenus au plus grand nombre possible. Ce partage permet donc aux criminels de bénéficier de contenus « supérieurs ». Le partage sur Internet donne l'opportunité aux criminels de retrouver les contenus par des mots clés spécifiques utilisés dans le but d'éviter les détections. En ce qui concerne les contenus générés par IA, ils sont alors utilisés comme contenu promotionnel, renvoyant sur des plateformes comme Telegram ou sur des RS tels que X. L'auteur signale que son analyse a été faite sur une conversation Reddit⁸ où un utilisateur aurait offert le modus operandi de la distribution de MASE sur le Clear web. Il apparaît que plus les liens contenant les adresses Discord, Telegram sont ouverts et partagés, plus la personne reçoit de récompenses. Les liens renvoient à des adresses qui offrent alors du contenu moyennant un paiement. Le monde de la cybercriminalité a donc saisi l'opportunité que l'IA lui offrait, c'est-à-dire de pouvoir maximiser les gains relatifs à l'exploitation d'enfants (Police Fédérale - DJSOC FCCU, s. d.). Le phénomène se passe de façon déguisée et avec des mots codés, mais il s'avère très simple de trouver des liens pour avoir accès à des images d'abus sexuels sur mineurs générées ou non par l'IA. Ce processus est peu conscientisé par l'utilisateur lambda du web. L'IA semble être ici utilisée plutôt comme vitrine d'un réseau très complexe et comme élément facilitateur. Ainsi, les pédocriminels n'ont alors plus besoin d'être expert en informatique pour consommer ce type de contenu. (Fondation pour l'enfance, 2024) Le

⁸ Reddit est un réseau social où il est possible de créer et de partager du contenu (*What Is Reddit*, s. d.).

Clear web est utilisé presque systématiquement comme devanture avec les RS et avec de faux profils renvoyant vers des messageries cryptées. Sur le Clear Web, les messageries sont adoptées comme moyen de contact pour distribuer le contenu contre paiement ou services d'abonnement comme Onlyfans⁹. (Fondation pour l'enfance, 2024).

Les réseaux sociaux

[...] plus on constate qu'il y a 2 ans maintenant que même dans les médias sociaux tu vois de plus en plus des images créées IA qui sont distribuées via les médias sociaux avant 2 ans, une ou 2 par an, maintenant on a une augmentation de 10-15 %. Parce que les techniques possèdent des outils pour créer l'IA, c'est assez facilement accessible, donc beaucoup de jeunes les utilisent pour faire le con [...]

Personne travaillant à la police fédérale

Les images générées par IA envahissent nos RS. Europol explique que, cette année, les contenus générés par IA auront atteint 90 % du contenu trouvable en ligne (European Parliamentary Research Service & Negreiro, 2025). Plusieurs raisons sont à l'origine de cette augmentation nous raconte la police, des raisons non sans conséquences pour la propagation de MASE. Dans le cadre des échanges de MASE, le Clear web et ses RS constituent donc une voie d'accès aux vendeurs pour promouvoir la vente de MASE (Holderness, 2024). Les RS les plus utilisés pour partager et visionner le contenu MASE seraient Instagram, Tiktok et discord (Fondation pour l'enfance, 2024). L'une des personnes interrogées déclare que les contenus pédocriminels s'échangent également sur des plateformes dont le but premier n'est pas seulement de communiquer, mais parfois d'écouter de la musique.

[...] Donc ça veut dire que bien sûr que des auteurs vont d'abord chercher sur des plateformes où ils savent qu'il y a beaucoup de jeunes, ça peut être des plateformes sociales, mais ça peut être du gaming plateforme, ça peut être des plateformes dans lesquelles on sait que des jeunes cherchent de l'aide. Maintenant aussi je sais pas si vous avez vu dans la presse, mais Child Focus a sorti avec un développement qu'on a vu aussi l'utilisation du Spotify donc là même si c'est une application pour de la musique, il y a des comptes avec des images ou avec des textes de musique qui donnent des indications qu'il s'agit des enfants [...]

Personne travaillant chez Child Focus

Cela révèle quelque chose de fondamental, à savoir que les RS sont utilisés comme un moyen de distribution et comme source pour créer des MASE. Ils deviennent donc des

⁹ Onlyfans est une plateforme qui « permet de payer pour du contenu via un abonnement mensuel ». C'est également une plateforme rencontrant un certain succès au près de créateurs de contenu pour adultes (*Qu'est-ce Que le OnlyFans ?*, s. d.)

facilitateurs de commerces illégaux. Ce constat est également apparu comme un élément saillant à travers notre entretien avec la police.

[...] ce qui se passe en fait donc ils prennent des photos des réseaux sociaux et ils commencent à les manipuler en fait donc les poster sur les plateformes Dark Web ou end-to-end encrypted¹⁰ et donc il y a un vol d'image énorme qui est en cours [...]

Personne travaillant à la police fédérale

Ce passage témoigne de l'utilisation qui peut être faite des RS. Ceux-ci constituent alors une source pour les pédocriminels. À la base, ces images présentes sur les RS proviennent parfois du *sharenting*, c'est-à-dire des parents qui publient des photos de leurs enfants en ligne. La police fédérale alerte sur les dangers de cette pratique en ce que les photos publiées sont utilisées pour créer des *deepfakes* ou *deepnudes* des enfants de manière totalement invisible. Les images créées sont alors exploitées pour commettre d'autres crimes comme la sextorsion (chantage sexuel pour de l'argent), le revenge porn (diffusion non consentie d'une image à caractère sexuel) ou le pédopiégage. (*Les Risques du Sharenting : Pourquoi Il Vaut Mieux Y Réfléchir À Deux Fois Avant de Partager En Ligne des Images de Nos Enfants*, 2025 ; Niestadt & European Parliamentary Research Service, 2025)

Le *sharenting* a fait l'objet d'intérêt médiatique de la part de la presse belge nous annonçant que les photos d'enfants présents sur les RS alimentent les images qui circulent sur « les plateformes clandestines ». Ces journaux rapportent que le danger serait amplifié par l'IA. Ces propos sont aussi développés dans un article de la RTBF, les photos d'enfants postées par leurs parents ou eux-mêmes, une fois publiées, se perdent dans Internet. Plus largement, ces indications soulèvent des interrogations : comment ces images circulent-elles sur les médias ? Les médias seraient-ils alors responsables des contenus qui se trouvent sur leurs plateformes ? Nous répondrons à la question de la responsabilité dans notre partie sur la législation. Ici, nous allons examiner comment les événements se déroulent en pratique (Ladouce, 2025 ; Niestadt & European Parliamentary Research Service, 2025 ; Simonart & Damman, 2025).

L'échange de contenu apparaît alors dans les messageries, les groupes, les appels vidéo, l'échange de dossiers et par post ou référencement (Holderness, 2025). Par exemple, les plateformes comme X et Instagram sont plutôt utilisées pour le grooming. En 2023, le Média Arte nous rapporte qu'une plainte aurait été déposée contre Meta, maison-mère d'Instagram pour avoir fermé les yeux sur la pédocriminalité qui se déroule sur ses RS. Les journalistes d'Arte ont donc décidé de mener une enquête dont les conclusions se sont

¹⁰ End-to-end encrypted, traduit par chiffrée de bout en bout.

avérées très inquiétantes. En effet, grâce à une recherche à base de mot clé tel que « cp » (pour *child pornography*), l'ajout de x dans le nom de profil, il a été possible de découvrir des centaines de comptes Instagram qui vendent des MASE. Dans ce documentaire, les journalistes démontrent qu'il leur a été possible de craquer l'algorithme pour finalement n'avoir plus que des vidéos d'enfants dans le fil d'actualité. Les suggestions produites par l'algorithme permettent aussi de mettre en contact des criminels tout en les conduisant vers le même type de contenu (Bracket Foundation, 2024). Ainsi, tous les contenus trouvés sur les RS peuvent à chaque fois être pris pour être modifiés par une IA (*Pédocriminalité : Les Failles D'Instagram - la Méthode*, 2024 ; *Pédocriminalité, les Failles D'Instagram | Sources | ARTE*, 2024). Malheureusement, Instagram n'est pas le seul site à fermer les yeux sur les contenus de sa plateforme. Pornhub a été accusé en 2020 de laisser circuler des médias d'exploitation d'enfants sur ses plateformes, notamment des viols. Jusqu'en 2020, ce site permettait de télécharger du contenu, il devenait donc impossible de savoir ce que devenaient ces vidéos. Il était aussi accusé de stocker des enregistrements de viols d'enfants. Comme nous l'avons montré, dans ce type de trafic cela profite aux sites Internet, mais aussi aux banques. En réaction à la poursuite envers Pornhub, Visa et Mastercard ont décidé d'arrêter leur partenariat avec cette plateforme (*Notes des Comités Parlementaires : Exploitation Sexuelle D'enfants Sur Pornhub*, 2021). Le développement d'Internet et des RS a impacté considérablement l'échange des MASE en ligne.

Nous constatons que la démocratisation des RS comme mode de diffusion et de partage d'information impacte la commission des infractions présente sur ces plateformes. Les MASE seraient alors une des catégories les plus affectées par l'accessibilité des outils de communication (Holderness, 2024). Un autre phénomène lié directement à la démocratisation des RS vient alimenter les contenus qu'il est possible de trouver. Cela se passerait généralement de deux manières, soit un jeune prend une photo tirée des RS pour la dénuder grâce à l'intelligence artificielle, ce qui conduit parfois à des menaces, du harcèlement, etc. ; soit les jeunes s'échangent entre eux des nudes¹¹ qui sont parfois utilisés pour du revenge porn et qui tombent entre les mains de pédocriminels.

Pas mal de diffusion de nudes qui se font entre jeunes, donc qui rentrent aussi dans cette catégorie de diffusion d'images de pornographique, que l'image été envoyée au départ de manière volontaire ou qu'elle ait été prise à l'insu de la personne. Et puis alors qu'il véhicule dans les classes dans un groupe d'amis, etc. Donc ça, c'est aussi une problématique qu'on rencontre souvent. [...] Oui parce qu'ils font souvent transiter par des plateformes qui ne sont pas sécurisées pour lesquelles ils n'ont pas toujours les bonnes notions parce que combien de jeunes utilisent un ordinateur familial et enregistre les images directement sur l'ordinateur... ils ne se rendent pas compte qu'en fait tout est automatiquement enregistré dans le cloud. Et donc potentiellement on pourrait se retrouver avec un

¹¹ « Autoportrait numérique dénudé » (« Nude », s. d.).

signalement pour ces images et donc ces images qui se retrouvent un peu ouvertes à d'autres personnes et donc effectivement, c'est en tout cas le message que mes collègues font passer aux jeunes c'est en fait parfois quand toi tu fais partir une photo, tu ne sais pas où elle va aller, jusqu'où elle peut aller.

Criminologue de parquet

Lorsqu'Internet a facilité l'accès à la pornographie, il a aussi permis aux générations actuelles d'être exposées à des contenus à caractères sexuels. Les jeunes qui créent des *deepfake* ou qui nudifient des photos voient parfois cette action comme une blague ou encore de la curiosité sans se douter des conséquences. Entre eux, ils s'échangent alors les photos parfois dans le but de harceler des camarades de classe (Hotz, 2026). Ces agissements concernent plus souvent de jeunes filles et entraînent des effets considérables sur la santé mentale. Toutefois, les jeunes ne se rendent probablement pas compte de l'impact réel de l'utilisation de l'IA générative.

Les messageries chiffrées de bout en bout : le paradis des pédocriminels

Selon plusieurs sources, la pandémie du covid 19 aurait augmenté l'exploitation sexuelle des enfants, dont la distribution, consommation et production de MASE facilités par la technologie. L'augmentation serait due également à la propagation de messageries chiffrées de bout en bout. En 2024, selon le rapport annuel fait par INHOPE, le réseau de lignes d'urgence qui œuvre pour éliminer les MASE d'Internet, rapporte que les plateformes de messages chiffrés ont gagné en popularité. (INHOPE, 2024 ; Karagoz et al., 2025 ; Lykousas & Patsakis, 2025 ; Salter & Wong, 2024) L'émergence de ces nouveaux réseaux pose alors des difficultés pour le contrôle lié à ces images. L'interviewé nous indique aussi que les messages chiffrés de bout en bout (end-to-end encrypted) sont les plus utilisés. (Lykousas & Patsakis, 2025).

C'était Instagram et Facebook et maintenant c'est plus ça, ils sont descendus vers la 10e place. C'est plutôt Snapchat. Et naturellement, le fait que tout le monde sait que WhatsApp est end-to-end encrypted, on va utiliser WhatsApp. [...] Surtout sur les applications. Par exemple, on a fait Telegram, avec tout ce qui s'est passé avec Telegram et l'arrestation du CEO. On constatait ça aussi dans le domaine numérique. Du coup Telegram n'était plus populaire, c'était devenu Telegard, peut-être au Simplex, etc. Donc, mais c'est très très dynamique en fait ces environnements qui ont, il y a l'émergence de nouveaux réseaux et réseaux aussi qui ne sont pas forcément les mêmes.

Personne travaillant à la Police fédérale

Cela donne aussi des messageries très sécurisées où il est possible de cacher les méfaits. Bien que la littérature n'ait pas fait transparaître ce côté dynamique, les plateformes et les messageries utilisées se renouvellent continuellement ajoutant de la difficulté au travail des policiers. Le problème des conversations chiffrées de bout en bout nous est

raconté par une personne travaillant à la police fédérale (Negreiro & European Parliamentary Research Service, 2020).

[...] ce qui se passe, c'est que vous allez avoir une partie de la clé que l'émetteur va garder et une partie de la clé qui va être envoyée au récepteur et tout le long du chemin, vous ne saurez pas lire ce qui est imaginons que la communication va passer d'ici vers une personne. C'est un câble blindé, vous pourrez pas écouter donc les techniques pour déchiffrer sont soit d'avoir la clé, soit ce qu'on appelle un Man in the middle, l'attaque d'homme du milieu et donc avoir réussi à placer quelque chose sur le chemin qui lui va être dans le flux de l'info et avoir les données. Donc comme nous on n'a pas ça, si c'est chiffré de bout en bout, on ne sait pas trouver la solution ou alors il faut des puissances de calcul démentiel, mais qui sont certainement pas à notre disposition. [...] Si vous savez rentrer dans le groupe, vous pouvez regarder des infos. Parfois, il y a des clés de chiffrement qui sont disponibles et donc on peut avoir accès de déchiffrements qui sont disponibles, on peut avoir accès, mais souvent c'est pour ça qu'il y a beaucoup de pays dont la Grande-Bretagne qui force à ce niveau-là, mais il y a eu deux sujets à la Commission européenne récemment aussi, même si le projet loi été refusé pour interdire le chiffrement de bout en bout. [...]

Personne travaillant à la police fédérale

Nous comprenons donc qu'il est presque impossible sans la possession d'une clé de déchiffrement spécifique de rentrer dans une messagerie cryptée et d'y découvrir les données. Cette possibilité de communication entre les auteurs permet la discrétion et la sécurité. En conséquence, cela fait de ces applications chiffrées un véritable paradis pour commettre l'infraction (Negreiro & European Parliamentary Research Service, 2026 ; Lykousas & Patsakis, 2025). Le stockage cloud partage les mêmes avantages que les messageries chiffrées de bout en bout. Cela englobe les téléphones ou encore les USB qui gagnent en popularité chaque année pour la détention des MASE. L'avantage du cloud réside dans la quantité d'information téléchargeable, et il permet aussi un accès privé. D'autant plus que certaines grandes industries ne pratiquent pas encore la détection dans les cloud (Negreiro & European Parliamentary Research Service, 2020).

La face cachée

Pour accéder au Dark web, les utilisateurs doivent passer par des darknets, que nous avons expliqués plus haut. The Onion Router plus connu sous le nom de TOR est un réseau qui fournit une anonymisation, un domaine, la sécurité et une vie privée sur Internet. Il est le choix le plus fréquent pour passer sous la surveillance. Son utilisation n'a pas toujours une visée criminelle, il est parfois employé pour protéger les utilisateurs à risque comme les femmes ayant vécu des violences conjugales, le travail journalistique... Concrètement, TOR fonctionne en détournant les adresses IP des utilisateurs sur d'autres serveurs, cette manipulation rend la traçabilité de l'adresse de départ presque impossible. Ils deviennent de

ce fait les vecteurs idéaux pour des milliers d'individus souhaitant échanger librement sur leurs intérêts sexuels envers les enfants sans craindre d'être identifiés. Europol a aussi estimé que les réseaux P2P tels que TOR restent les lieux principaux pour l'échange. Plus encore, l'anonymat permet aussi d'accentuer d'autres comportements sur Internet tels que le harcèlement, les menaces, le racisme et l'homophobie. (Robin, 2021). Les Darknets ne sont pas sans conséquence sur le travail des autorités qui voient leurs tâches se complexifier avec les années. L'anonymat et l'absence de traçabilité entraînent une certaine liberté auprès des criminels. En effet, les données y sont cryptées et les outils sont également mis en place pour les aider dans le trafic. La manière pour une personne de se procurer ce type de contenu est également possible via les sites de peer-to-peer (P2P) (Lykousas & Patsakis, 2025).



!!! cum eaters !!!	68
!!! G O O N !!!	15
!!! LGBTQ+ !!!	396
!!! PAWS !!!	5
!! Sisk Idiots !!	16
! Italo Disco	36
! meow chat :3	55
!!! 90's Rare Riddim !!!	16
!! COLI SHOTA CUB ROOM!!	22
!! RIDDIM !!	16
! _~* A L I E N S *~_!	9
! ReGGaeGaLaXy	12
! Roots Archives!	8
#ANTI-FASCISTS	36
#ANUS	8
#CORONAVIRUS	20
#Femboys	7
#Horrorcore	9
#iciombre-hardcore	10
#La France	62
#polska	47
#vegan	10
\$\$RARE RAP MUSIC\$\$	21
+Autism+	57
+BlackMetal+	140
+HIP_HOP_SCENE_RELEASES...	25
+UndeadPurgatory+	8
/mu/	140
18+ Dirty XXX Music!	8
70 Rare groove Soul Jazz	16

Image extraite des salles de chat du site de P2P, Soulseek.

Ces derniers se sentent alors plus libres d'exposer et d'échanger directement sur leurs préférences sexuelles (Acar, 2017 ; *Child Sexual Exploitation*, s. d. ; Gannon et al., 2023 ; Nurmi et al., 2024 ; Robin, 2021). Le Dark web constitue pour ces personnes un terrain propice pour nourrir leurs déviances. A. Trivision (2024), dans une étude menée aux États-Unis, signale que la plupart du contenu produit par IA trouvé sur le Dark web provient de modèles *open source*, modèle facilement modifiable par les utilisateurs. Lors d'un de nos entretiens, la police nous signale que le Dark web contient des plateformes ayant seulement pour but d'échanger sur la pédocriminalité (Fondation pour l'enfance, 2024).

Il y a des plateformes Dark web uniquement consacrées à l'échange d'informations concernant l'IA et l'IA qui est utilisé pour des faits de pédocriminalité.

Personne travaillant à la police fédérale

Comme mentionné précédemment, nous trouvons des MASE sur le Clear web et le Dark web. Sur le Dark web, cela se construit plutôt autour du processus créatif sur l'utilisation de l'IA (IWF, 2026). Par exemple, les utilisateurs peuvent créer des manuels de pédophile, accéder à des conseils sur la manière de générer une image à partir d'instructions précises. Admettons qu'un individu ne soit pas familier avec l'utilisation de l'IA, celui-ci trouvera toujours quelqu'un pour l'aider à la manipuler. Passons maintenant à l'explication d'une organisation concrète d'un darknet qui fait circuler des MASE. À l'intérieur de ces forums s'installe une hiérarchie allant des administrateurs aux membres. Chaque poste a des compétences particulières et donne accès à des contenus différents. Les personnes les plus importantes opèrent une modération du contenu qui se trouve sur le réseau. Ces espaces ne sont pas seulement faits pour échanger du contenu, mais aussi pour discuter de passage à l'acte (Gannon et al., 2023). Nous supposons qu'une quête à acquérir un certain statut peut motiver certains individus à commettre des infractions. Les policiers pensent que les criminels payaient par cryptomonnaie pour accéder aux forums sur le Dark web et ainsi, télécharger des MASE (*28 Arrests In International Strike Against Child Sexual Exploitation*, 2026).

La consommation

Nous avons vu qu'Internet avait facilité la communication entre les individus, la circulation de l'information et l'expansion des matériels d'abus sexuels sur mineurs. Pour comprendre, comment une consommation d'images d'abus d'enfant s'installe, nous allons situer la première consommation, y compris ses conséquences et l'installation des MASE comme un bien économique.

5.2.1 Un « accident » aux lourdes conséquences

Une étude quantitative menée par S. Napier et al. (2025) nous interpelle sur la première consommation de MASE. Elle montre qu'une partie importante des répondants a été exposée à ces contenus illicites en étant mineure, ces expositions intentionnelles et surtout, l'exposition de mineurs constituent un réel problème. Les utilisateurs Reddit témoignaient d'une désensibilisation progressive les amenant à chercher un effet « choquant » lors du visionnage de la pornographie et à envisager l'attirance envers les enfants comme normale (Eelmaa, 2022). Dans cette même lignée, J. Nurmi et al. (2024) précisent que l'utilisation problématique de la pornographie légale conduit parfois à terme à la consommation d'images d'abus sexuels sur enfants. Par exemple, le site Pornhub, réputé pour héberger des MASE, contient des vidéos sous des catégories nommées « jeunes » ou « adolescence » (Wortley et al. 2024). Les auteurs Napier S et al. (2025) et N. Lykousas et C. Pastakis (2025) précisent qu'une exposition aux MASE peut arriver « par accident » et

ont constaté que les femmes sont plus susceptibles d'être exposées involontairement à un type de pornographie sortant du « normal », tandis que les hommes recherchaient les MASE intentionnellement. Cette différence est à son tour soulevée par C. Benouamer et al. (2026) qui remarquent que les principaux consommateurs seraient des hommes là où les femmes ne représenteraient qu'une faible partie des consommateurs et plutôt dans un contexte de co-délinquance. Ces propos nous sont également rapportés par une criminologue de Parquet et permettent d'éclairer sur ce caractère accidentel.

Mais l'idée du pédocriminel, même là pour moi c'est pas tout à fait juste parce qu'il y a aussi toute une série de personnes pour lesquelles il y a une grosse consommation de contenu pornographique et dans lequel se noient parfois des images à contenu pédopornographique, sans forcément les rechercher au départ, mais parce que ça répond à un besoin au départ de s'alimenter en fantasmes divers et variés. Ils consomment sans avoir toujours vraiment ce qu'on va appeler la pédophilie... pour les mineurs. C'est pas toujours le cas et d'ailleurs c'est très souvent de gros consommateurs de contenus pornographiques qui se retrouvent comme ça un moment donné avec. On n'a pas beaucoup d'images d'ailleurs c'est très symptomatique ce qu'on voit, c'est des dossiers où on va avoir peut-être une ou deux images dans tout leur matériel qu'on va pouvoir retrouver dans le contenu, dans l'ordinateur ou dans le téléphone. Ce seront les seules images pédopornographiques qu'on retrouvera, mais elles se sont perdues dans une masse, les gens qui consomment de manière un peu compulsive et donc se retrouvent à consommer par mégarde.

Criminologue de parquet

Même si la première exposition arrive parfois accidentellement, nous avons vu précédemment que l'augmentation de la distribution de MASE coïncide avec la création des messageries chiffrées de bout en bout facilitant les échanges et la consommation. Selon la Fondation de l'enfance (2024), le caractère virtuel des images générées par l'IA entraîne une normalisation et une banalisation qui sont également alimentées par une consommation croissante de la part des usagers (Lykousas & Patsakis, 2025). Cette normalisation passe par les technologies qui facilitent alors l'infraction. Cette dernière nécessitait auparavant d'avoir un contact potentiel avec une victime. Quant à l'IA, elle descend les barrières psychologiques qui pouvaient être présentes, rendant la production de contenu illégal plus supportable. Elle offre aussi la possibilité aux pédocriminels de générer des contenus extrêmes avec facilité (IWF, 2026). La banalisation est impactée d'une part par le côté immatériel des images IA et d'autre part par une volonté de rendre l'infraction moins grave. Cet aspect est également mis en lumière par une étude menée à travers des récits de vie de consommateurs. Les participants avaient tendance à se distancier du caractère illégal de leurs actes parce qu'ils ne les considéraient que comme de simples images. Pourtant, ces médias concernaient bel et bien des enfants « réels ». La distanciation présente par le simple fait que

cela soit des images, interroge d'autant plus lorsque ces images sont générées complètement par IA. Cet aspect amènerait alors à une minimisation, un processus qui est souvent constaté chez les consommateurs d'images IA (Pugnière-Saavedra, 2018). Les consommateurs de MASE en ligne sont notamment appelés cyberpédocriminels et selon la Fondation de l'enfance (2024), ils auraient un comportement se rapprochant de l'addiction. Les pédocriminels sont alors pris dans des comportements compulsifs de collections des MASE par âge, genre, type d'acte sexuel et fantasme (Nurmi et al., 2024). Ce comportement entraîne, de la part de ces consommateurs, une recherche de contenus nouveaux et toujours plus violents et extrêmes (Fondation pour l'enfance, 2024). Ce processus est déjà bien connu des services de police.

Violence plus décomplexée, on va dire. Et encore les victimes de plus en plus jeunes aussi. Il y a 20 ans, l'âge moyen était de 11 ans, maintenant c'est 4-5 ans l'âge moyen de votre victime. Et avec IA, tu peux décider quel âge a votre image

Personne travaillant à la police
fédérale

La descente de ce seuil d'âge interroge par rapport à ce qui a été exposé précédemment. Nous pouvons alors nous poser la question si cette descente est liée à la banalisation et à la normalisation croissante.

5.2.2. Les MASE : quand l'horreur devient rentable

Retraçons un bref historique, avant Internet, nous l'avons vu, les échanges ne s'effectuaient que de personne à personne, n'empêchant pas ce marché d'atteindre des sommes conséquentes. Cependant, ils étaient plus faciles à contrôler. Avec l'arrivée d'Internet, les personnes peuvent stocker plus et payer moins cher. Le cyberspace devient alors le lieu de prédilection pour échanger ces MASE. Selon K. Acar (2017), l'exploitation sexuelle des enfants en lignes ne représente plus une priorité. Pourtant, nous verrons qu'énormément de législation encadre ce phénomène et des mesures sont continuellement prises pour contrôler cette criminalité. Ces espaces économiques créés sur le Dark Web et le Clear Web sont alimentés à la fois par des acheteurs pédocriminels, mais aussi par la sextorsion qui implique souvent le paiement par un enfant afin d'éviter d'être affiché sur Internet (Childlight - Searchlight et al., 2025). Le chercheur P. Mandloi indique que l'opération Carbon réalisée en Inde a pu démontrer comment les criminels parviennent à gagner de l'argent avec le commerce des MASE. Le procédé se déroule comme suit : la création et le téléchargement sur des sites pornographiques, parfois rémunérés ; le contenu est ensuite téléchargé sur une plateforme gratuite qui touche une plus large audience, par exemple des RS ; ces réseaux utilisent des URL chiffrées pour le paiement ; ces étapes

rendent les médias difficiles à poursuivre. Ces changements de plateformes qui rémunèrent, permettent aux pédocriminels de recevoir un paiement à chaque fois que le contenu migre d'endroit. Les pédocriminels rentrent alors dans un cercle vicieux dans lequel l'exploitation sexuelle d'enfant devient un gain financier considérable. Les paiements sont souvent effectués sur des banques classiques ou pas cryptomonnaies. Le paiement était au départ effectué par carte bancaire et aidait donc à retracer les personnes derrière le virement bancaire. Désormais, les paiements s'effectuent souvent par bitcoin ce qui ne favorise plus la traçabilité. Le but est identique, c'est-à-dire enrichir le système (Mandloi, 2025). Un autre aspect qui fait grandir l'économie de ce système est la monétisation des RS par les abonnements et les publicités. Cette configuration pose de réels problèmes en ce que ces mécanismes permettent de dissimuler des contenus illicites tels que des MASE sur les RS. En ce qui concerne l'IA, elle ne vient que renforcer ce système et selon la Fondation de l'enfance (2024) un nouveau business émerge par le biais de l'IA générative.

Les abus sexuels sur les enfants sont un business. L'échange des MASE revêt une dimension économique qui est à prendre en compte quand nous voulons combattre ce crime. K. Acar (2017), dans son étude réalisée pour la police turque, nous explique que cet aspect économique du crime ne serait pas pris en compte de manière suffisante. Le contexte se présente comme suit ; alors que les autorités se concentrent à faire fermer les plateformes en ligne pour diminuer l'offre et la demande des MASE, les avancées technologiques fournissent de nouvelles manières de consommer rendant ces mesures inefficaces. Cela pose de réelles questions lorsque nous voyons la quantité de normes présentes pour légiférer et encadrer ce phénomène qui ne mentionne que très peu comment cadenasser cet aspect lucratif.

5.3. Les MASE sans frontières

L'enjeu international du commerce des MASE prend racine dans le fondement même d'Internet et des progrès technologiques. L'IA ne reconnaît pas non plus les frontières géographiques (Trivison, 2024). Le cyberspace, lieu dans lequel s'échangent les MASE, est un territoire sans périmètre avec des zones de non-droit. L'impression de ne posséder aucune frontière découle aussi d'une définition donnée au cyberspace : « l'Internet et l'"espace" qu'il génère : un espace intangible dans lequel s'opèrent des échanges déterritorialisés entre des citoyens de toutes nations, à une vitesse instantanée qui abolit toute notion de distance » (Douzet, 2014, cité par Pugnière-Saavedra, 2018, p. 1). Dans cette section, nous évoquerons la manière dont cette absence de frontières géographiques tangibles influence et renforce le commerce des MASE.

Le chercheur A.Trivison (2024), dans une étude menée aux États-Unis, précise à plusieurs reprises que l'augmentation des MASE générés par l'IA constitue un problème fondamentalement international dépourvu de barrières géographiques. Par conséquent, cela exige des gouvernements de tous les pays une coopération contre la problématique des images d'abus sexuels sur mineurs générées par l'IA. Ces propos sont aussi soulevés par E. Quayle et M. Taylor (2003) ils rapportent que les MASE représentent « une conspiration internationale complexe ». (p. 8) Cela se traduit surtout par une quantité importante de pays concernés par cette criminalité. N. Lykousas & C. Patsakis (2025) décrivent que pas moins de 110 pays étaient concernés par le marché des MASE, donnant à cette problématique un aspect global. INHOPE nous rapporte que les IA MASE et les MASE répertoriés à travers le monde mettent en lumière l'aspect global de cette problématique (INHOPE, 2024). En ce qui concerne l'Europe, elle est largement concernée par le commerce des MASE par son rôle actif dans la lutte contre cette criminalité et figure, en même temps, comme l'hébergeur principal de ces activités (Negreiro & European Parliamentary Research Service, 2026 ; Parti & Szabo, 2024). Les plus grands lieux d'hébergements de MASE seraient les Pays-Bas et les États-Unis. L'absence de frontière géographique implique également que lors des opérations policières de nombreux pays soient concernés. Tel était le cas pour l'opération CUMBERLAND menée par Europol en 2025 qui visait 19 pays, elle a été une des premières à concerner les IA MASE. (Negreiro & European Parliamentary Research Service, 2026) Une autre opération policière internationale « Kidflix » a démantelé, avec la collaboration de la police fédérale belge, l'une des plus grandes plateformes d'exploitation sexuelle d'enfant (*The Belgian Federal Police Contributes To An International Operation Against A Major Child Sexual Exploitation Platform*, 2025) Les MASE ont alors été découverts dans 86 pays soit 37 de plus qu'en 2020.

La portée internationale de cette criminalité impacte le suivi judiciaire. Le contenu poursuivi nécessite d'abord d'identifier la position géographique exacte de la commission de l'infraction. La tâche est complexifiée par des outils permettant de modifier voire dissimuler les coordonnées géographiques. Les auteurs sont parfois localisés dans des juridictions ou pays différents de ceux de leurs victimes rendant le traitement de l'affaire plus compliquée. C'est en tout cas ce que P. Bleakly et al. (2024) expliquent, lorsque l'auteur de l'infraction se trouve sous le même régime juridique que la victime, la poursuite judiciaire se déroule assez facilement. Pour pallier ces difficultés, la littérature recommande que les différents pays coopèrent face à cette criminalité. La coopération passe notamment par une harmonisation de la législation parfois lacunaire qui doit être renforcée par l'avènement de l'intelligence artificielle. Derrière ces luttes, des objectifs précis doivent être recherchés, la

protection des enfants (Mandloi, 2025; Negreiro & European Parliamentary Research Service, 2026 ; Parti & Szabo, 2024 ; ten Hulsen, 2025 ; Trivison, 2024 ; Westlake, 2019).

Partie 6. État des lieux réglementaire

Cette partie présente le périmètre des réglementations touchant directement aux thématiques de ce mémoire. Cette partie abordera conjointement les textes relatifs aux images d'abus sexuels sur mineurs, la protection de l'enfance et la vie privée. Dans un souci de concision de notre raisonnement, nous avons pris le parti de ne pas mentionner tous les instruments légaux disponibles pour ce sujet et nous nous sommes limités à offrir un éventail des fondements juridiques dans lesquels s'inscrit le phénomène des MASE.¹² Entrons dans l'examen des normes internationales, européennes et nationales concernant la problématique des matériels d'abus sexuels sur mineurs, dont ceux générés par l'intelligence artificielle.

Nous allons aborder des normes émanant d'organismes pouvant porter à confusion. À cette fin nous voulons distinguer le Conseil de l'Europe du Parlement européen. Le Conseil de l'Europe est l'organisation principale de défense des droits humains et se repose sur la Convention européenne des droits de l'Homme. Il a été créé en 1949 et compte 46 États membres. Cet organe adopte des traités ou Conventions, des Chartes, des accords et des recommandations et des résolutions. Le Parlement européen quant à lui, est composé de Chefs d'États et de gouvernements des États membres regroupant 705 députés des 27 pays membres. Il respecte la Charte des droits fondamentaux (*Le Conseil de L'Europe : Éléments Clés*, s. d. ; *Ne Pas Confondre*, s. d.).

Une première distinction doit être effectuée entre les instruments juridiquement contraignants (hard law) et non contraignants (soft law). De manière générale, les instruments dits de soft law sont principalement des accords, des principes ou des déclarations tandis que le hard law concerne des obligations légales qui lient les parties. Au niveau de l'UE, le règlement est directement applicable dans les États membres. La directive nécessite une transposition de la part des États impliquant donc que ceux-ci disposent d'une marge de manœuvre par rapport à la forme et aux moyens de la mise en œuvre. Les décisions sont obligatoires et lient les destinataires. Finalement, les réglementations et les avis ne sont pas obligatoires (*Hard Law/Soft Law*, s. d. ; *Instruments Juridiques de L'UE*, s. d.).

6.1. Les instruments universels

Quels sont les textes internationaux qui régissent le domaine des MASE ? À travers ce chapitre, nous allons retracer les différentes Conventions, notamment celles des Nations

¹² Nous renvoyons le lecteur à l'article Dabrowska (2025) Terminological Developments in the Criminalization of Child Sexual Abuse Material (MASE) in International and European Union Law, qui offre une version plus exhaustive des réglementations.

unies qui sont applicables dans le domaine des images d'abus sexuels sur mineurs, de protection de l'enfance et de cybercriminalité. Ces instruments ont pour effet de lier les États faisant partie et ont pour but de s'appliquer à travers le plus de pays possibles.

Tout d'abord, en 1989, la Convention des droits de l'enfant est adoptée et comporte les termes suivants « exploitation de l'enfant dans des performances et contenus pornographiques ». Cette convention a pour objectif de protéger l'enfant et le phénomène des MASE sans en donner une définition légale. Onze ans après l'adoption de cette convention, un protocole vient s'ajouter sur la vente d'enfant, la prostitution des enfants et la pornographie infantile. Les parties signant la convention doivent protéger les enfants de la production et distribution de MASE. Le protocole additionnel donne une définition de la pornographie mettant en scène des enfants comme « toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles »¹³. Ce protocole alarme aussi sur la croissance des MASE disponibles sur Internet, une croissance qui a fait l'objet d'une Conférence internationale à Vienne en 1999. La terminologie employée à l'époque, mentionnant « quelques moyens que ce soit » et « réelles ou simulées », fait en sorte que ce protocole ne soit pas totalement désuet à l'ère de l'intelligence artificielle. L'emploi de formules larges et/ou floues permet dans la réglementation d'avoir un large champ d'application et de s'appliquer à des situations nouvelles. En 1999, La Convention sur les pires formes de travail des enfants mentionne dans son article 3 que le recrutement d'un enfant pour produire du matériel pornographique constitue l'expression « les pires formes de travail des enfants ». Néanmoins, il n'apparaît pas non plus que les MASE soient définis dans cette convention.¹⁴ C'est en 2001, avec la Convention sur la cybercriminalité qu'un cadre complet apparaît afin d'encadrer la poursuite des images d'abus sexuels sur mineurs. Dans son article 9, la Convention exige des États membres qu'ils érigent en infraction la production, la mise à disposition, la diffusion, l'échange et la possession de contenu.¹⁵ Cette Convention donne aussi une indication sur le statut de minorité « “mineur” désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans. » L'établissement de cette réglementation visait à renforcer la coopération entre les États et à améliorer les poursuites. Les instruments universels ont été parfois précisés, adapté par de

¹³ Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, article 2, adopté le 25 mai 2000.

¹⁴ Convention internationale relative aux droits de l'enfant, signée à New York le 20 novembre 1989, approuvée loi du 25 novembre 1991, article 3, *M.B.*, 17 janvier 1992, pp. 803-826 ; Convention concernant l'interdiction des pires formes de travail des enfants et l'action immédiate en vue de leur élimination, signée à Genève le 17 juin 1999.

¹⁵ Convention du Conseil de l'Europe sur la cybercriminalité, signé à Budapest le 23 novembre 2001, approuvée par la loi du 3 août 2012, article 9, *M.B.*, 21 novembre 2012, p. 69092

la soft law pour aider les États parties dans l'adoption des réglementations (Bourcelet & Mathieu, 2025 ; Convention de l'Europe, 2024).

Il existe également des textes internationaux qui visent expressément à la protection de l'enfance, un enjeu fondamental dans la problématique des IA MASE. La charte des droits fondamentaux de l'Union européenne en son article 24¹⁶ et la Convention des Nations unies relative aux droits de l'enfant (CNUDE), préalablement cité, encadrent en partie la protection des enfants. Cela vient répondre aux demandes du Comité des droits de l'enfant qui, à l'ère du numérique, encouragent une protection des jeunes dans l'environnement d'Internet. L'objectif est alors de permettre la détection et le signalement pour protéger les intérêts des enfants.¹⁷ La Convention internationale relative aux droits de l'enfant (CIDE) reconnaît l'enfant en tant que sujet de droit et comme personne vulnérable. Cette reconnaissance amène la question de l'autodétermination sexuelle en ligne qui regroupe le respect de son autonomie et sa protection contre les risques liés au numérique. Le deuxième protocole de la CIDE adoptée en réaction à l'essor du matériel pornographique des enfants en ligne condamne la production, la diffusion, la détention et toute transaction.¹⁸ Ce protocole considère que les mineurs sont effectivement jugés plus vulnérables face à ce qui se passe en ligne. Pour protéger l'enfant de l'espace numérique, le Comité recommande des bases solides pour éviter la victimisation secondaire, expliqué dans la partie intitulée « des préjudices considérables » (Bourcelet & Mathieu, 2025). La protection passe également par l'autorisation d'effectuer la détection de contenu. Nous retrouvons également, en 2007, La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels¹⁹, également appelée Convention de Lanzarote qui condamne les infractions à caractère sexuel contre les enfants. Les États ont donc l'obligation de prendre des mesures pour protéger les victimes en prévenant l'infraction. Cette réglementation comporte également une définition de ce qu'ils appellent « la pornographie infantile ». La protection des enfants passe également par leur fournir un environnement en ligne plus respectueux et plus adapté. En 2022, la Commission européenne a publié une stratégie œuvrant dans ce sens avec « Better Internet for Kids » (IWF, 2026 ; Niestadt, 2025).

Plus récemment, en 2024, Les Nations Unies ont élaboré une Convention contre la cybercriminalité²⁰, et son article 14 intitulé « infractions relatives à des contenus en ligne

¹⁶ Charte des droits fondamentaux de l'Union européenne, signé à Nice le 7 décembre 2000, article 24.

¹⁷ Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, *C.O.M.* (2022) 209 final.

¹⁸ Convention internationale relative aux droits de l'enfant, signée à New York le 20 novembre 1989, approuvée loi du 25 novembre 1991, article 3, *M.B.*, 17 janvier 1992, pp. 803-826

¹⁹ Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, signée à Lanzarote le 25 octobre 2007, approuvée par la loi du 7 février 2012, *M.B.*, 21 juin 2013, p. 39977

²⁰ Convention contre la cybercriminalité, signée le 24 décembre 2024.

présentant des abus sexuels sur enfants ou l'exploitation sexuelle d'enfant » incrimine les auteurs et demande aux États de prendre des mesures concernant la production, la diffusion, la détention ou la publication de MASE grâce à des systèmes d'information et de communication. Cette Convention repose aussi sur la coopération entre les États pour poursuivre les objectifs prévus. À ce jour, ce texte n'est pas encore entré en application, les signatures sont encore ouvertes, et ce jusqu'au 31 décembre 2026 et ne pourra entrer en vigueur que 90 jours après le 40e État devenant Parties à la Convention, c'est-à-dire quand la signature est ratifiée ou acceptée. En l'état actuel, 78 signataires et 3 États sont Parties à la Convention. Pour la Belgique, elle a signé la Convention contre la cybercriminalité le 25 octobre 2025. La réglementation demeure encore loin d'atteindre les quotas pour entrer en application.²¹

À titre informatif, certains rapports de la Commission servent d'appui à la mise en place des réglementations par les Parties signataires. Par exemple, dans l'évolution de la définition de la pornographie enfantine, déjà en 2014, un rapport suggérait une modification du terme pédopornographie pour images/matériels d'abus sexuels sur mineurs (Dabrowka, 2025). Pour comprendre ce basculement, nous renvoyons aux explications dans notre partie une intitulée « Les abus sexuels sur mineurs : d'une image à l'autre » et plus précisément dans le point 2.2. « Une définition en évolution », p.17.

6.2. Les normes européennes

Nous avons exploré les instruments universels principaux touchant aux MASE. Nous entrons dans ce chapitre dans le niveau inférieur de la hiérarchie des normes de droit et nous nous concentrons sur les directives européennes et les réglementations intermédiaires. Ici, nous allons exposer un bref récapitulatif des réglementations en vigueur dans l'espace européen. Plus particulièrement, nous discuterons de la Directive de 2011 relative à la lutte contre l'exploitation sexuelle d'enfant et la pédopornographie.²² Nous envisagerons aussi d'autres directives qui protègent les enfants dans l'espace numérique.

6.2.1. Le cadre général des MASE dans l'espace européen

Retraçons un bref historique des réglementations concernant les MASE dans l'espace numérique européen. C'est en 1998, à Vienne, qu'apparaît pour la première fois le concept de cybercriminalité infantile. Le Conseil de l'Europe en réaction à cette

²¹ Pour de plus amples informations sur la procédure, nous renvoyons le lecteur sur le site suivant : https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/Overview_of_the_signature_and_ratification_processes_of_the_UN_Convention_Cybercrime.pdf

²² Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, *J.O.U.E.*, 17 décembre 2011, L 335, pp.1-14

problématique adopte la Convention sur la cybercriminalité en 2001 à Budapest et propose une définition des MASE. Quelques années plus tard, en 2004, naît la Décision-Cadre 2004/68/JAI du Conseil européen du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie.²³ Par la suite, en 2011, une directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie prévoit d'étendre les propositions de la directive 2004/68/JHA en proposant des peines dissuasives par rapport aux abus sexuels, l'exploitation sexuelle, la pédopornographie et la sollicitation d'enfants à des fins sexuelles. Elle incrimine les abus sexuels facilités par les technologies. Le terme de « pédopornographie » désormais désuet a été progressivement remplacé par « matériels relatifs à des abus sexuels sur mineurs » ou « images d'abus sexuels sur mineurs ». Dans cette directive, la notion d'image concerne dès lors les pseudo-photographies, les bandes dessinées, les dessins et les dessins animés. La nouvelle définition comprend aussi des manuels pédophiles, c'est-à-dire les étapes à suivre pour commettre un abus sur un enfant.²⁴ Les normes européennes concernant les MASE ont pour objectif de répondre à l'augmentation inquiétante des signalements reçus par certains services tels que Child Focus, durant ces dernières années, surtout après la période du Coronavirus. C'est dans ce cadre qu'une proposition de directive est portée en vue de modifier la Directive de 2011, prévoyant également une nouvelle définition qui aura pour objectif de prendre en compte toutes les évolutions techniques et technologiques comme le cas des deepfake (Bourcelet & Mathieu, 2025 ; Karagoz H., Lacour L. & Maillot N., 2025). En plus des réglementations principales, d'autres instruments juridiques ont des effets directs ou indirects sur le domaine des abus sexuels en ligne. Toujours en 2024, une directive basée sur les violences de genre a eu pour effet de criminaliser la création et la distribution des images non consenties à caractère sexuel manipulées par IA (Boutier, 2026 ; Parti & Szabo, 2024).

6.2.2. Réguler l'espace numérique : une course contre la montre

6.2.2.1. Le cyberspace

En 2020, un code des communications électroniques est adopté pour protéger la confidentialité des communications, mais une année plus tard, un autre règlement temporaire a été adopté pour déroger à ces obligations de confidentialité.²⁵ La proposition de règlement visait à une obligation de détection des MASE y compris dans les plateformes cryptées ou non. Ce régime temporaire ne devait être appliqué seulement dans l'attente d'une

²³ *Ibid.*

²⁵ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (Texte présentant de l'intérêt pour l'EEE), *J.O.U.E.*, du 27 octobre 2022, L 277, pp. 1-102.

proposition de règlement visant à prévenir et combattre les abus sexuels sur enfants. Les dérogations avaient été étendues jusqu' avril 2026 puis renouvelée jusqu'août de la même année. H. Karagoz et al., au moment de la rédaction de leur article sur l'action de l'UE en matière de cyberviolences sexuelles affectant les enfants, constataient qu'aucun consensus n'avait été trouvé sur la faisabilité technique de la détection et soulèvent des tensions des droits fondamentaux concernant la vie privée et la protection de l'enfance (Karagoz et al., 2025).

Ensuite, en 2022, un projet de règlement a vu le jour pour prévenir et combattre les abus sexuels d'enfants. Cela concerne la directive e-commerce et le Digital service ACT (ou règlement sur les services numériques) (DSA). L'objectif était de réguler les plateformes numériques pour la détection, la modération et le retrait des contenus illicites, y compris MASE. La directive e-commerce cherchait à tempérer la responsabilité des plateformes avec pour obligation de la part des services numériques de coopérer avec les autorités publiques. Cette directive prévoyait aussi une exonération de responsabilité par rapport aux contenus trouvés sur les plateformes. À la suite de l'évolution du monde numérique, la Commission européenne a décidé d'élaborer une nouvelle législation intitulée Digital Service Act. Dans les articles, 8,9 et 10, le DSA précise et donne de nouvelles obligations aux prestataires des technologies, notamment en prévoyant le maintien l'absence d'obligation de surveillance généralisée et en renforçant les injonctions de retrait. Cela s'inscrit dans une lutte face aux contenus illégaux qui prolifèrent en ligne. Le dispositif législatif a donc pour but d'obliger les services en lignes dont les RS, d'être transparent quant à la modération et à la suppression des contenus. La directive exige également la mise en place d'un environnement numérique sain et sécurisé. Du point de vue des plateformes numériques, la Directive aide à répartir des responsabilités par rapport à la modération des IA MASE et vise aussi leur suppression par des actions rapides. Ces exigences nécessitent également une collaboration étroite avec les autorités institutionnelles (Dushi et al., 2025 ; Niestadt, 2025).

6.2.2.2. L'intelligence artificielle : le nouveau défi juridique

Une nouvelle technologie telle que l'Intelligence artificielle nécessite un contrôle, c'est pourquoi l'Union européenne a élaboré une loi sur l'intelligence artificielle. Cette base légale décomposée en douze titres principaux classe les IA en fonction des risques et veut réguler les systèmes. L'IA ACT (Règlement 2024/1689) a pour objectif de veiller à la transparence des systèmes d'IA utilisés dans l'UE. Cette législation consiste également à offrir un cadre à la criminalité présente sur Internet et des moyens d'action pour la

combattre.²⁶ Dans cette réglementation, il est possible de retrouver des bases légales concernant l'émergence des deepfakes, tentant d'offrir des outils de détection de ces productions synthétiques ²⁷ (*Artificial Intelligence : Threats And Opportunities*, 2020 ; Romero-Moreno, 2025).

Depuis le 2 août 2026, les autorités et le Bureau de l'IA ont débuté la mise en application de ce règlement avec les obligations de transparence pour les fournisseurs et déployeurs d'IA générative. Ces obligations concernent un marquage et une détection des contenus générés par IA. Les fournisseurs et déployeurs ont désormais l'obligation d'étiqueter s'il s'agit de deepfake ou une publication générée par IA. (*Résumé de haut niveau de la loi sur l'intelligence artificielle de l'UE*, 2024) Les personnes concernées par ces obligations peuvent s'aider d'un Code de bonnes pratiques et de transparence mis au point par des experts. L'Union européenne propose des icônes pour aider à étiqueter les images.²⁸ (*Approche européenne de l'intelligence artificielle*, s. d. ; *Code de bonnes pratiques sur la transparence des contenus générés par l'IA*, s. d.) Avant la mise en application de ces obligations, nous nous sommes entretenu avec une personne travaillant chez Child Focus qui nous a indiqué que cela serait une solution envisageable, mais insuffisante.

[...] On y parle, mais ça reste compliqué c'est de dire voilà toutes les images qui sont générées par l'IA doivent avoir un label doit être reconnaissable. Mais bon est-ce que, allez on sait tellement faire avec de l'AI on peut je pense même facilement effacer [...] Mais bon en tout cas ce serait bien que chaque produit qui a été généré par l'IA est reconnaissable que ça a été créé par le IA et qu'on peut pas supprimer cette Waterark, on appelle cette Watermark ce qui est derrière l'image. [...]

Personne travaillant chez Child Focus

Il deviendra de plus en plus difficile de cacher une production faite par IA. Dans cette course avec le temps, le simple fait d'apposer une étiquette sur une photo ne permettra pas à ralentir le phénomène. L'objectif est sans doute de rendre les contenus facilement identifiables, mais la personne interviewée soulève à juste titre que ce label pourra être facilement supprimé par l'IA elle-même. L'Union européenne profitant de sa lancée, aurait accepté de simplifier les règles de l'IA ACT pour « booster l'innovation et interdire les applications de nudification ». Cette simplification tend vers une interdiction, d'ici

²⁶ Question n° 2169 de Mr Michael Freilich du 23 novembre 2023, (NI.), *Q. R.*, Ch.repr., sess.ord. 2023-2024, n° 55, p. 249.

²⁷ Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (Texte présentant de l'intérêt pour l'EEE), *J.O.U.E.*, 12 juillet 2024, L 2024/1689.

²⁸ Nous renvoyons le lecteur sur le site Internet suivant : <https://digital-strategy.ec.europa.eu/en/policies/eu-icons-labelling-ai-generated-content>. Vous y trouverez un tableau avec les étiquettes et leur utilisation.

décembre 2026, de la génération de matériel d'abus sur mineurs (Negreiro et al., 2026 ; Commission européenne, 2026).

Par l'examen de ces dispositions légales européennes, nous nous alertons sur la production législative autour de la thématique des MASE qui semble tendre vers une densité législative pouvant parfois entacher la portée des règles fondamentales. Même s'il n'est pas encore question d'une inflation, la quantité de dispositions présente interroge quant à leur réelle efficacité.

6.3. Les normes belges

Dans le paysage législatif belge, nous avons récemment accueilli de nouveaux articles dans le Code pénal, notamment les articles 417/43 et suivants qui ont l'intitulé « des images d'abus sexuels de mineurs ». Dans ces articles, nous retrouvons la définition, les risques de la production ou la diffusion de MASE, de la détention et de l'acquisition et l'accès. L'article 417/43 procure une définition des images d'abus sexuels sur mineurs : « on entend par images d'abus sexuels de mineurs : - tout matériel représentant de manière visuelle, par quelque moyen que ce soit, un mineur se livrant à un comportement sexuellement explicite, réel ou simulé, ou représentant les organes sexuels d'un mineur à des fins principalement sexuelles ; - tout matériel représentant de manière visuelle, par quelque moyen que ce soit, une personne qui paraît être un mineur se livrant à un comportement sexuellement explicite, réel ou simulé, ou représentant les organes sexuels de cette personne, à des fins principalement sexuelles ; - des images réalistes représentant un mineur qui n'existe pas, se livrant à un comportement sexuellement explicite, ou représentant les organes sexuels de ce mineur à des fins principalement sexuelles. »²⁹

Une analyse réalisée par les chercheuses O. Gangi et al. (2022) nous éclaire sur cette nouvelle législation concernant les MASE. Cet article renvoie également aux images générées par l'IA et nous donne quelques indications supplémentaires concernant leur traitement. Il est précisé que celles-ci doivent constituer un abus sur une personne réelle ou de synthèse. L'utilisation des termes « représentant les organes sexuels à des fins principalement sexuelles » ne semble toutefois pas assez large pour couvrir le cas d'une personne dénudée. Dans ce cas précis, la victime qui se retrouve dénudée devrait être représentée à des fins sexuelles. Si une photo est prise à l'insu d'une personne, dans des vestiaires, et que les clichés sont diffusés, cela l'exclut de cette disposition légale. L'infraction est alors incriminée non pas par les articles 417/43 et s. qui concernent les MASE, mais par l'art. 417/9 intitulé « La diffusion non consentie de contenus à caractère sexuel » du Nouveau code pénal qui utilise la terminologie « personne dénudée ». La

²⁹ C. pén., art. 417/43.

combinaison des deux articles offre un large champ d'application. Il apparaît alors que le cas des *Deepnudes* n'est pas compris dans l'art. 417/43. L'analyse sur la question du consentement que nous avons évoquée dans la première partie est toujours d'application ici³⁰ (Giacometti et al., 2022). De plus, des sous-sections ont également été ajoutées dans le cadre de cette réforme. Ces bases légales apportent une avancée en ce qu'elles condamnent la production, la diffusion, la détention, l'acquisition et l'accès à des contenus. Elles donnent également la possibilité de poursuivre en justice les « manuels de pédophiles » qui pourraient circuler sur Internet. Ces derniers consistent en une marche à suivre et des conseils facilitant la perpétration d'infractions pédocriminelles. E. Bourcelet (2024) apporte des nuances importantes sur ces nouvelles appellations. Le terme « images » reprend non seulement des photographies, mais aussi des vidéos ou tout autre support visuel. Comme pour beaucoup de situations comportant un flou juridique, la jurisprudence vient combler les lacunes existantes. C'est pourquoi une des limites de ce texte se situe dans la quantité d'images nécessaire pour tomber sous le champ d'application de cet article. Ce dernier est rédigé au pluriel pourtant la Cour de cassation, dans sa jurisprudence, condamne l'infraction même s'il s'agit d'une seule image.³¹

6.4. Des dispositions légales fragiles

6.4.1. Chat Control 1.0 : beaucoup de bruit pour rien ?

6.4.1.1. L'art de bâtir un empire sur une ombre

Dernièrement de nombreux médias se sont emparés de l'affaire « Chat Control », cette expression désignant, par ses détracteurs, le projet de règlement de l'Union européenne CSAR. Ce dernier donne la possibilité aux RS et aux messageries de scanner automatiquement les messages entre utilisateurs. Le règlement viendra normalement lutter contre le phénomène des MASE. Dans ce point, nous allons comprendre pourquoi ce règlement est au cœur des débats médiatiques et politiques.

Le règlement 2021/1232³² établissant les règles en vue de prévenir et combattre les abus sexuels sur enfant intervient comme dérogation à la Directive E-privacy et à la suite de

³⁰ Question n° 2169 de Mr Michael Freilich du 23 novembre 2023, (Nl.), *Q. R.*, Ch.repr., sess.ord. 2023-2024, n° 55, p. 249

³¹ Cass., (2e ch.), 15 mai 2024, P.24.0290.F., J.T., 2024/27, pp. 469-470, note B. Dejemeppe « Le fantasme de l'interprétation littérale.

³² Règlement (UE) 2021/1232 du Parlement européen et du Conseil du 14 juillet 2021 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne (Texte présentant de l'intérêt pour l'EEE), *J.O.U.E.*, 30 juillet 2021, L 274, pp. 41-51.

la croissance de la cybercriminalité. Dans le cas particulier des MASE, nous avons démontré précédemment que les services en ligne sont des outils facilitateurs pour commettre un crime et que les enfants sont des individus considérés comme particulièrement vulnérables. Ces deux problèmes ont conduit le législateur à prendre des mesures pour protéger les mineurs du danger en ligne (Rojszczak, 2025). La proposition de règlement « MASE », appelée Chat Control par ses détracteurs, avait donc pour but d'établir un cadre juridique clair et harmonisé pour combattre et prévenir le phénomène d'abus sexuels sur mineurs en ligne. Cette proposition vient alors réglementer les stratégies déjà mises en place par l'UE dans la lutte contre les abus sexuels sur mineurs. Pour remplir ces objectifs, la réglementation demande aux fournisseurs de prendre leurs responsabilités dans l'évaluation et l'atténuation des risques liés aux outils technologiques, y compris en ce qui concerne la détection et le retrait des MASE. La dérogation demande aux plateformes de continuer leurs volontariats dans la détection, le signalement et la suppression. Elle veut trouver un équilibre entre les droits et les différents intérêts en jeu tout en fournissant des règles qui combattent des MASE en ligne. Ce texte tient également à respecter le Règlement général de protection des données (RGPD) pour traiter les données à caractères personnels qui nécessitent une détection et un signalement à cause de la présence de MASE. L'article 8 du RGPD spécifie que le consentement du mineur au traitement de ses données n'est acceptable qu'à partir de 16 ans, seuil qui peut être descendu à 13 ans par les états membres. Pour l'instant, la directive relative aux abus sexuels sur mineurs et le règlement 2021/1232 étaient en vigueur dans ce domaine et devaient s'appliquer jusqu'au 3 août 2024. En avril 2024, le Parlement a voté en faveur de la poursuite de la dérogation qui devait s'étendre jusqu'au 3 avril 2026, dérogation qui permettait notamment aux RS de détecter sur base volontaire les MASE à l'exclusion des messageries chiffrées de bout en bout. (Child Sexual Abuse Online : current rules extended until April 2026, 2024) Le 9 juillet 2026, un consensus a été trouvé et Chat Control 1.0 a été voté pour lutter contre la pédocriminalité. (Karagoz et al., 2025) Si la détection sur base volontaire était déjà effectuée depuis quelques années, ce débat éclate dans les médias et dans la politique. ³³Cette mesure constitue donc une dérogation au règlement 2021/1232 plusieurs fois prolongé et en l'attente du vote de « Chat control 2.0 » qui prévoit la détection y compris dans les messageries chiffrées de bout en bout (AB-Arts, 2026 ; Bourcelet, et Mathieu, 2025 ; Negreiro & European Parliamentary Research Service, 2026).

³³ Résolution législative du Parlement européen du 9 juillet 2026 sur la position du Conseil en première lecture en vue de l'adoption du règlement du Parlement européen et du Conseil relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne, *C.O.M.*, (2023) 0777 – 2023/0452 (COD)) P10_TA (2026).

6.4.1.2. Un danger pour la vie privée ?

Plus largement, parmi les droits en tension, nous retrouvons la vie privée (Bourcelet, 2022). Beaucoup d'utilisateurs et de réseaux de communication s'inquiètent du respect de celle-ci lorsqu'il est désormais possible de scanner de manière quasi automatique toutes nos communications.

La vie privée c'est quoi ça ?

Personne travaillant à la police fédérale

Cette phrase est tirée d'un des entretiens menés avec une personne travaillant dans la police et nous permet de nous questionner sur le respect de la vie privée à l'ère des IA et des nouveaux outils technologiques. Pour envisager cette thématique, il convient de définir ce que nous entendons par vie privée. D'un point de vue juridique, la vie privée est consacrée dans l'article 8 de la Convention européenne des droits de l'homme indiquant que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »³⁴. Cet article trouve son équivalence dans la Constitution belge en ces termes « Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. »³⁵ Nous comprenons donc que la vie privée est un droit fondamental qui se doit d'être respecté. Que faire lorsque ce respect peut être balancé par une absolue nécessité ? Récemment, nous avons vu que l'UE a proposé un règlement prévoyant de scanner toutes nos conversations grâce notamment à l'IA et qui a pour but de combattre les MASE en ligne. Une proposition qui inquiète quant au respect de la vie privée des utilisateurs (Bourcelet, 2022 ; Attaque, 2025). Lors de l'un de nos entretiens avec Child focus, ils nous ont apporté quelques précisions concernant ce fameux règlement.

La proposition qui va ressortir voilà c'est un nouveau compromis qui est beaucoup plus faible que la proposition qui a été mise au cours de table pour nous Child Focus, il faut certainement garantir et protéger les droits fondamentaux, mais nous avec tout ce qu'on a suivi, parce qu'on suit tous ces négociations de près, il y a assez de safe guards, comment on appelle ça de garanties en place ...ça a pris trois ans pour négocier donc tu peux t'imaginer avec toute les experts qui ont contribué que c'était un parcours loin, mais malheureusement le code des textes il a été compromis, il a été tellement polarisé, il y a eu voilà des experts qui qui allez de différents côtés qui ont pris des positions très très très extrêmes, on va dire comme ça et qui est très malheureux parce que les plateformes en fait ils ont en fait ils utilisent déjà un tas de technologies pour faire du marketing pour faire allez... Ils ont déjà beaucoup de données personnelles de nous, beaucoup trop et en fait il faut qu'on ait beaucoup plus protecteur de ça. Mais quand des technologies comme qui sont été envisagées dans le texte sont mis

³⁴ Convention européenne des droits de l'homme, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, article 8, *M.B.*, 19 août 1955, p.5028

³⁵ Art. 22, C°.

en place sous beaucoup de différentes garanties avec un contrôle des différents organes et tout ça pour nous c'est sécurisant, c'est cette technologie sont utilisées que cette technologie sont utilisées de façon

Personne travaillant chez Child Focus

Des garanties seraient donc en place pour limiter cette atteinte à la vie privée et le texte comporterait les sécurités suffisantes. Elle estime également que le texte adopté s'écarte de manière significative par rapport à ce qui avait été soumis au Parlement. Nous nous questionnons tout de même sur ce terme « polarisé ». Cela pourrait renvoyer à une polarisation politique puisque nous le rappelons le Parlement européen est composé de chefs d'État (MR, 2026).

Mais bon ils ont voilà à cause des polarisations, ils sont revenus à vraiment limiter l'utilisation d'une détection obligatoire. [...] Pour nous, c'est très dommage qu'on voit que voilà en même temps nous on pense que c'est bien possible de faire une bonne balance et de trouver des solutions. On a beaucoup d'experts, ça doit pas être tellement difficile d'en trouver si on veut vraiment. [...] donc voilà on est pas très content de comment les négociations vont, mais à suivre.

Personne travaillant chez Child focus

La surveillance de nos conversations défie les exigences concernant la protection de la vie privée. Plus largement, il est important de questionner et de repenser la question de la vie privée à l'ère du numérique surtout avec l'avènement de l'intelligence artificielle. Concernant l'étape suivante à propos de la détection des messageries chiffrées de bout en bout, il semblerait que le combat entre la protection de la vie privée et la protection de l'enfance est loin d'avoir dit son dernier mot.

6.4.2. Les IA MASE : penser l'impensable

Ces avancées s'ancrent dans une conception considérant que l'IA générative permet à n'importe qui ayant accès à Internet de créer une image réaliste ou modifiée d'un enfant (Dushi et al., 2025). À travers ces différentes réglementations, nous avons constaté que les autorités peuvent s'appuyer sur une quantité importante de bases réglementaires pour combattre les images d'abus sexuels sur mineurs. En Belgique, les infractions liées aux MASE générés par l'IA tombent dans le champ d'application des articles du nouveau Code pénal. Ainsi, il apparaît clairement que le fait de perpétrer ces agissements constitue quand même une violation du droit des enfants. Les contenus d'enfant générés par l'IA concernent parfois des mineurs fictifs, n'empêchant pas qu'il soit effectué une sexualisation de l'enfant. Cela pose la question de la nécessité de repenser les nouvelles zones d'ombres qui engendrent cette sexualisation dans la vie réelle. Les réglementations que nous connaissons

se sont implémentées en réaction à la nouvelle manière pour les auteurs de commettre des infractions. Pourtant, le droit est souvent incapable de suivre les avancées technologiques ou de la société, le rendant souvent désuet dès son entrée en vigueur. Des mesures plus proactives offriraient une possibilité de tempérer ce phénomène. Nous constatons également qu'il existe une quantité importante de normes visant à prévenir ce phénomène, sans que celui-ci semble contrôlé (Dushi et al., 2025 ; Ende, 2025). Nous avons également observé dans notre partie sur le marché que pour empêcher l'expansion des MASE, les autorités devraient agir sur l'apport lucratif à tous les niveaux d'un tel réseau criminel. Un aspect lucratif qui n'est que très peu mentionné dans les réglementations que nous avons analysées. Les écarts entre les réglementations nationales et régionales impliquent un manque dans la protection des enfants, ces manquements sont utilisés par les auteurs d'infraction pour éviter les poursuites. ³⁶

Partie 7. La réaction sociale aux phénomènes

La détection des images est cruciale dans la lutte contre la propagation des MASE. Seulement, effectuer cette étape sollicite énormément de temps et d'investissement humain. Pour mesurer l'impact des IA MASE sur la détection, nous allons envisager les techniques les plus pertinentes mises en place et les challenges imposés par l'IA quant à la modération et aux signalements. Dans un second temps, nous mentionnerons quels sont les actes de préventions qui sont et qui peuvent être mis en place. Enfin, nous discuterons de l'impact de l'IA sur la santé mentale des acteurs de terrain.

7.1. L'itinéraire des images d'abus sexuels sur mineurs

7.1.1. Les techniques de détection

Nous avons vu que les plateformes détectaient parfois de manière automatique le contenu qui se trouvait sur leurs réseaux. Il existe également une autre voie pour déceler des MASE qui se situe dans les signalements faits aux associations tels que Child Focus ou la Cybertipline du NCMEC, aux réseaux de communications (Instagram, Facebook, Tiktok...) ou aux autorités (Police judiciaire...). Ces signalements émanent à la fois des potentielles victimes ou des réseaux de communications concernés. Une fois le signalement fait à une organisation, il arrive parfois que celle-ci la redirige vers le pays concerné. En Belgique, les autorités et organisations reçoivent parfois des signalements de la part des États-Unis. Une

³⁶ Proposition de directive du parlement européen et du conseil relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que contre les matériels relatifs à des abus sexuels sur enfants, et remplaçant la décision-cadre 2004/68/JAI du Conseil (refonte), *C.O.M.*, (2024) 60 final.

fois ce processus enclenché, la détection débute (*About Us & Our Work – Internet Watch Foundation*, s. d.).

Une distinction importante dans le cadre des MASE doit être effectuée. D'une part, nous retrouvons les MASE connus et, d'autre part, les nouveaux MASE nécessitant un processus de détection différent. Cette distinction est fondamentale, car les bases de données reposent sur des MASE connus. Les bases de données sont la compilation d'images auxquelles un hash a été attribué. Le hash est entendu ici comme un code, une sorte d'empreinte numérique pour chaque document et qui change à chaque fois que l'image est modifiée. À l'intérieur des technologies de hachage, E. Daskalaki et al. (2025) identifient les hash cryptographiques et perceptuels. Les cryptographiques sont plutôt choisis pour préserver la sécurité des données et les résultats obtenus sont uniques et irréversibles. Les perceptuels sont utilisés pour identifier des contenus multimédias similaires. Ils sont plus efficaces dans la modération de médias visuels. La technique du hachage joue donc un rôle déterminant dans la détection automatique de contenu illégal. Ainsi, lorsque l'outil détecte un hash similaire à du contenu illégal déjà identifié et présent dans la base de données, il peut le bloquer automatiquement (Bursztein et al., 2019 ; Lykousas & Patsakis, 2025 ; Westlake, 2019).

Au début des années 2000, l'informaticien Henry Farid et l'entreprise Microsoft créent la technologie PhotoDNA fonctionnant sur la base d'*hash* perceptuel pour la détection de MASE (Evangelia et al., 2025). Cette technologie identifie des contenus illégaux sans la nécessité d'un accès direct à l'image. Pour ce faire, l'outil repose sur des bases de données et compare l'image à identifier à des images illégales précédemment stockées. Pourtant prometteuse, Photo DNA et les technologies reposant sur le même processus de détection possèdent plusieurs limites. Premièrement, la base de données n'est pas exhaustive. Par exemple, si l'image n'est pas dans la base de données utilisée, PhotoDNA ou toute autre technologie fonctionnant identiquement, ne va pas la reconnaître. Les nouveaux MASE générés ou modifiés par IA sont alors plus difficiles à détecter que les MASE connus. Cela impliquait aussi que les conversations, les vidéos et les nouveaux contenus n'étaient au départ pas détectés (Bursztein et al., 2019 ; Lykousas & Patsakis, 2025 ; Westlake, 2019). Deuxièmement, un autre point négatif important de l'utilisation des hash est leur incidence sur les données personnelles. Finalement, la technologie basée sur le hash est facilement contournable par les criminels ; ces derniers changent le nom du document, y apportent de petites modifications et ainsi, les médias ne seront pas détectés. L'utilisation des technologies tel que Photo DNA est facilitée par certaines organisations telles que la NCMEC (National Center for Missing and Exploited Children), ou encore IWF (Internet Watch foundation) qui produisent et mettent à disposition une base de données exploitable,

et surtout nécessaire, aux entreprises et aux experts en forensique numérique afin d'identifier du contenu illégal (Steel, 2024). International Child Sexual Exploitation (ICSE) base de données d'images et de vidéo d'Interpol produit, grâce à l'IA, un moyen de partager des données pour aider les investigateurs. Cette base de données est en place dans 72 pays (*International Child Sexual Exploitation Database*, s. d. -b). Ces bases de données sont, la plupart de temps, alimentées par les signalements reçus via des *hotlines*, comme la « INHOPE Network hotlines ». À titre d'exemple, la base de donnée fournie par NCMEC est utilisée par les systèmes de détection tels que Project arachnid, Thorn (développé plus tard) (Daskalaki, 2025).

D'autres manières de détecter des MASE sont les robots d'exploration aussi appelé Web-crawler, comme Project Arachnid, qui survolent les sites web pour télécharger les médias et les indexer dans une base de données. Ces robots suivent toujours les mêmes procédures, il serait alors possible pour eux de détecter du MASE grâce à des mots clés. Contrairement au hachage, ils peuvent aussi détecter du contenu nouveau. Le *webcrawling* repose malheureusement sur une base de données souvent incomplète puisqu'Internet et les nouvelles technologies sont en évolution ce qui nécessiterait une mise à jour constante. Cela peut aussi amener à de faux positifs. En solution, Lee et al. (2020) soulèvent que la combinaison des deux méthodes, le hash et le *web-crawler* mènerait à de meilleurs résultats. Une autre manière pour détecter le contenu repose sur la base des noms de document et metadata³⁷, aidé de l'apprentissage profond. Cette possibilité nécessite de distinguer correctement les documents MASE des documents pornographiques classiques. Enfin, la détection visuelle permet de déceler les nouveaux MASE, les policiers nous indiquaient effectuer ces détections sur base de l'iris de l'œil.

Jusqu'à il y a quelques mois, on essayait d'élargir le Iris de de l'œil quoi donc, et s'il y avait là, si l'image correspondait à ce qu'on constatait dans l'image même et ce qu'on constatait dans les Iris de de l'œil, les reflets. Si ça correspondait, bah oui, on pouvait constater d'une manière humaine qu'il s'agit d'une image IA ou non. Mais depuis peu, ce n'est plus le faisable puisque la technologie a avancé tellement. Donc on doit utiliser, des moyens techniques pour constater cet abus.

Personne travaillant à la Police fédérale

Dans la pratique, il n'est plus possible pour les policiers de détecter à vue d'œil si l'image a été générée par l'IA ou non. Ainsi, en fonction du contenu, qu'il soit connu ou inconnu, il nécessite des techniques de détection différentes qui accompagnent le contrôle humain. Les MASE connus seront souvent détectés via du hachage tandis que pour les

³⁷ La metadata est définie par l'IBM comme « une information tel que l'auteur, la date de création ou la taille du fichier qui décrit un élément ou un ensemble de données » (<https://www.ibm.com/think/topics/metadata>)

MASE inconnus d'autres techniques doivent être utilisées (Bursztein et al., 2019 ; Negreiro & European Parliamentary Research Service, 2026). Notons que le hachage donne un taux très significatif de précision même s'il ne s'applique malheureusement qu'aux MASE connus. Les IA et le grooming donnent un taux important de faux positifs avec des techniques traditionnelles et nécessitent un contrôle humain (Negreiro & European Parliamentary Research Service, 2026 ; Salter & Hanson, 2021). La détection ne sert pas seulement à identifier si c'est de l'IA ou non, mais surtout si une victime est identifiable. L'objectif principal reste de prévenir un passage à l'acte et de venir en aide aux victimes. C'est là tout l'enjeu des nouvelles technologies selon la police.

L'importance de détecter si c'est de l'IA ou pas, c'est qu'on va pas investir une capacité d'enquête dans le fait d'essayer d'identifier une victime qui finalement n'existe pas vu qu'elle a été entièrement générée.

Personne travaillant à la Police fédérale

Le risque de passer à côté d'une victime entraîne des conséquences. Les capacités d'enquêtes sont alors concentrées sur cet objectif précis. Cependant, l'IA générative nécessite énormément d'effort de la part des autorités pour identifier les vraies victimes pour qu'elles ne passent pas entre les mailles du filet (Fondation pour l'enfance, 2024). Cette difficulté d'identification de la victime est impactée par les images générées par IA réalistes rendant la détection plus difficile. Cela est dû aussi aux technologies générant des images. Distinguer le vrai du faux consiste donc en une étape importante (European Parliamentary Research Service & Negreiro, 2025 ; IWF, 2023). Cette préoccupation ne concerne pas seulement la police, mais aussi les organismes disposant de lignes de signalements comme Child focus.

[...] il y a quelqu'un qui nous signale et qui met un petit texte en disant voilà ici il s'agit de l'IA voilà on peut le savoir, mais si la personne ne nous dit pas et nos analyses ne voient pas sur l'image même qu'il s'agit bien d'un image qui a été manipulée aujourd'hui. L'évolution technologique est de ce niveau que c'est plus difficile plus difficile de voir ces changements. Donc là pour l'instant même quand je demande de temps en temps à nos analystes. Par rapport à quelques dossiers qu'on a parce que quelqu'un nous a signalé, on n'a pas d'autres dossiers ou pas tellement des dossiers IA qui sont gérés.

Personne travaillant chez Child Focus

Face à toutes ces difficultés, des organisations non gouvernementales et des autorités telles qu'Interpol ou Europol ont décidé d'intervenir. Leur collaboration a mené à considérer

non par l'IA comme source de leur problème, mais comme une solution envisageable. L'IA est envisagée, selon Sanchez et al. (2019), dans une étude quantitative menée aux États-Unis, comme un outil qui octroiera la possibilité de détecter et d'identifier les MASE. Certains de ceux-ci sont déjà en place comme iCOP qui est utilisé seulement dans les réseaux P2P et il offre une opportunité aux investigateurs d'identifier les fichiers MASE sur la base des hash. De plus, Yahoo a également mis au point Not Safe for Work qui détecte les images pornographiques (Sanchez et al., 2019). Nous avons constaté précédemment que les hash se limitent à la détection de MASE connus et n'empêchent pas la prolifération de nouveaux contenus qu'ils soient créés ou édités (Wolbers et al., 2025). La technologie Thorn, machine learning qui détecte de manière proactive les MASE et CSE (child sexuel exploitation), pourrait pallier ces effets indésirables. Thorn repose sur une approche « Safety by Design » qui place la sécurité au cœur du développement des outils numériques. Appliquer une telle approche permet de réduire les menaces par l'anticipation, la détection et l'élimination du préjudice avant son apparition (Bracket Foundation, 2024). Il pourra alors identifier de nouveaux MASE sans base de données grâce à de l'IA prédictive (Holderness, 2024 ; THORN, 2024). Dans les outils proactifs, nous retrouvons Project Arachnid, outil gratuit de détection proactive de MASE. Google a également créé une technologie pour aider à détecter et signaler les MASE qui utilise la technologie du deep neural network (Lee et al., 2020). Ces programmes dépendant de l'IA ont aussi des points négatifs. Ces outils doivent s'entraîner sur une quantité de données parfois importante, ils souffrent aussi de biais entraînant une perte de fiabilité. Une tension existe entre les mesures proactive et réactive nous explique P. Mandloi. (2025) La lutte contre les MASE regroupe les deux impliquant des difficultés importantes. Selon cet auteur, les mesures proactives présentent par exemple le risque de mettre à mal le principe de vie privée et générer de faux résultats. Quant au problème des mesures réactives, elles arrivent après le préjudice commis. Nous l'avons remarqué avec l'implantation du règlement CSAR qui a pour but d'analyser nos messages afin de détecter des MASE que la mise en place d'un outil proactif questionne. *In fine*, si le contenu généré se trouve sur une plateforme hors ligne, cela échappe à la détection (Fondation pour l'enfance, 2024).

7.1.2. La modération : une tentative de maîtriser les excès

Depuis une dizaine d'années maintenant, le monde numérique, toutes plateformes confondues, fait de la modération de contenu envers des informations, des discours de haine et des MASE. Selon J. Espindola (2025), la modération humaine entraîne parfois des problèmes psychologiques. La solution de détecter par l'IA n'empêchera malheureusement pas l'implication humaine. La modération humaine dépend surtout de la taille du réseau

social. Les plus grands RS emploient souvent des personnes aux salaires médiocres pour modérer le contenu. Cet auteur nous rapporte également que la plupart des modérateurs se situent dans l'hémisphère sud. La modération de MASE implique surtout de protéger une victime même si la tâche est compliquée par l'avènement dans l'IA dans le domaine des abus sexuels sur mineurs. En effet, les victimes ne sont pas toujours identifiables lorsque l'image a été manipulée par l'IA. Le même auteur nous alerte que la modération ne devrait pas être la seule ressource pour lutter contre le problème des MASE. La poursuite des créateurs de MASE et les lois mériteraient selon lui d'être renforcées. La modération a besoin d'humains, de programmes avec ou sans Intelligence artificielle, de se mettre à jour et de respecter la donnée privée.

Légalement, le contrôle que les plateformes doivent exercer repose sur le Digital Service Act (expliqué dans notre partie 6) qui demande la suppression des contenus illégaux en ligne (Niestadt, 2025). Les RS emploient alors des modérateurs pour effectuer la lourde tâche de lutter contre la diffusion des MASE sur Internet et d'autres crimes. Ces modérateurs deviennent alors la première ligne du combat. Sous cette réglementation se trouvent des « Trusted flaggers » ou signaleurs de confiance, c'est-à-dire des « experts à la détection de certains types de contenus illégaux en ligne comme les propos haineux ou contenus terroristes ». Leur rôle est donc de notifier aux plateformes le contenu illégal. Les services ont la responsabilité de décider de supprimer le contenu ou non (Bleakley et al., 2024 ; *Signaleurs de Confiance Au Titre de la Législation Sur les Services Numériques*, s. d.). La modération des MASE, P. Bleakley et al. (2024) l'ont étudié dans un article où ils évaluent si l'autorégulation suffisait à modérer ces contenus. Leur étude démontre que l'autorégulation est plus avantageuse pour les compagnies et les consommateurs. Le prix à payer pour la modération serait plus avantageux pour les RS que de prévenir la propagation des MASE. Le rôle de modérateur n'est pas seulement de supprimer le contenu, mais selon eux, d'avoir une connaissance suffisante des médias et des normes sociétales en vigueur pour effectuer une suppression. Notons que la modération ou encore l'interception par les forces de l'ordre dépend des services de communications qui octroieraient l'accès pour la lecture. L'auteur Holderness M. remarque que les services peuvent parfois contrôler les conversations si celles-ci apparaissent par inadvertance et favoriser la commission d'un crime (Holderness, 2024).

7.2. La prévention : une urgence de santé publique

Nous avons séparé ce point en deux pour illustrer les deux points d'action principaux à envisager afin de prévenir les images d'abus sexuels sur mineurs.

7.2.1. La prévention dans l'espace social

La Fondation pour l'enfance (2024) recommande de favoriser l'innovation pour tenter de faire face aux difficultés que supposent les images générées par l'IA. Certaines applications entravent aussi la détection et la suppression. Nous pensons évidemment aux messageries chiffrées de bout en bout telles que Telegram ou encore Whatsapp. Dans ses recommandations, la Fondation de l'enfance demande aussi la mise en place de campagnes de sensibilisation à la cyberpédocriminalité et des dangers du *sharenting*. En effet, il est établi que le *sharenting* des parents sur les RS nourrit ce phénomène. Les rendre plus vigilants serait une solution qui pourrait être envisagée. La prévention ne doit pas seulement s'effectuer du côté des victimes, mais la prise en charge des personnes ayant un comportement déviant serait une solution possible. (Fondation pour l'enfance, 2024). Notons que le rôle de prévention est souvent assuré par les associations ou collectifs qui luttent contre l'exploitation des enfants et par ce biais, mettent en place des campagnes de sensibilisation. Une approche sur la santé publique avec des facteurs de risques et des facteurs de protection à des niveaux différents offrirait une première étape dans ce combat face aux MASE. Beier (2024) conseille de commencer dans les écoles primaires et chez les familles, l'éducation sexuelle. La compréhension de l'aspect économique du marché des images d'abus sexuels sur mineurs donne également des pistes pour développer des campagnes de prévention. (Acar, 2017). A titre informatif, Le 18 novembre est déclaré comme la journée de l'abolition des abus sexuels contre les enfants inscrite dans le prolongement de la campagne UN sur CINQ réalisée de 2010 à 2015. Cette journée vise à prévenir ces crimes, poursuivre les auteurs et protéger les victimes. Elle encourage également à organiser des activités de sensibilisation pour alerter. À cette fin, le Conseil de l'Europe fournit des outils pour les enfants, les parents, les pouvoirs et les professionnels travaillant avec les enfants (*18 Novembre : Journée Pour la Protection des Enfants Contre L'exploitation et les Abus Sexuels*, s. d. ; *Nos Outils et Ressources*, s. d.). Il convient de garder à l'esprit que l'exploitation est accentuée par l'utilisation des intelligences artificielles génératives. Il devient alors urgent de trouver des pistes de prévention pour tenter d'encadrer ce problème.

En Belgique, des associations luttent activement contre l'exploitation sexuelle d'enfants. Par exemple, Défense des Enfants International Belgique a élaboré un projet PEPS pour la protection des enfants. Le délégué général aux droits de l'enfant Laqdim Soleyman défend les droits des enfants et des jeunes jusqu'à 18 ans en proposant un accompagnement juridique et psychologique. (*Défense des Enfants International - Belgique*, s. d.)

7.2.2. La prévention auprès des auteurs d'infractions à caractère sexuel en ligne

Une thérapie par l'IA a été parfois conseillée dans la prévention des auteurs. (Beier et al., 2024). En Allemagne, le projet Dunkefeld vise à contrôler le comportement des auteurs par le biais d'une thérapie et d'une médication. Les auteurs de ces infractions ont souvent un problème dans leur utilisation d'Internet, leur gestion des fantasmes, leur perception de l'illégalité de ce type de consommation ou encore une addiction au visionnage d'un tel contenu (Gannoni et al., 2023). Un débat académique est en cours autour de la question d'un lien, ou non, entre consommations de MASE et la commission d'une infraction sexuelle avec contact ou la recherche de contact avec un enfant. Un lien, qui mériterait, selon nous, d'être approfondi afin de mieux cerner le mécanisme par lequel s'opère le basculement d'une criminalité vers une autre. L'étude de ce passage à l'acte serait un point important à envisager pour adapter les stratégies de prévention auprès des auteurs (Paradise, 2025).

7.3. L'IA et la santé mentale : symbiose ou antibiose ?

La santé mentale des policiers et des modérateurs est un problème qui ne concerne pas seulement les personnes en contact direct des MASE. Les policiers et les modérateurs n'apparaissent pas au même moment dans le déroulé d'une affaire de MASE. Les policiers peuvent se sentir un peu moins impuissants puisqu'ils poursuivent effectivement la criminalité. Cependant, des effets ont été constatés tels qu'un stress post-traumatique, une surprotection des enfants et des difficultés dans les relations. Certains mécanismes permettent aux travailleurs de se protéger : l'humour et le tracé de limites claires entre vie personnelle et travail. (Espíndola, 2025 ; Mitchell et al., 2023)

Je sais pas tout dépend de est-ce qu'on va le ramener chez soi ou pas et ça je sais pas vous expliquer comment ça se fait qu'il y en a qui ramènent ça chez eux ou qu'il y en a d'autres qui arrivent à faire.

Personne travaillant à la Police Fédérale

Nous nous sommes alors demandé quel est l'impact de l'intelligence artificielle dans le quotidien de ces personnes. La prise en charge psychologique semble alors nécessaire pour faire face aux conséquences d'une exposition à de tels contenus. Comment protéger des effets dont nous ne connaissons pas encore l'étendue ? (Mitchell et al., 2023)

Par contre, avec l'IA, ce qu'on constate, c'est le volume qui pose aussi un souci puisqu'on est confronté à une masse d'images. Beaucoup plus qu'avant et aussi les images extrêmes sont devenues beaucoup plus accessibles, sont diffusées beaucoup plus qu'avant donc... Et si on est dans une plateforme ou un groupe pédocriminel et bref c'est aussi bien la quantité et la qualité extrême qui sont

devenus beaucoup plus extrêmes qu'avant... Et on va voir ce que ça va donner comme résultat pour les enquêteurs aussi puisque de plus en plus, non seulement en Belgique, mais aussi dans les pays qui coopèrent avec nous, on constate que l'impact est devenu beaucoup plus intense pour les enquêteurs qui sont actifs dans le monde numérique. Donc il y a un suivi qui se passe au niveau des enquêteurs, un suivi psychologique

Personne travaillant à la police fédérale

Nous avons dépeint une facette plutôt négative de l'intelligence artificielle à travers ce mémoire. Cependant, d'autres auteurs pensent que le futur de la détection des MASE et IA MASE est entre les mains des IA elles-mêmes. L'IA semble être la cause de leur problème, mais pourrait être aussi la solution. En effet, l'IA a la capacité d'alléger le poids d'une partie de leur travail et du poids psychologique d'être face à ces images. Une détection par une technologie IA comporte des aspects bénéfiques pour la capacité, le temps d'investigation et l'exposition aux images. Cependant, les aspects négatifs ne sont pas encore contrebalancés par les aspects positifs de l'implantation d'une telle technologie dans la police. Les IA nécessitent énormément de données pour s'entraîner, les autorités manquent de classifications standardisées des MASE. L'IA ne semble pas encore capable de fournir les mêmes résultats et le même respect de la vie privée que les techniques existantes. (Negreiro & European Parliamentary Research Service, 2020 ; Wolbers et al., 2025)

Conclusion

Au fil de ce mémoire, nous nous étions donné pour objectif d'explorer l'impact de l'intelligence artificielle sur la création et la diffusion accrues des images d'abus sexuels sur mineurs. Si nos premières réflexions s'étaient orientées vers l'analyse des techniques de détection de l'IA, ce champ de recherche s'est révélé difficile à atteindre. La réorientation de notre analyse nous a ainsi amené à découvrir des nuances fondamentales dans la lutte contre les MASE. Quant à notre position réflexive, la recherche menée ces derniers mois nous a fait prendre conscience d'un élément intrinsèque à notre position de chercheuse et d'internaute : l'utilisatrice lambda que nous sommes ne pouvait pas imaginer ni même mesurer l'étendue de ce phénomène encore en expansion.

Dans le cadre de notre recherche, nous avons donc exploré différentes thématiques pour donner un aperçu du retentissement occasionné par l'IA. L'image, la criminalité, l'économie, les lois et la prévention sont autant de champs qui ont nourri et conduit notre analyse de la thématique des IA MASE. Ce cadre théorique, structuré en plusieurs points, a constitué une base solide pour dresser des constats dont nous rappelons l'étendue ici. Le point 3, intitulé « Images d'abus sexuels sur mineurs : d'une image à l'autre » de ce mémoire, a permis de conclure que le concept d'image doit être pensé dans son contexte propre. Un concept qui sera encore sujet à des interprétations diverses dans les époques qui nous attendent. Cette partie indique que des chamboulements vont bousculer encore la définition donnée aux MASE d'ici quelques années. Ensuite, nous avons mis en lumière Internet, comme un précurseur de cette criminalité et comme terrain pour le développement d'une utilisation détournée de nouveaux outils. Les conséquences d'une mauvaise utilisation de l'IA sont mesurables non seulement sur les victimes, mais aussi sur la société dans son entièreté, poussant les autorités législatives à concourir avec un phénomène qui leur échappe. Pour pallier leurs lacunes, des techniques sont mises en place pour aider à détecter et modérer la multitude d'images présente sur Internet. Notre partie « La réaction sociale au phénomène » apporte des précisions et nous laisse entendre que les techniques actuelles souffriraient d'une obsolescence programmée, nécessitant une réaction imminente. Les techniques mises en place, auparavant suffisantes pour contrôler et pour cadenasser le développement des MASE, sont progressivement dépassées par l'IA. Il ne reste alors que des miettes pour agir. Si nous aspirions au départ à démontrer un quelconque impact, nous avons été confronté à des effets qui ne sont pour la plupart pas encore mesurables dans leur entièreté. Ce travail entend néanmoins fournir un état actuel des pratiques. Face à l'expansion croissante du phénomène, le mémoire aura souligné le caractère urgent pour les sociétés démocratiques de s'emparer de cette bombe à retardement et de proposer des outils

proactifs. Toutefois, une lueur d'espoir est née avec l'interdiction de générer des MASE pour décembre 2026.

La configuration actuelle et temporelle du mémoire ne nous permettait pas d'approfondir certains points. Néanmoins, nous espérons avoir ouvert des pistes pour de futures recherches. Ces ouvertures sont notamment le côté pécunier de la criminalité des MASE, nous estimons qu'une étude poussée des dynamiques économiques et l'impact de leur prise en compte sur l'efficacité des normes serait pertinente. Nous avons également remarqué que l'IA pouvait aussi servir d'outil pour éviter un passage à l'acte sexuel ou comme contrôle des déviations sexuelles. Ce paradigme du passage à l'acte mériterait de s'y attarder dans des recherches futures, d'autant qu'il est au cœur des débats dans le champ scientifique. Sur le plan artistique, nous n'avons pas pu explorer le genre littéraire « Hentai » qui selon nous, mériterait une attention particulière. Le *Hentai* joue avec les limites de la légalité s'appuyant sur une distinction prépubère et post-pubère. Finalement, le rajeunissement d'une photo d'adulte constitue également une production de MASE que nous n'avons pas exploré. Cette thématique est peu apparue dans la littérature que nous avons consultée, et mériterait d'être approfondie. Ainsi, ce travail soulève des sous-questions, chacune ouvrant la voie à de nombreuses recherches.

Bibliographie

Normes juridiques

Convention européenne des droits de l'homme, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, p.5028

Convention relative aux droits de l'enfant, signée à New York le 20 novembre 1989, loi du 25 novembre 1991, *M.B.*, 17 janvier 1992, pp. 803-826.

Convention concernant l'interdiction des pires formes de travail des enfants et l'action immédiate en vue de leur élimination, signée à Genève le 17 juin 1999.

Charte des droits fondamentaux de l'Union européenne, signé à Nice le 7 décembre 2000.

Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, signée à Lanzarote le 25 octobre 2007, approuvée par la loi du 7 février 2012, *M.B.*, 21 juin 2013, p. 39977

Convention contre la cybercriminalité, signée le 24 décembre 2024.

Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, *J.O.U.E.*, 17 décembre 2011, L 335, pp.1-14.

Règlement (UE) 2021/1232 du Parlement européen et du Conseil du 14 juillet 2021 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne (Texte présentant de l'intérêt pour l'EEE), *J.O.U.E.*, 30 juillet 2021, L 274, pp. 41-51.

Proposition de directive du parlement européen et du conseil relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que contre les matériels relatifs à des abus sexuels sur enfants, et remplaçant la décision-cadre 2004/68/JAI du Conseil (refonte), *C.O.M.*, (2024) 60 final.

Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, *C.O.M.* (2022) 209 final.

Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, article 2, adopté le 25 mai 2000.

Résolution législative du Parlement européen du 9 juillet 2026 sur la position du Conseil en première lecture en vue de l'adoption du règlement du Parlement européen et du Conseil relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels

commis contre des enfants en ligne, *C.O.M.*, (2023) 0777 – 2023/0452 (COD)) P10_TA (2026).

Constitution, art. 22.

C. pén., art. 417/43 et s.

Nouveau C. pén., art. 170.

Question n° 2169 de Mr Michael Freilich du 23 novembre 2023, (Nl.), *Q.R.*, Ch.repr., sess.ord. 2023-2024, n° 55, p. 249.

Jurisprudence

Cass., (2e ch.), 15 mai 2024, P.24.0290.F., J.T., 2024/27, pp. 469-470, note B. Dejemeppe
« Le fantasme de l'interprétation littérale. »

Ouvrages

Beaud, S., & Weber, F. (1997). Guide de l'enquête de terrain. Produire et analyser des données ethnographiques. Dans *Lire les sciences sociales* (pp.65-69).

Beuscart, J.-S., Dagiral, E., & Parasie, S. (2019). Une histoire d'Internet. Dans *Sociologie d'Internet* (pp.23-44). Armand Colin.

Bonnet, G. (2021). *Comment peut-on être pervers ? : Inceste, viol, pédophilie*.

Bourcelet, E., & Mathieu, G. (2025). L'autodétermination sexuelle du mineur en ligne à l'aune de sa vulnérabilité. Dans *Combattre les violences sexuelles* (1^{re} éd., pp.11-45). Larcier.

Bréchon, P. (2011). Glossaire général. Dans *Enquêtes qualitatives, enquêtes quantitative*. (pp. 211-222). Presses Universitaires de Grenoble <https://doi.org/10.3917/pug.abria.2011.01.0211>

Cohen, S. (2002). *Folk Devils and Moral Panics*. Routledge. <https://criminologiacabana.wordpress.com/wp-content/uploads/2015/08/stanley-cohen-folk-devils-and-moral-panics.pdf>

Coman, R., Crespy, A., Louault, F., Morin, J. -F., Pilet, J.-B., & Van Haute, E. (2022). Les grandes options méthodologiques. Dans *Méthodes de la science politique* (pp. 27-44). <https://shs.cairn.info/methodes-de-la-science-politique--9782807337756-page-27?lang=fr>.

Kalika, M., Moricou, P., & Garreau, L. (2023). La méthodologie. Dans *Le mémoire de master* (pp. 97-147).

Kaufmann, J.-C., & Singly, F. de. (1996). L'entretien compréhensif. Nathan.

Lépinard, E., & Lieber, M. (2020). Ruptures épistémologiques et nouveaux savoirs. Dans *Les théories en études de genre* (pp. 23-40).

- Mandloi, P. (2025). AI and Machine Learning : Revolutionizing the Fight Against Online Child Sexual Abuse Material (CSAM). Dans *Communications in Computer and Information Science* (pp. 30-48). https://doi.org/10.1007/978-3-031-87511-3_3
- Mucchielli, A., Pourtois, J. – P., Desmet, H., Savoie-Zajc, L., Bonnet, J., Coulon, A., Blanquis-Gasser, I. et Collettere, P. (2009). E. Dans *Dictionnaire des méthodes qualitatives en sciences humaines* (pp. 69-95). Armand Colin. <https://doi.org/10.3917/arco.mucch.2009.02.0069>.
- Paradise, A. (2025). Child Sexual Abuse Material, Progression to Contact Offending and the Evolution of Technology. Dans *Rethinking the Police for a Better future : Navigating Policing Challenges with Accountability and Trust* (pp. 259-273). https://doi.org/10.1007/978-3-031-83173-7_17
- Pickover, C.-A. (2021). Deep Blue bat le champion d'échecs. La fabuleuse histoire de l'intelligence artificielle : Des automates aux robots humanoïdes (pp. 225-227). Dunod. <https://stm.cairn.info/la-fabuleuse-histoire-de-l-intelligence-artificielle--9782100813186-page-225?lang=fr>
- Rigaud, F., Cadre, M., Saule, M. -A., & Rivière, D. (2017). Introduction générale. In *Travail et management à l'épreuve des sciences sociales* (pp.13-16) <https://doi.org/10.3917/ems.rigau.2017.01.0013>
- Salter, M., & Hanson, E. (2021). 'I Need You All to Understand How Pervasive This Issue Is' : User Efforts to Regulation Child Sexual Offending on Social Media. Dans *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (pp. 729-748). Jane Bailey ; Asher Flynn ; Nicola Henry <https://doi.org/10.1108/978-1-83982-848-520211053>
- Saporta, G. (2023). Histoire et enjeux de l'IA. Dans *L'IA éducative : L'intelligence artificielle dans l'enseignement supérieur* (pp. 41-50). Thèmes & Débats.
- Sifer-Rivière, L. (2023). Chapitre 6. Enquêter par entretien : se saisir du discours et de l'expérience des personnes. *Les recherches qualitatives en santé* (pp. 174-194). Armand Colin. <https://stm.cairn.info/les-recherches-qualitatives-en-sante--9782200631970-page-174?lang=fr>.
- Taylor, M., & Quayle, E. (2003). Child Pornography.
- Westlake, B.G. (2019). The Past, Present, and Future of Online Child Sexual **Exploitation**: Summarizing the Evolution of Production, Distribution, and Detection. Dans *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1–29) Palgrave Macmillan, Cham https://doi.org/10.1007/978-3-319-90307-1_52-1

Articles de revues

- Acar, K. V. (2017). Child abuse materials as digital goods : Why we should fear new commercial forms. *Economic Discussion Papers*, 2017-15. <https://www.econstor.eu/bitstream/10419/157247/1/884350916.pdf>
- Beaudouin, V., & Velkovska, J. (2023). Enquêter sur l'« éthique de l'IA ». *Réseaux*, 240 (4), 9-27. <https://doi.org/10.3917/res.240.0009>
- Béchu, V. (2025). Cyberpédocriminalité : dérives polymorphes et technologiques. *Servir*, 541 (8), pp. 40-41. <https://doi.org/10.3917/servir.541.0040>.
- Beier, K. M., Nentzl, J., von Heyden, M., Fishere, M., & Amelung, T. (2024). Preventing Child Sexual Abuse and the Use of Child Sexual Abuse Materials : Following up on the German Prevention Project Dunkelfeld. *Journal of Prevention*, 45(6), pp. 881-900. <https://doi.org/10.1007/s10935-024-00792-0>
- Benouamer, C., Libert, B., Janssens, M., & Pham, T. H. (2024). Effet du genre des victimes parmi les consommateurs de pédopornographie et les auteurs de viol : Étude exploratoire et résultats préliminaires. *Annales Médico-psychologiques, revue psychiatrique*, 182 (2), pp.167-171. <https://doi.org/10.1016/j.amp.2023.12.005>
- Benouamer, C., Libert, B., Janssens, M., Lagneaux, J., & Pham, T. H. (2026). Les consommateurs de matériel d'exploitation sexuelle d'enfants : Analyses comparatives. *Annales Médico-psychologiques, revue psychiatrique*. <https://doi.org/10.1016/j.amp.2026.06.002>
- Bitouk, D., Kumar, N., Dhillon, S., N Belhumeur, P., & K. Nayar, S. (2008). Face swapping : automatically replacing faces in photographs. *SIGGRAPH '08*, 39, pp.1-8. <https://doi.org/10.1145/1399504.1360638>
- Blais, M., & Martineau, S. (2022). L'analyse inductive générale :description d'une démarche visant à donner un sens à des données brutes. *Recherches qualitatives*, 26 (2), pp. 1-18. <https://doi.org/10.7202/1085369ar>
- Bleakley, P., Martellozzo, E., Spence, R., & DeMarco, J. (2024). Moderating online child sexual abuse material (CSAM): Does self-regulation work, or is greater state regulation needed? *European Journal of Criminology*, 21(2), 231–250.
- Bordron, J.-F. (2025). La situation historique de l'IA et le statut de l'image. *Actes Sémiotiques*, (133) <https://doi.org/10.25965/as.9115>
- Bourcelet, E. (2024). Les “images d'abus sexuels de mineurs”, une criminalité aux mille défis dans l'environnement numérique”, *Journal du droit des Jeunes*, n° 437, pp. 17–24.
- Boussaguet L. (2009) Les faiseuses d'agenda : Les militantes féministes et l'émergence des abus sexuels sur mineurs en Europe. *Revue française de Science Politique*, 59(2), pp. 221–246.

- Boutier, I. (2026). Artificial Intelligence and Child Sexual Exploitation : The Digitalisation of Harm. *UN Human Rights Office*. <https://researchonline.gcu.ac.uk/ws/portalfiles/portal/106691267/106638123.pdf>
- Ciardha, C. O., Buckley, J., & S. Portnoff, R. (2026). AI-generated child sexual abuse material : what's the harm ? *AI & Society*. <https://doi.org/10.1007/s00146-026-02932-y>
- Corriveau, P. (2010). Les groupes de nouvelles à caractère pédopornographique : Une sous-culture de la déviance. *Déviance et Société*, 34 (3), pp. 381-400. <https://doi.org/10.3917/ds.343.0381>
- Dąbrowska, M. (2025). Terminological Developments in the Criminalization of Child Sexual Abuse Material (CSAM) Dans International and European Union Law. *Eastern European Journal of Transnational Relations*, 9(2), 7–24. <https://doi.org/10.15290/eejtr.2025.09.02.01>
- Daskalaki, E., Kokolaki, E., & Fragopoulou, P. (2025). Hashing in the Fight Against CSAM: Technology at the Crossroads of Law and Ethics. *Journal of Cybersecurity and Privacy*, 5(4), 92. <https://doi.org/10.3390/jcp5040092>
- Davidson, B. I., Muir, K., Burnat, F. A. D., & Joinson, A. N. (2026). Regulatory gray areas of LLM Terms. *arXiv*. <https://doi.org/10.48550/arXiv.2601.08415>
- Dushi, D., Berdufi, N., & Karagianni, A. (2025). The legal framework and legal gaps for AI-generated child sexual abuse material. *Computer Law & Security Review*, 59 <https://doi.org/10.1016/j.clsr.2025.106205>
- Eelmaa, S. (2022). Sualization of children in deepfakes and hentai. *A Journal Of The Humanities & Social Sciences*, 26(2). <https://doi.org/10.3176/tr.2022.2.07>
- Ende, J. (2025). Don't throw the baby out with the bathwater: Protecting children against CSAM deepfakes without banning ai technology. *Family Court Review*, 63(2), pp. 324–338. <https://doi.org/10.1111/fcre.12854>
- Espíndola, J. (2025). Against Human Content Moderation : Algorithms without Trauma. *Journal of Applied Philosophy*, 42(4), pp. 1285-1300. <https://doi.org/10.1111/japp.70024>
- Faccioli, P. (2007), La sociologie dans la société de l'image. *Sociétés*, 95, pp. 9 à 18 <https://doi.org/10.3917/soc.095.0009>
- Gangi, O., Giacometti, M., & Gilen, A. (2022). Diffusion non consentie de contenus à caractère sexuel et diffusion d'images d'abus sexuels de mineurs : entre distinctions et chevauchements, quelles implications d'un point de vue légal, criminologique et psycho-social ? *Revue de la Faculté de Droit de L'Université de Liège*, pp.635-674.

- Gannon, C., Blokland, A. A. J., Huikuri, S., Babchishin, K. M., & Lehmann, R. J. B. (2023). Child sexual abuse material on the darknet. *Forensische Psychiatrie, Psychologie, Kriminologie*, 17(4), pp. 353-365. <https://doi.org/10.1007/s11757-023-00790-8>
- Gannoni, A., Voce, A., Napier, S., Boxall, H., & Thomsen, D. (2023). Preventing child sexual abuse material offending : An international review of initiatives. *Australian Institute Of Criminology*. <https://doi.org/10.52922/rr78764>
- Guern, N. L. (2025), Les développements récents de la photographie : De la menace des smartphones au potentiel démesuré de l'IA. *Marché et organisations*, 52 (1), pp. 217-247 <https://doi.org/10.3917/maorg.pr1.0117>
- Haiech, J. (2020). Parcourir l'histoire de l'intelligence artificielle, pour mieux la définir et la comprendre. *Med Sci*, 36 (10), pp. 919-923. <https://doi.org/10.1051/medsci/2020145>
- Holderness, M. (2024). The Dark Side of the Internet : The Facilitation of CSAM by Social Media Companies and What Should Be Done about It Student Notes. *South Carolina Journal of International Law and Business*, 21(2), pp. 312-332.
- Hotz, D. (2026). Explaining peer-generated AI-CSAM : A criminological analysis of youth offending, gendered harm and technology-facilitated sexual abuse. *Criminology & Criminal Justice*.
- Leduc, C. (2025). L'automatisation de l'imaginaire : Sur l'art à l'ère de l'intelligence artificielle. *Cahiers Société*, (7), pp. 133-163. <https://doi.org/10.7202/1125079ar>
- Lee, H. -E., Ermekova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material : A comprehensive survey. *Forensic Science International : Digital Investigation*, 34.
- Lykousas, N., & Patsakis, C. (2025). Just in Plain Sight : Unveiling CSAM Distribution Campaigns on the Clear Web. *2025 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1-9. <https://doi.org/10.1109/eCrime66972.2025.11327714>
- Metz, C. (1970). Au-delà de l'analogie, l'image. *Communications*, 15 (1), pp. 1-10. <https://doi.org/10.3406/comm.1970.1212>
- Mitchell, K. J., Gewirtz-Meydan, A., Finkelhor, D., O'Brien, J. E., & Jones, L. M. (2023). The mental health of officials who regularly examine child sexual abuse material : Strategies for harm mitigation. *BMC Psychiatry*, 23(1). <https://doi.org/10.1186/s12888-023-05445-w>
- Mouheb, H. (2024). Intelligence artificielle, accélérateur de cybercriminalité : Appréhender le rôle complice de l'intelligence artificielle en matière de cybercriminalité. *Question(s) de management*, 49 (2), pp. 93-98. <https://doi.org/10.3917/qdm.229.0093>
- Musiani, F. (2020). Les réseaux pair-à-pair : plonger dans les coulisses d'Internet. *Effeillage*, 9. <https://doi.org/10.3917/eff.009.0075>

- Napier, S., C. Seto, M., Shackel, R., Cashmore, J., & McGeechan, K. (2025). Viewing Child Sexual Abuse Material for the First Time : Findings From an Anonymous Survey of Internet Users. *Sexual Abuse*, 37(7), 853-880. <https://doi.org/10.1177/10790632251326550>
- Nurmi, J., Paju, A., Brumley, B. B., Insoll, T., Ovaska, A. K., Soloveva, V., Vaaranen-Valkonen, N., Aaltonen, M., & Arroyo, D. (2024). Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy. *Scientific Reports*, 14(1). <https://doi.org/10.1038/s41598-024-58346-7>
- Parti, K., & Szabo, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material : Regulatory and Enforcement Perspectives in Europe. *Laws*, 13(6), pp.1-19.
- Pugnière-Saavedra, F. (2018). Un usage déviant du numérique : Le cas des détenteurs et des diffuseurs de vidéos pédopornographiques sur Internet. *Terminal*. <https://doi.org/10.4000/terminal.3317>
- Raphaël, F. (2007). Le rapport à l'image, *Revue des sciences sociales*. 37 (1), pp. 167-170.
- Reverchon, M. (2020). Imagination et Représentation chez Platon. *Philosophique*, 23 <https://doi.org/10.4000/philosophique.1408>
- Robin, M. (2021). Darknets : Les enjeux stratégiques et éthiques d'une technologie à double emploi. *Questions internationales*, 109 (5), pp.106-111. <https://doi.org/10.3917/quin.109.0106>
- Rojszczak, M. (2025). Preventing the dissemination of child sexual abuse material (CSAM) with surveillance technologies : The case of EU Regulation 2021/1232. *Computer Law & Security Review*, 56, 106097. <https://doi.org/10.1016/j.clsr.2024.106097>
- Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. *Computer Law & Security Review*, 58, <https://doi.org/10.1016/j.clsr.2025.106162>
- Sablon, M.-A. (2025). Réalités truquées et visages volés : l'UE risque-t-elle d'y perdre la face ? : La nécessité d'harmoniser les droits de la personnalité dans l'UE en réponse au développement de l'hypertrucage. *Les Cahiers de Propriété Intellectuelle*, 37 (1), 213-249.
- Salter, M., & Whitten, T. (2022). A Comparative Content Analysis of Pre-Internet and Contemporary Child Sexual Abuse Material. *Deviant Behavior*, 43(9), pp. 1120–1134 <https://doi.org/10.1080/01639625.2021.1967707>
- Salter, M., & Wong, T. (2024). Parental Production of Child Sexual Abuse Material : A Critical Review. *Trauma, Violence, & Abuse*, 25(3), pp. 1826-1837. <https://doi.org/10.1177/15248380231195891>
- Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual

- Abuse Material (CSAM). *Digital Investigation*, 29.
<https://doi.org/10.1016/j.diin.2019.04.005>
- Schmoll, P. (2002). Le statut anthropologique de l'image à l'ère du virtuel. *Futurs indicatifs*, 53, pp. 22-36.
- Steel, C. M. S. (2024). Artificial intelligence and CSEM - A research agenda. *Child Protection And Practice*, 2. <https://doi.org/10.1016/j.chipro.2024.100043>
- ten Hulsen, L. (2025). Digital fixes and techno-solutionism : The EU's tech-based battle against child sexual abuse. *New Journal of European Criminal Law*, 16(2), pp. f154-175.
<https://doi.org/10.1177/20322844251348131>
- Terrenoire, J. -P. (1985), Images et sciences sociales : L'objet et l'outil. *Revue française de sociologie*, 26, pp. 509-527 <https://doi.org/10.2307/3321747>
- Trivison, A. (2024). Understanding the Line between Art and Abuse : How Generative AI Changes the Landscape of Child Sexual Abuse Materials Comments. *Catholic University Journal of Law and Technology*, 33(1), pp. 87-114.
- Wolbers, H., Cubitt, T., & Cahill, M. (2025). Artificial intelligence and child sexual abuse : A rapid evidence assessment. *Trends & issues in crime and criminal justice*, 711.
<https://doi.org/10.52922/ti77802>
- Wortley, R., Findlater, D., Bailey, A., & Zuhair, D. (2024). Accessing child sexual abuse material : Pathways to offending and online behaviour. *Child Abuse & Neglect*, 154.
<https://doi.org/10.1016/j.chiabu.2024.106936>

Conférences

- Bursztein, E., Clarke, E., DeLaune, M., M. Eliff, D., Hsu, N., & Olson, L. (2019). Rethinking the Detection of Child Sexual Abuse Imagery on the Internet. Dans *WWW '19 : The World Wide Web Conference*. <https://doi.org/10.1145/3308558.3313482>
- Easttom, C. (2025). Malicious Use of Artificial Intelligence. Dans *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*.
<https://doi.org/10.1109/CCWC62904.2025.10903787>
- François, G., & Aubernon, M. (2024). Brève histoire de l'intelligence artificielle. *Administration & Éducation*, 183 (3), pp. 119-124. <https://doi.org/10.3917/admed.183.0119>
- M. Ngo, V., Thorpe, C., N. Dang, C., & McKeever, S. (2022). Investigation, Detection and Prevention of Online Child Sexual Abuse Materials : A Comprehensive Survey. Dans *2022 RIVF International Conference on Computing and Communication Technologies (RIVF)*.
<https://doi.org/10.1109/RIVF55975.2022.10013853>

Rapports

Dakota Szyf, N., Gilen, A., Giacometti, M., Van de Heyning, C., & Walvare, M. (2023). *Les deepnudes parmi les jeunes belges : les chiffres, le marché, l'impact*. <https://igvm-iefh.belgium.be/fr/documentation/les-deepnudes-parmi-les-jeunes-belges-les-chiffres-le-marche-limpact>

Fondation pour l'Enfance. (2024). *L'IA générative, nouvelle arme de la pédocriminalité*.

Internet Watch Foundation (IWF). (2026). *Harm without limits : AI child sexual abuse material through the eyes of our Analysts*. <https://admin.iwf.org.uk/media/h11nvditi/iwf-ai-csam-report-2026.pdf>

Internet Watch Foundation [IWF]. (2023). *How AI is being abused to create child sexual abuse imagery*. https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf

Negreiro, M. & European Parliamentary Research Service. (2020). *Curbing the surge in online child abuse : The dual role of digital technology in fighting and facilitating its proliferation*.

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659360/EPRS_BRI\(2020\)659360_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659360/EPRS_BRI(2020)659360_EN.pdf)

Negreiro, M. & European Parliamentary Research Service. (2026). *Combating child sexual abuse online*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI\(2022\)738224_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf)

Negreiro, M., Dilara Anaç, Ö., & European Parliamentary Research Service. (2026). *AI image generation and the spread of online child sexual abuse material*. [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/789297/EPRS_ATA\(2026\)789297_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/789297/EPRS_ATA(2026)789297_EN.pdf)

THORN. (2024). *Safety by Design for Generative AI : Preventing Child Sexual Abuse*. <https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf>

Childlight - Searchlight, Mojica, K., Harker, A., Norza, E., Giatis, K.-K., & Fry, D. (2025). *Where does the money flow ? An exploratory study on the financial structures of serious organised crime linked to child sexual exploitation*. https://www.pure.ed.ac.uk/ws/portalfiles/portal/499298134/Childlight_Searchlight_Report_2025.pdf

European Parliamentary Research Service, & Negreiro, M. (2025). *Children and deepfakes*.

INHOPE. (2024). *Annual Report 2024*. <https://inhope.org/media/pages/home/data-insights/4d2f6f4817-1767872796/inhope-annual-report-2024.pdf>

Niestadt, M. & European Parliamentary Research Service. (2025). *Protecting children online : Selected EU, national and regional laws and initiatives*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI\(2025\)769570_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI(2025)769570_EN.pdf)

Internet Watch Foundation (IWF). (2024). *What has changed in the AI CSAM landscape ?* https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf

Articles de journal en ligne

AFP. (2026). *Cyberattaque autonome menée par des modèles d'OpenAI : l'IA est-elle devenue trop puissante pour être contrôlée ?* RTBF. Consulté le 4 août 2026, à l'adresse <https://www.rtf.be/article/cyberattaque-autonome-menee-par-des-modeles-d-openai-l-ia-est-elle-devenue-trop-puissante-pour-etre-controlee-11762090>

Bracket Foundation. (2024). *Generative AI : A New Threat for Online Child Sexual Exploitation and Abuse*.

Drouelle, F. (2019). Eva Ionesco, itinéraire d'une enfance gâchée [Retranscription du podcast]. dans *France Inter*. Radio France. <https://www.radiofrance.fr/franceinter/podcasts/affaires-sensibles/eva-ionesco-itineraire-d-une-enfance-gachee-3415229>

Jaussent, V. (2022). Dessins « pédopornographiques », « apologie de l'inceste » . . . Pourquoi certaines BD de Bastien Vivès font l'objet d'un débat sur leur conformité à la loi. *Franceinfo*. https://www.franceinfo.fr/culture/bd/dessins-pedopornographiques-apologie-de-l-inceste-pourquoi-certaines-bd-de-bastien-vives-font-l-objet-d-un-debat-sur-leur-conformite-a-la-loi_5545998.html

Jaussent, V. (2026). « *C'est totalement indécent* » : des images dénudées de victimes de l'incendie de Crans-Montana générées avec l'intelligence artificielle Grok. *Franceinfo*. Consulté le 3 juillet 2026, à l'adresse https://www.franceinfo.fr/faits-divers/incendie-dans-un-bar-de-crans-montana-en-suisse/c-est-totalement-indecent-des-images-denudees-de-victimes-de-l-incendie-de-crans-montana-generees-avec-l-intelligence-artificielle-grok_7728565.html

Ladouce, F. (2025, août 10). Comment les pédocriminels récupèrent les photos de vos enfants publiées sur les réseaux sociaux. *RTBF Actus*. <https://www.rtf.be/article/comment-les-pedocriminels-recuperent-les-photos-de-vos-enfants-publiees-sur-les-reseaux-sociaux-11586271>

Le Monde. (2012). Irina Ionesco condamnée pour les photos sulfureuses de sa fille. *Le Monde*. https://www.lemonde.fr/societe/article/2012/12/17/irina-ionesco-condamnee-pour-les-photos-sulfureuses-de-sa-fille_1807528_3224.html

Qu'est-ce que l'"IA agentique" ? Comprendre son histoire pour dépasser l'effet de mode. (2026). *RTBF Actus*. <https://www.rtb.be/article/qu-est-ce-que-l-ia-agentique-comprendre-son-histoire-pour-depasser-l-effet-de-mode-11702497>

Résumé de haut niveau de la loi sur l'IA. (2024). EU Artificial Intelligence Act. Consulté le 10 juillet 2026, à l'adresse <https://artificialintelligenceact.eu/fr/high-level-summary/>

Simonart, C., & Damman, S. (2025). Vous postez des photos de vos enfants sur les réseaux sociaux ? Attention, elles peuvent alimenter les sites pédopornographiques. *RTL Info*. <http://www.rtl.be/actu/belgique/societe/vous-postez-des-photos-de-vos-enfants-sur-les-reseaux-sociaux-attention-elles/2025-08-05/article/758927>

Sites Internet

Défense des Enfants International - Belgique. (s. d.). Consulté le 13 août 2026, à l'adresse <https://www.dei-belgique.be/>

Soulseek. (s. d.). <https://www.slsknet.org/news/search/node/search%20this%20site>

Pages Internet

« *hacking* ». (s. d.). *belgium.be*. Consulté le 6 août 2026, à l'adresse https://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/hacking

18 novembre : Journée pour la protection des enfants contre l'exploitation et les abus sexuels. (s. d.). Conseil de L'Europe. Consulté le 10 août 2026, à l'adresse <https://www.coe.int/fr/web/children/end-child-sexual-abuse-day>

28 arrests in international strike against child sexual exploitation. (2026). Europol. <https://www.europol.europa.eu/media-press/newsroom/news/28-arrests-in-international-strike-against-child-sexual-exploitation>

AB-Arts. (2026). *Chat Control 1.0 et 2.0 : ce que l'Europe veut scanner*. AB - Arts. Consulté le 14 juillet 2026, à l'adresse <https://ab-arts.be/chat-control-1-0-2-0-europe-vie-privee>

About Us. (s. d.). Internet Watch Foundation. Consulté le 4 juillet 2026, à l'adresse <https://www.iwf.org.uk/about-us/>

Apprentissage profond (deep learning). (s. d.). CNIL. Consulté le 21 décembre 2025, à l'adresse <https://www.cnil.fr/fr/definition/apprentissage-profond-deep-learning>

Approche européenne de l'intelligence artificielle. (s. d.). Commission Européenne. Consulté le 4 août 2026, à l'adresse <https://digital-strategy.ec.europa.eu/fr/policies/european-approach-artificial-intelligence>

Artificial intelligence : threats and opportunities. (2020). European Parliament. <https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificial-intelligence-threats-and-opportunities>

Bergmann D. & Stryker C. *Qu'est-ce qu'un modèle de diffusion ?* IBM. Consulté le 2 juillet 2026, à l'adresse <https://www.ibm.com/fr-fr/think/topics/diffusion-models>

Bergmann, D. (s. d.). *Qu'est-ce que le machine learning (ML) ?* IBM. Consulté le 2 juillet 2026, à l'adresse <https://www.ibm.com/fr-fr/think/topics/machine-learning>

Bindé, J. (2022). Le festival d'Angoulême annule l'exposition de Bastien Vivès, accusé de pédopornographie. *BeauxArts*. <https://www.beauxarts.com/grand-format/le-festival-dangouleme-annule-lexposition-de-bastien-vives-accuse-de-pedopornographie/>

Child sexual exploitation. (s. d.). Europol. Consulté le 20 juillet 2026, à l'adresse <https://www.europol.europa.eu/crime-areas/child-sexual-exploitation>

Code de bonnes pratiques sur la transparence des contenus générés par l'IA. (s. d.). Commission Européenne. Consulté le 4 août 2026, à l'adresse <https://digital-strategy.ec.europa.eu/fr/policies/code-practice-ai-generated-content>

Conseil de l'Europe. (2024). *Adhérer à la Convention sur la cybercriminalité : les avantages*. <https://rm.coe.int/cyber-buda-benefits-fr-8-fev-2024/1680ae7112>

Darknet, dark web, clear web ou deep web ? (2022). CyberSecura. Consulté le 14 juillet 2026, à l'adresse <https://www.cybersecura.com/post/darknet-dark-web-clear-web-ou-deep-web>

Datta, A. (2026). Les législateurs européens réclament l'interdiction des IA génératrices d'images de nudité. *Euractiv*. <https://euractiv.com/fr/news/les-legislateurs-europeens-reclament-linterdiction-des-ia-generatrices-dimages-de-nudite/>

Défense des Enfants International - Belgique. (s. d.). Consulté le 13 août 2026, à l'adresse <https://www.dei-belgique.be/>

Direction centrale de la lutte contre la criminalité grave et organisée. (s. d.). Police Fédérale. Consulté le 8 juillet 2026, à l'adresse <https://www.police.be/5998/fr/propos/police-federale/police-judiciaire-federale/direction-centrale-de-la-lutte-contre-la>

Hard law/soft law. (s. d.). European Center For Constitutional And Human Rights. Consulté le 18 juillet 2026, à l'adresse <https://www.ecchr.eu/en/glossary/hard-law-soft-law/>

IBM Data & AI Team. (s. d.). AI vs. machine learning vs. deep learning vs. neural networks : What's the difference ? *IBM*. <https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks>

Images d'abus sexuel sur les mineurs. (s. d.). Childfocus. Consulté le 10 août 2026, à l'adresse <https://childfocus.be/fr-be/Exploitation-Sexuelle/Images-dabus-sexuels-sur-les-mineurs>

Instruments juridiques de l'UE. (s. d.). Union Européenne. Consulté le 16 juillet 2026, à l'adresse <https://eur-lex.europa.eu/FR/legal-content/glossary/eu-legal-instruments.html>

Intelligence artificielle : définition et utilisation. (2020). Parlement Européen - Thèmes. Consulté le 25 juin 2026, à l'adresse <https://www.europarl.europa.eu/topics/fr/article/20200827STO85804/intelligence-artificielle-definition-et-utilisation>

International Child Sexual Exploitation database. (s. d. -b). Interpol. Consulté le 12 août 2026, à l'adresse <https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database>

Interpol. (s. d.). *Terminologie adéquate.* <https://www.interpol.int/fr/Infractions/Pedocriminalite/Terminologie-adequate>

Le Conseil de l'Europe : éléments clés. (s. d.). Conseil de L'Europe. Consulté le 16 juillet 2026, à l'adresse <https://www.coe.int/fr/web/portal/the-council-of-europe-key-facts>

Le renseignement de sources ouvertes : qui et pourquoi ? (2024, 29 juillet). Police Locale Bruneau. Consulté le 7 juillet 2026, à l'adresse <https://www.police.be/5337/actualites/le-renseignement-de-sources-ouvertes-qui-et-pourquoi-osint>

Les risques du sharenting : pourquoi il vaut mieux y réfléchir à deux fois avant de partager en ligne des images de nos enfants. (2025, août 26). Police Fédérale. Consulté le 20 juillet 2026, à l'adresse <https://www.police.be/5998/fr/actualites/les-risques-du-sharenting-pourquoi-il-vaut-mieux-y-reflechir-deux-fois-avant-de-partager>

Ne pas confondre. (s. d.). Conseil de L'Europe. Consulté le 16 juillet 2026, à l'adresse <https://www.coe.int/fr/web/about-us/do-not-get-confused>

Nos outils et ressources : À qui s'adresse la Journée du 18 novembre et comment la promouvoir ? (s. d.). Conseil de L'Europe. Consulté le 10 août 2026, à l'adresse <https://www.coe.int/fr/web/children/our-material>

Notes des comités parlementaires : Exploitation sexuelle d'enfants sur Pornhub. (2021). Sécurité Publique Canada. Consulté le 17 juillet 2026, à l'adresse <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210722/026/index-fr.aspx>

Open-source Models vs. Closed-Source Models : A Simple Guide. (2026). Koat. Consulté le 1 juillet 2020, à l'adresse <https://koat.ai/open-source-models-vs-closed-source-models-a-simple-guide/>

Pédocriminalité : les failles d'Instagram - La méthode. (2024). Arte. Consulté le 16 juillet 2026, à l'adresse <https://papa.arte.tv/fr/articles/pedocriminalite-les-failles-dinstagram-la-methode>

Python : Définition et Guide Complet. (s. d.). Kern-it. Consulté le 26 juin 2026, à l'adresse <https://www.kern-it.be/fr/definitions/python/>

Qu'est-ce qu'un ransomware ? (s. d.). Microsoft. Consulté le 1 juillet 2026, à l'adresse <https://www.microsoft.com/fr-be/security/business/security-101/what-is-ransomware>

Qu'est-ce que le OnlyFans ? (s. d.). Internet Matters. Consulté le 15 août 2026, à l'adresse <https://www.internetmatters.org/fr/advice/apps-and-platforms/entertainment/onlyfans/>

Question. (s. d.). CNIL. Consulté le 1 juillet 2026, à l'adresse <https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi>

Signaleurs de confiance au titre de la législation sur les services numériques. (s. d.). Commission Européenne. Consulté le 25 juillet 2026, à l'adresse <https://digital-strategy.ec.europa.eu/fr/policies/trusted-flaggers-under-dsa>

Stryker, C. (s. d. a). *Qu'est-ce qu'un LLM ?* IBM. Consulté le 2 juillet 2026, à l'adresse <https://www.ibm.com/fr-fr/think/topics/large-language-models>

Stryker, C. (s.d. b). *Qu'est-ce que l'IA agentique ?* IBM. Consulté le 13 août 2026, à l'adresse <https://www.ibm.com/fr-fr/think/topics/agent-ai>

The Belgian Federal Police contributes to an international operation against a major child sexual exploitation platform. (2025). European Migration Network. Consulté le 26 juillet 2026, à l'adresse <https://emnbelgium.be/news/belgian-federal-police-contributes-international-operation-against-major-child-sexual>

What is Reddit : What parents need to know. (s. d.). Internet Matters. Consulté le 10 juin 2026, à l'adresse <https://www.internetmatters.org/fr/hub/news-blogs/what-is-reddit-what-parents-need-to-know/>

Dictionnaires en ligne

Connexionnisme. (s. d.). Dans *Larousse*. Consulté le 25 juin 2026, à l'adresse <https://www.larousse.fr/encyclopedie/philosophie/connexionnisme/191372>

Intelligence artificielle. (s. d.). Dans *Larousse*. Consulté le 25 juin 2026, à l'adresse https://www.larousse.fr/encyclopedie/divers/intelligence_artificielle/187257

nude. (s. d.). Dans *Le Robert - Dico En Ligne*. <https://dictionnaire.lerobert.com/definition/nude>

Prompt, prompté. (s. d.). Dans *Larousse*. <https://www.larousse.fr/dictionnaires/francais/prompt/64306>

Autres

Commission européenne. (2026). *EU agrees to simplify AI rules to boost innovation and ban “nudification” apps to protect citizens* [Communiqué de presse].

https://ec.europa.eu/commission/presscorner/detail/en/https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1024

Conseil de l'Europe, *MODÉRATION DE CONTENU* Meilleures pratiques en vue de la mise en place de cadres juridiques et procéduraux efficaces pour les mécanismes d'autorégulation et de corégulation de la modération de contenu, 19-21 mai 2021.

Fortin F. (2014), *C'est ma collection mais c'est bien plus que ça : analyse des processus de collecte et de l'évolution des images dans les collections de pornographie juvénile*, [Thèse de doctorat], Université de Montréal.

Grossman, S., Pfefferkorn, R., & Liu, S. (2025). *AI-generated child sexual abuse material*.

Karagoz, H., Lacour, L., & Maillot, N. (2025). *L'action de l'Union européenne en matière de lutte contre les cyberviolences sexuelles affectant les enfants* [Note dans le cadre d'une clinique juridique]. Université d'Angers.

MR. (2026, 9 janvier). *Le MR veut une réponse ferme contre les deepfakes sexuels* [Communiqué de presse]. Consulté le 10 août 2026, à l'adresse <https://www.mr.be/le-mr-veut-une-reponse-ferme-contre-les-deepfakes-sexuels/>

Pédocriminalité, les failles d'Instagram | Sources | ARTE. (2024). [Vidéo]. Youtube.

Consulté le 26 juillet 2026, à l'adresse https://www.youtube.com/watch?v=y_4aHv9lJss

Police Fédérale - DJSOC FCCU. (s. d.). *Comment l'IA façonne l'avenir de la cybercriminalité*. Document imprimé reçu lors d'un entretien, consultable lors de la défense orale.

Rougaïbi, M. (2024). *Les hypertrucages ou « deepfake » en droit canadien : exemples de l'inadéquation du droit face à cette technologie émergente* [Mémoire de Maîtrise, Faculté de Droit et la Faculté des Sciences de l'Université de Sherbrooke, Québec]. <https://usherbrooke.scholaris.ca/server/api/core/bitstreams/b2b43ef3-2c8d-4a6d-9a6e-89b87415ad99/content>

Annexes

Annexe A. Modèle d'analyse des entretiens

Exemple 1

Thématique	Procédure
Séquence	5 : 00 à 6 : 01
Résumé	Échange bilatéral entre les différentes organisations Europol, Interpol, OSINT et Child Focus. La détection dépend du nombre reçu. Dépend aussi si le site est hébergé en Belgique.
Mots-clés	Bilatéral, site, détection
Concepts	Procédure, sources de signalement, rôles des acteurs
Nuances	Distinction si le site est hébergé en Belgique ou non
Attitude	Ton plutôt monotone
Intervention	Relance pour savoir si ce sont les acteurs cités les principales sources de signalement
Extraits	« Notre détection est surtout basée sur ce qu'on reçoit des informations des différents pays autour de nous, via interpol europol ou bilatéral ou OSINT (...) ou Child Focus »

Exemple 2

Thématique	Dark-web/recherche
Séquence	6 : 01 à 7 : 05
Résumé	Différence entre aspect et criminel et l'aspect commercial. Diffusion dans un environnement classique comme les réseaux sociaux et enlever les images via le parquet. Le darkweb est plus difficile, car c'est un environnement criminel, pas moyen d'aller effacer des images de manière judiciaire. L'enquête et la localisation du serveur est une tout autre procédure. Le serveur est rarement chez nous
Mots-clés	Aspect criminel et commercial, darkweb, diffusion, procédure, serveur
Concepts	Commercialisation, inaccessibilité
Nuances	Précision quant au fait que les serveurs sont rarement belges
Attitude	Ne rentre pas trop dans les détails
Intervention	/

Extraits	« Il faut faire la différence entre l’aspect criminel ou l’aspect commercial si les images sont diffusées dans un environnement classique comme les réseaux sociaux, y a la procédure qui existe déjà pour enlever les images euh... via le parquet mais si les images sont diffusées via le darkweb par exemple, ça c’est beaucoup plus difficile puisque c’est un environnement criminel dont on a pas les moyens d’aller effacer les images d’une manière judiciaire donc là il faut une enquête, il faut une localisation du serveur et aller saisir le serveur donc c’est tout à fait une autre procédure pour obtenir l’effacement des images quoi.. » « puis le serveurs qui est pas forcément chez nous non plus quoi » « c’est rarement chez nous »
----------	---

Annexe B. Liste des personnes contactées

Type d’acteurs	Moyens de contact	Intérêts	Entretiens
Police Fédérale – direction centrale de la lutte contre la criminalité grâce et organisée – section child abuse	Formulaire de contact	Rencontre d’un expert <i>computer crime unit</i> , un spécialiste Child Abuse, un chercheur OSINT, organisme au cœur de la thématique, enquête et détecte	Réalisé le 24 mars 2026
Police locale de Jodoigne	Email	Section mœurs	
Police des communes d’Uccle, Watermael – Boitsfort et Auderghem	Email	Section mœurs	
Policière travaillant dans une section mœurs	Email	Spécialement recommandée par une autre personne travaillant à la police. Personne souvent confrontée au <i>deepfake</i>	

Internet Watch Foundation	Formulaire de contact	Organisation qui fournit des bases de données, des rapports sur l'impact de l'IA générative dans le domaine des MASE	
National Center for Missing Children	Formulaire de contact	Base de données pour les MASE, détection, prévention et lutte	
Institut pour l'égalité des femmes et des hommes	Formulaire de contact	Article sur les <i>deepnudes</i> , violence de genre, combat les discriminations de genre https://igvm-iefh.belgium.be/fr/propos-de-linstitut	
We protect global alliance	Formulaire de contact	Lutte contre l'exploitation sexuelle des enfants en ligne https://www.weprotect.org/about-us/	
Child Focus	Email	Exploitation sexuelle d'enfants Signalement possible via leur site internet	Entretien réalisé le 8 juin 2026
Child Focus – trusted flaggers	Email	Modérateur de contenu en ligné dont le rôle est inscrit dans une loi	
Cecilian Johanson	Email	Elle a écrit un document sur une thématique similaire à notre recherche	
Project Arachnid	Formulaire de contact	Service qui développe une technologie de webcraling automatique pour aider à la détection des images d'abus sexuels sur mineurs	
Europol	Formulaire de contact	Prévention et combat notamment de la cybercriminalité	
Interpol	Formulaire de contact	Organisation internationale de police criminelle – lutte contre la	

		criminalité internationale	
Cybertipline	Formulaire de contact	Site afin de signaler de l'exploitation sexuelle d'enfant https://report.cybertip.org/	
INHOPE	Formulaire de contact	Support pour les services d'assistances téléphoniques – suppression de contenu et signalement https://www.inhope.org/	
Criminologues de parquet	Email	Expérience de terrain – impact dans les dossiers judiciaires	Entretien réalisé le 9 juin 2026

Charlier Faustine

août 2026

Une étude exploratoire de l'impact de l'intelligence artificielle sur les images d'abus sexuels sur mineurs

Promotrice : Professeure Marie-Sophie Devresse

Les images d'abus sexuels sur mineurs manipulées par l'intelligence artificielle : un raz de marée, un phénomène incontrôlé, une course contre la montre. Cette recherche exploratoire envisage la reconfiguration des images d'abus sexuels sur mineurs à l'ère de l'intelligence artificielle. En combinant apports théoriques et extraits illustratifs issus de nos entretiens exploratoires, nous avons tenté de produire un état des lieux francophone sur la question. En toile de fond de cette recherche inductive : l'intelligence artificielle occupe une grande place dans notre quotidien, a priori inoffensive, mais certains s'en sont emparés pour en faire une utilisation détournée. Les résultats sont sans appel : une nouvelle criminalité, un impact considérable sur les victimes, une économie bien organisée, une obsolescence programmée des outils de détection et bien d'autres.

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR

Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique | www.uclouvain.be/drt