COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Respecter les droits de l'homme et l'État de droit lors de l'utilisation de technologies automatisées pour détecter l'exploitation et les abus sexuels d'enfants en ligne

Rapport d'experts indépendants

Direction générale des droits de l'homme et de l'État de droit (DG I) et Direction générale de la démocratie (DG II)

Juin 2021

Le présent rapport a été établi par les experts indépendants ci-après :

Liora Lazarus, Jean-Christophe Le Toquin, Manuel Magriço Aires, Francisco Nunes, Katarzyna Staciwa (apportant également son concours à l'expert principal), Gert Vermeulen et Ian Walden, sous la direction de Linos-Alexandre Sicilianos, ancien Président de la Cour européenne des droits de l'homme, et avec le soutien du Secrétariat du Conseil de l'Europe.

Les vues exprimées dans cet ouvrage relèvent de la responsabilité des auteurs et ne reflètent pas nécessairement la ligne officielle du Conseil de l'Europe.

Table des matières

RÉSUMÉ

L'ampleur de l'exploitation et des abus sexuels d'enfants en ligne augmente à un rythme alarmant. D'après l'Évaluation de la menace que représente la criminalité organisée sur l'internet (Europol, 2020), les chiffres découlant des activités de détection de matériels d'abus sexuels sur des enfants augmentaient déjà chaque année mais ils se sont brusquement envolés au plus fort de la crise de la covid-19.

En 2020, par exemple, les signalements reçus par CyberTipline, un service de signalement aux États-Unis, concernaient notamment 33,6 millions d'images, dont 10,4 millions inédites, et 31,6 millions de vidéos, dont 3,7 millions inédites. En 2020, CyberTipline a reçu 21,7 millions de signalements, soit 28 % de plus qu'en 2019. Selon le réseau INHOPE, 60 % de toutes les URL évaluées en 2020 contenaient du matériel déjà analysé, ce qui signifie que les mêmes contenus sont diffusés et signalés à maintes reprises, et que les enfants concernés subissent de nouvelles victimisations du fait de la circulation ininterrompue des images des abus qu'ils ont endurés.

Face à cette tendance des plus préoccupantes, il faut adopter des techniques innovantes. À ce jour, la réponse à ce grave problème passe essentiellement par les mesures qu'appliquent volontairement les acteurs du secteur privé qui, à l'aide de technologies automatisées, peuvent détecter, puis signaler et retirer, le matériel d'abus sexuels sur des enfants ainsi que les menaces par textos, comme la sollicitation à des fins sexuelles (également appelé « grooming »).

La détection automatique de contenu et/ou de comportements repose sur trois grandes familles de technologies : la plus élémentaire est le hachage de fichiers (« hashing »), l'intermédiaire est la vision par ordinateur, et la plus innovante repose sur l'intelligence artificielle et notamment sur son application la plus avancée : l'apprentissage en profondeur.

S'il est essentiel de trouver des méthodes pour identifier et aider à secourir les enfants victimes, pour enquêter sur les infractions et pour stopper la circulation du matériel d'abus sexuels sur des enfants, le recours à une technologie automatisée peut avoir un impact sur la confidentialité – que les fournisseurs de service doivent assurer – du contenu des communications et des données relatives au trafic. Ces méthodes peuvent donc entraîner une ingérence dans le droit au respect de la vie privée et de la vie familiale et dans la protection des données à caractère personnel des personnes concernées.

En septembre 2020, la Commission européenne a proposé une dérogation temporaire à certaines dispositions de la directive vie privée et communication électronique afin de permettre le traitement des données à caractère personnel et autres données dans le but de lutter contre l'exploitation et les abus sexuels d'enfants en ligne. Le débat qu'a suscité cette proposition illustre bien la complexité des enjeux.

Les États ont l'obligation positive de protéger les enfants contre l'exploitation et les abus sexuels. Pour ce faire, ils doivent toutefois tenir compte d'un environnement complexe et évolutif, tant du point de vue technologique que juridique. En décembre 2020, les États Parties à la Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels, ont demandé au Conseil de l'Europe de réunir les experts de l'Organisation afin que ceux-ci les aident à trouver des solutions appropriées pour concilier les différents droits humains en jeu tout en assortissant de garanties les dispositions prises dans l'intérêt public.

Le présent rapport constitue la première étape de la réponse du Secrétaire général à l'appel du Comité de Lanzarote.

Ce rapport est basé sur les contributions individuelles et l'effort collectif d'un groupe d'experts indépendants dans les domaines des droits humains, de la protection de l'enfance, de la protection des données et de la lutte contre la cybercriminalité. Le groupe était dirigé par Linos-Alexandre Sicilianos, ancien président de la Cour européenne des droits de l'homme, avec le soutien du Secrétariat du Conseil de l'Europe.

Tout en évoquant les avantages que pourraient apporter des dispositions obligatoires, ce rapport se concentre sur la mise en place volontaire de mécanismes de détection et de signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne qui soient principalement fondés sur l'intérêt public tel que décrit dans les cadres juridiques en vigueur. C'est ce qui a dicté le choix des solutions technologiques analysées dans le présent document.

Après avoir évoqué le volume considérable de contenus d'abus sexuels d'enfants en ligne et l'intérêt de leur détection automatique, les experts décrivent les technologies utilisées, leurs limites et leur potentiel. L'enjeu principal reste de déterminer quels sont les moyens les moins restrictifs permettant de détecter les cas d'exploitation et d'abus sexuels d'enfants en ligne tout en protégeant dûment les victimes. Pour y répondre, il faut comprendre très précisément l'objectif recherché et l'environnement pour lequel telle ou telle technologie sera sélectionnée. Selon les experts, le choix devrait être guidé par la complexité de l'objectif, de l'environnement et de la technologie ainsi que par la maturité de la technologie (une technologie bien éprouvée, bien documentée et stable est un choix plus sûr pour les décideurs, alors qu'il sera plus difficile de définir le niveau approprié de garanties pour une technologie qui en est aux premiers stades de son développement).

Les experts mettront en outre l'accent sur le cadre juridique applicable et décriront les principales normes internationales concernées (à l'échelon mondial, à celui du Conseil de l'Europe et à celui de l'UE). Jouent un rôle particulièrement important :

- la Convention des Nations Unies relative aux droits de l'enfant et son Protocole facultatif concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants ;
- la Convention du Conseil de l'Europe sur les droits de l'homme, la Charte sociale européenne et les conventions sur la protection des enfants contre l'exploitation et les abus sexuels, sur la cybercriminalité, et sur la protection des données (également appelée Convention 108+) ;
- la directive de l'UE 2002/58/CE du Parlement européen et du Conseil (directive vie privée et communications électroniques) ainsi que le Code européen des communications électroniques.

L'importance de la jurisprudence européenne ressort par ailleurs de l'analyse d'arrêts de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne.

Le rapport contient neuf recommandations portant sur des sujets tels que la nécessité de s'adapter au rythme de l'évolution technologique, d'accroître la transparence et la responsabilité, de coordonner les efforts et de renforcer le dialogue entre le secteur privé et les décideurs/régulateurs, d'intégrer des garanties dès les premières étapes du développement technologique, d'accorder l'importance

nécessaire à l'obligation positive de protéger les enfants contre la violence sexuelle et de définir un cadre juridique offrant une sécurité juridique aux fournisseurs de services et tenant compte des évolutions technologiques futures. Les experts appellent également à la mise en place d'un cadre fondé sur l'intérêt public, ancré dans la Convention de Lanzarote, permettant aux fournisseurs de services de détecter automatiquement, puis de supprimer, de signaler et de transférer les contenus d'exploitation et d'abus sexuels en ligne, dans le respect des conditions et des garanties décrites dans le rapport en matière de protection des données et de respect de la vie privée.

Ce rapport est un incontournable pour toute personne soucieuse de la protection des enfants contre la violence sexuelle et active dans ce domaine. Les experts ont veillé à rendre le contenu accessible à la plupart des lecteurs, malgré la complexité de la question.

Le rapport devrait par ailleurs contribuer à la consultation lancée par la Commission européenne en décembre 2020 au sujet d'une proposition de règlement du Parlement européen et du Conseil sur la détection, la suppression et le signalement des abus sexuels d'enfants en ligne.

1. INTRODUCTION

1.1 Objet du présent document

L'ampleur de l'exploitation et des abus sexuels d'enfants en ligne augmente – dans l'absolu aussi bien qu'en termes de quantité de signalements aux forces de l'ordre et à la société civile – à une vitesse alarmante[1] et appelle à l'adoption de nouvelles techniques de lutte, innovantes. Cet appel a été renforcé par une publication stratégique phare d'Europol[2] – l'Évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA, 2020)[3] – dont il ressort qu'alors que les principales menaces liées à l'exploitation et aux abus sexuels d'enfants en ligne étaient restées assez stables ces dernières années, la pandémie de covid-19 a changé la donne. Selon les résultats de cette évaluation, de plus en plus de matériels d'abus sexuels sur des enfants en ligne étaient déjà détectés chaque année mais les chiffres ont brutalement augmenté au plus fort de la crise, sous l'effet de l'intensification des échanges en ligne de matériels d'abus sexuels sur des enfants qui s'est produite lors des restrictions de contacts et de déplacements. Il devrait en outre y avoir, dans le sillage de la pandémie ainsi que du confinement et des restrictions de déplacement qu'elle a entraînés, un accroissement des signalements de cas d'exploitation et d'abus sexuels d'enfants en ligne, car les abus commis durant la pandémie de covid-19 pourraient n'être signalés aux autorités que bien après les faits. De même, la

[1] WePROTECT Global Alliance, Global Threat Assessment 2019, *'Working together to end the sexual exploitation of children online'*, p. 2, (consultable à l'adresse : https://www.end-violence.org/sites/default/files/paragraphs/download/Global%20Threat%20Assessment%202019.pdf).

[2] L'Agence de l'Union européenne pour la coopération des services répressifs, mieux connue sous l'acronyme Europol, anciennement Office européen de police et Unité Drogues Europol, est l'agence de police de l'Union européenne (UE) créée en 1998 pour faciliter le traitement du renseignement en matière pénale et combattre la criminalité internationale et le terrorisme à l'aide d'une coopération entre les autorités compétentes des États membres de l'UE. Son siège est à La Haye.

[3] IOCTA 2020, p. 35, *(consultable à l'adresse :* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020).

quantité de matériels indécents autoproduits devrait augmenter considérablement, entraînant probablement une hausse de la sollicitation et de l'exploitation en ligne[4].

À ce jour, les mesures en vigueur pour lutter contre le problème que posent l'exploitation et les abus sexuels d'enfants en ligne sont essentiellement celles qu'appliquent volontairement les acteurs du secteur privé à l'aide de technologies de détection automatique[5] pour détecter, signaler et supprimer le matériel d'abus sexuels sur des enfants ainsi que les menaces par textos, comme la sollicitation à des fins sexuelles (le « grooming »). Il existe une exception, aux États-Unis, où la législation fédérale impose aux fournisseurs de services basés dans le pays[6] de signaler à CyberTipline, qui relève du National Center for Missing & Exploited Children (NCMEC), les cas de « *pornographie enfantine* »[7] apparents qu'ils découvrent dans leurs systèmes[8]. Ces signalements, que le NCMEC communique ensuite aux services répressifs du monde entier[9], forment une part considérable des affaires sur lesquelles des enquêtes approfondies doivent être menées.

Les signalements faits par les acteurs du secteur privé sont indispensables pour permettre d'identifier les enfants victimes et de les soustraire aux abus qu'ils subissent ainsi que pour stopper la diffusion du matériel d'abus sexuels sur des enfants, mais deux problèmes se posent en l'état actuel des choses. Premièrement, il existe un décalage notable entre le recours à des technologies de détection automatique et la quantité d'informations publiées sur l'adoption de ces technologies. De par ce décalage, les décideurs et régulateurs ont du mal à définir une approche cohérente pour réglementer ces technologies et veiller à ce que des garanties adéquates soient offertes. Deuxièmement, le cadre juridique régissant le comportement des fournisseurs de services peut sembler inadéquat car il s'appuie sur l'adoption volontaire par ces derniers de technologies de détection de l'exploitation et des abus sexuels d'enfants en ligne, et car même lorsque les règles sont impératives, comme aux États-Unis, les fournisseurs de services ne sont pas obligés de rechercher ce phénomène de façon proactive. Pour ce qui est des signalements, la plupart des pays s'en remettent à leur transmission volontaire aux forces de l'ordre car vu les volumes concernés, il est concrètement exclu que celles-ci doivent systématiquement soumettre une demande impérative. En conséquence, comme il n'existe actuellement pas de cadre ad hoc fondé sur l'intérêt public qui permettrait aux acteurs du secteur privé d'adopter des pratiques visant à répondre efficacement aux graves problèmes que posent

---

[4] Ibid, p. 41.

[5] Voir section 2, « *Tour d'horizon technique* ».

[6] Un fournisseur de services est un « prestataire de services de communications électroniques ou de services informatiques à distance » (18 USC § 2258E(6)).

[7] La législation fédérale des États-Unis définit la « pornographie enfantine » comme « *toute représentation visuelle d'un comportement sexuellement explicite impliquant un mineur (une personne de moins de 18 ans)* ». Allant plus loin que la définition légale, le NCMEC choisit de qualifier ces images de matériel d'abus sexuels sur des enfants afin de mieux rendre compte de ce qui est représenté : l'abus sexuel et l'exploitation d'enfants. Pour en savoir plus, voir : https://www.missingkids.org/theissues/csam

[8] Gérée par le National Center for Missing & Exploited Children. Le National Center for Missing & Exploited Children (NCMEC) est une organisation de droit privé à but non lucratif dont la mission est d'aider à retrouver les enfants disparus, de réduire l'exploitation sexuelle des enfants et d'empêcher la victimisation des enfants. Le NCMEC travaille avec les familles, les victimes, le secteur privé, les forces de l'ordre et le public pour aider à prévenir les enlèvements d'enfants et à retrouver les enfants disparus, et pour fournir des services visant à empêcher l'exploitation sexuelle des enfants et à la combattre. Voir section 2.2.1, « Rôle spécifique du National Center for Missing & Exploited Children (NCMEC, États-Unis) ».

[9] Les rapports de 2019 et 2020 par pays peuvent être consultés à l'adresse : https://www.missingkids.org/gethelpnow/cybertipline.

l'exploitation et les abus sexuels d'enfants en ligne, ces acteurs n'ont aucune sécurité juridique pour ce faire et les initiatives prises pour combattre ce phénomène sont souvent fragmentées et font double emploi.

Le présent document a donc pour objet de donner des orientations aux États membres du Conseil de l'Europe[10] afin qu'ils puissent veiller au respect des droits humains et de l'État de droit lorsqu'ils emploient une technologie automatisée pour détecter l'exploitation et les abus sexuels d'enfants en ligne. Ces orientations ont été déclarées nécessaires à la 30e réunion du Comité de Lanzarote[11], dont le Secrétariat a été invité à vérifier s'il était envisageable d'établir un avis exhaustif du Conseil de l'Europe qui serait fondé sur les droits humains et évoquerait toutes les dimensions susmentionnées[12]. Elles devraient en outre venir contribuer aux travaux de la Commission européenne sur un projet de solution à long terme à l'été 2021[13].

Ces orientations avaient notamment pour antécédent le débat tenu au sein de l'Union européenne sur une dérogation temporaire[14] aux articles 5, paragraphe 1, et 6 de la Directive 2002/58/CE (directive vie privée et communications électroniques)[15] en ce qui concerne l'utilisation volontaire de technologies par des fournisseurs de services de communications interpersonnelles non fondés sur la numérotation, par exemple la voix sur protocole internet (VOIP) ou les services de messagerie et de courrier électronique par internet, 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.

Tout en évoquant les avantages que pourraient apporter des dispositions obligatoires, en termes de clarté et de sécurité juridiques, de processus démocratiques inclusifs ainsi que de reconnaissance et de soutien généralisés, ce rapport se concentre sur la mise en place volontaire, par les fournisseurs de services, de mécanismes de détection et de signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne, principalement fondés sur l'intérêt public tel que décrit dans les cadres juridiques en vigueur. C'est ce qui a dicté le choix des solutions technologiques analysées dans le présent document.

Vu le contexte, il est par ailleurs important de rappeler que la terminologie utilisée dans les instruments du Conseil de l'Europe et de l'UE n'est pas toujours harmonisée. Aux fins du présent document, il convient notamment de préciser que dans ses dispositions, la directive vie privée et communications électroniques fait référence aux « *services de communications électroniques* », notion plus étroite que celle de « *fournisseurs de services* » qu'emploie la Convention de Budapest[16][17]. En

[10] https://www.coe.int/fr/web/portal/home
[11] https://www.coe.int/fr/web/children/lanzarote-committee
[12] Liste des décisions adoptées par le Comité de Lanzarote le 10 décembre 2020 (consultable à l'adresse : https://rm.coe.int/liste-des-decisions-30eme-reunion-comite-de-lanzarote/1680a0b1ec).
[13] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Lutte-contre-les-abus-sexuels-concernant-des-enfants-detection-suppression-et-signalement-des-contenus-illicites-en-ligne_fr
[14] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52020PC0568
[15] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). Journal officiel de l'Union européenne, L 201, 31/07/2002 P. 0037–0047, (consultable à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32002L0058&from=FR).
[16] https://rm.coe.int/168008156d
[17] Voir section 3.2.1, *La notion de* « *fournisseur de services* ».

outre, si les notions de protection de la vie privée et de protection des données sont inextricablement liées dans la Convention européenne des droits de l'homme (CEDH)[18], la Charte des droits fondamentaux les distingue en tant que droits. C'est ainsi que la directive vie privée et communications électroniques repose sur le droit à la protection de la vie privée alors que le Règlement général sur la protection des données (RGPD)[19] repose quant à lui sur le droit à la protection des données. Il faut garder ces divergences à l'esprit à la lecture du présent document.

Enfin, il faut souligner que la question – qui mérite un avis à elle seule – de la portée extraterritoriale des obligations positives relatives à la lutte contre l'exploitation et les abus sexuels d'enfants en ligne n'est pas traitée de manière exhaustive dans le présent document.

1.2 Méthodologie

Les informations présentées dans ce document reposent sur les diverses contributions d'un groupe d'experts indépendants invité par le Secrétariat du Conseil de l'Europe. Liora Lazarus, Jean-Christophe Le Toquin, Manuel Aires Magriço, Francisco Nunes, Katarzyna Staciwa (apportant également son concours à l'expert principal), Gert Vermeulen et Ian Walden, sous la direction de Linos-Alexandre Sicilianos, ancien Président de la Cour européenne des droits de l'homme. Lorsqu'il y avait lieu, des documents publics disponibles au moment de la rédaction sont venus compléter leurs contributions, par exemple des informations provenant d'autres sources spécialisées, d'entreprises du secteur privé et de diverses organisations et institutions.

Le document est scindé en deux parties : la première propose un tour d'horizon technique et explique le rôle que jouent actuellement les technologies automatisées pour lutter efficacement contre l'exploitation et les abus sexuels d'enfants en ligne, une analyse simplifiée des solutions technologiques concernées ainsi que des exemples de leurs applications concrètes. Dans sa seconde partie, le document donne un aperçu du cadre juridique applicable : il décrit le débat relatif à la proposition de la Commission européenne de déroger temporairement à certaines dispositions de la directive vie privée et communications électroniques, il explique la notion de « *fournisseur de services* » et en décrit le comportement, et il informe les lecteurs au sujet des propositions de réglementation concernant les fournisseurs de services annoncées par la Commission dans le processus de consultation publique. Il se concentre ensuite sur les obligations positives liées à la lutte contre l'exploitation et les abus sexuels d'enfants en ligne, en particulier sur celles qui découlent de la jurisprudence de la Cour européenne des droits de l'homme[20] (la Cour) ainsi que des conventions du Conseil de l'Europe : en matière de protection des enfants contre l'exploitation et les abus sexuels (la Convention de Lanzarote), en matière de cybercriminalité (la Convention de Budapest) et en matière de protection des données (la Convention 108+).[21] [22]

[18] https://www.echr.coe.int/documents/convention_fra.pdf
[19] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[20] https://www.echr.coe.int/Pages/home.aspx?p=home&c=fre
[21] https://www.coe.int/fr/web/children/lanzarote-convention
[22] https://www.coe.int/fr/web/data-protection

1.3 Description du phénomène

Le phénomène de l'exploitation et des abus sexuels d'enfants est en constante évolution. L'on compte à l'heure actuelle au moins deux fois plus de formes d'exploitation et d'abus sexuels d'enfants par rapport à la fin des années 1990. À cette époque, des matériels tels que des copies numériques d'images commerciales plus anciennes représentant des enfants victimes et montrant que l'on avait affaire à des productions familiales, ont commencé à circuler en ligne, à côté de diverses vidéos commerciales produites pour la vente.

L'arrivée des technologies de l'information et de la communication (TIC) dans notre quotidien a créé un lien indestructible entre les environnements hors ligne et en ligne où les enfants peuvent être exposés aux mêmes risques, et par exemple être poussés à s'engager dans un comportement sexuel explicite (réel ou simulé), être recrutés pour participer à des spectacles pornographiques ou être contraints d'y participer ou d'assister à des activités ou abus sexuels. De nombreux enfants sont victimes d'exploitation et d'abus sexuels de multiples façons : ils sont victimes à la fois des délinquants qui commettent des abus sexuels physiques à leur encontre et des délinquants qui produisent, diffusent, exigent, commandent, vendent ou achètent, échangent, téléchargent ou diffusent en streaming du contenu relatif à de l'exploitation sexuelle et à des abus sexuels à l'encontre d'enfants, ou qui, par le biais d'autres TIC, assistent et contribuent à l'exploitation sexuelle et aux abus sexuels contre ces enfants[23]. Il ressort clairement de recherches soigneusement menées à partir de divers éléments probants que les infractions à caractère sexuel commises contre des enfants, notamment celles qui sont facilitées par l'utilisation des TIC, ont un impact préjudiciable durable sur les victimes. C'est particulièrement le cas lorsque des matériels – images ou vidéos représentant les victimes – circulent bien après que les abus sexuels physiques ont été commis.

Les enfants subissent de nouvelles victimisations du fait de la circulation ininterrompue des images des abus qu'ils ont endurés. La technologie qui sert à identifier ces images est par conséquent essentielle à leur protection. Étant donné que les autorités répressives du monde entier sont confrontées à une immense quantité de matériels en ligne d'abus sexuels sur des enfants, il est indispensable que des solutions technologiques permettant de combattre efficacement ce phénomène soient mises en œuvre pour apporter une réponse adaptée, notamment en donnant rapidement la priorité à ces affaires.

Pour réussir à prévenir et combattre l'exploitation et les abus sexuels d'enfants en ligne, il faut se tenir au courant de l'évolution constante de ce domaine et y réagir, évolution que facilite notamment l'utilisation prédominante des TIC, qui ne cessent de se développer. L'un des éléments capitaux d'une telle approche, essentielle à la protection efficace des enfants contre l'exploitation et les abus sexuels en ligne dans le monde d'aujourd'hui, consiste à adopter des solutions technologiques dans ce domaine, susceptibles – selon la solution choisie – de soutenir ou, tout en faisant toujours appel à une intervention humaine, de remplacer dans une certaine mesure le facteur humain pour diverses tâches. Toutefois, ce choix doit être fait dans le respect des droits fondamentaux des enfants, notamment le droit au respect de la vie privée ou à la liberté d'expression.

[23] Avis interprétatif sur l'applicabilité de la Convention de Lanzarote aux infractions sexuelles commises à l'encontre des enfants et facilitées par l'utilisation des technologies de l'information et de la communication (TIC), adopté par le Comité de Lanzarote le 12 mai 2017, p. 5 (consultable à l'adresse : https://rm.coe.int/t-es-2017-03-fr-final-avis-interpretatif/168071cb5e).

2. TOUR D'HORIZON TECHNIQUE

2.1 Les trois grandes familles d'outils de détection automatique de l'exploitation et des abus sexuels d'enfants en ligne[24]

La présente section propose un tour d'horizon schématique des principales technologies automatisées permettant de détecter l'exploitation et les abus sexuels d'enfants en ligne. La détection automatique de contenu et/ou de comportements repose sur trois grandes familles de technologies : la plus élémentaire est le hachage de fichiers, l'intermédiaire est la vision par ordinateur, et la plus innovante est l'intelligence artificielle et notamment l'apprentissage en profondeur, qui est la forme la plus avancée d'intelligence artificielle, susceptible d'arriver à traiter les scénarios les plus complexes.

Le tableau ci-après offre un tour d'horizon des trois principales familles d'outils de détection automatique du contenu et/ou des comportements et en décrit la complexité.

Cible	**Fichier → Image → Contenu spécifique de l'image → Comportements→ Personnes**				
(In)connu	**Contenu connu → Nouveau contenu ou comportement**				
Maturité	**Technologie mature → Technologie en phase de recherche**				
Qualité	**Données homogènes provenant de sources crédibles → Données hétérogènes**				
Technologies	**Hachage de fichiers**	**Vision par ordinateur (images et vidéos)**		**Intelligence artificielle (comportements et personnes)**	
Types		**Descripteurs globaux**	**Descripteurs locaux**	**Apprentissage automatique**	**Apprentissage en profondeur**

Simple *Complexe*

Pour choisir la technologie la mieux adaptée à ses besoins, il faut avoir une compréhension précise des objectifs et de l'environnement dans lequel la technologie est utilisée. Elles sont les suivantes :

- *Facteur lié à la cible* – Qu'est-ce qui doit être détecté : un fichier, du contenu ou une personne ? Par exemple, il est bien plus simple de repérer un fichier connu de type « csam1.jpg » que d'identifier une personne à l'aide de la reconnaissance faciale.
- *Facteur lié à un contenu/comportement (in)connu* – Qu'est-ce qui doit être détecté : un contenu et/ou un comportement connu ou inconnu ? La tâche la plus difficile ne consiste pas tant à rechercher du contenu déjà connu qu'à détecter du contenu inédit et/ou des comportements nouveaux : du matériel inédit d'abus sexuels sur des enfants ou des cas d'adultes sollicitant des enfants à des fins sexuelles. Par exemple, un fournisseur

[24] On trouvera en annexe un autre graphique donnant un aperçu des technologies de détection du contenu visuel des images et vidéos.

d'hébergement ou de réseaux sociaux peut décider de détecter du matériel d'abus sexuels sur des enfants de façon réactive, après avoir reçu une notification, ou il peut agir de façon proactive et analyser tous les contenus téléchargés sur ses serveurs. Dans les deux cas, la technologie de détection utilisée reste la même.

- *Facteur lié à la maturité* – La technologie de détection est-elle mature ou en est-elle au stade de la recherche ? Une technologie mature peut être définie comme étant stable, bien documentée et testée au fil des ans ; elle est plus facile à comprendre et à réglementer, et ses résultats sont nettement plus fiables.
- *Facteur lié à la qualité* – Quel est le degré de fiabilité de la base de données de référence ? La technologie de détection automatique s'appuie souvent sur un jeu de données préexistant : plus la base de données de référence est fiable, meilleure est l'efficacité.

2.1.1 Hachage de fichiers

Le hachage de fichiers repose sur un algorithme mathématique dans lequel un fichier est réduit à une signature, par exemple : 3CBCFDDEC145E3382D592266BE193E5BE53443138EE6AB6CA09FF20DF609E268[25]. Cette technologie, qui permet de détecter un fichier identique, est capable d'interroger d'importantes bases de données de signatures avec peu de ressources informatiques. Sa limite tient au fait qu'elle est trompée par la modification du moindre bit ou pixel : celle-ci entraîne la création d'une signature différente et il n'est plus possible de comprendre si les deux fichiers sont identiques ou non. D'aucuns soulignent parfois que le hachage de fichiers ne renvoie pas de faux positifs, c'est-à-dire que deux images différentes ne peuvent pas avoir la même signature. Si c'est exact, c'est alors un avantage dans le cadre des enquêtes et des procès, principalement lorsque les éléments de preuve sont uniquement fondés sur le hachage sans intervention humaine. Toutefois, une recherche a montré qu'il existait un risque infime que deux fichiers différents renvoient à une même image : c'est ce qui s'appelle le « *risque de collision* »[26].

Les algorithmes les plus fréquents sont le MD5 et le SHA-1, que de nombreux services répressifs ont adopté ainsi que des entreprises et quelques services de signalement, dont CyberTipline (États-Unis), Internet Watch Foundation (IWF) (R.-U.)[27], Expertisebureau Online Kindermisbruik (EOKM) (Pays-Bas)[28] et Point de Contact (France)[29].

2.1.2 Vision par ordinateur

Deux exemples de cette technique sont examinés dans cette catégorie : les descripteurs globaux et les descripteurs locaux.

Descripteurs globaux

La technologie des descripteurs globaux repose sur un processus dans lequel l'image est transformée en un quadrillage dont chaque carré est traduit en une signature. Elle compare les images identiques

[25] https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.1
[26] https://en.wikipedia.org/wiki/MD5#Collision_vulnerabilities et https://en.wikipedia.org/wiki/SHA-1
[27] https://www.iwf.org.uk/
[28] https://www.eokm.nl/
[29] https://www.pointdecontact.net/

et peut détecter une similitude même s'il y a eu un léger recadrage (jusqu'à 20 %). Cette technologie ne reconnaît toutefois pas les images si elles ont été considérablement modifiées : orientation modifiée, retournement, étirement, gros plan, recadrage supérieur à 20 %, insertion d'une autre photo ou d'une vidéo, etc. Les algorithmes les plus fréquemment utilisés sont : PhotoDNA (Microsoft),[30] pHash (source ouverte)[31] et TMK PDQF (Facebook).[32] PhotoDNA est employé par certains numéros d'urgence, comme CyberTipline, par Cybertip, l'IWF ainsi que l'EOKM et ses partenaires.

Descripteurs locaux

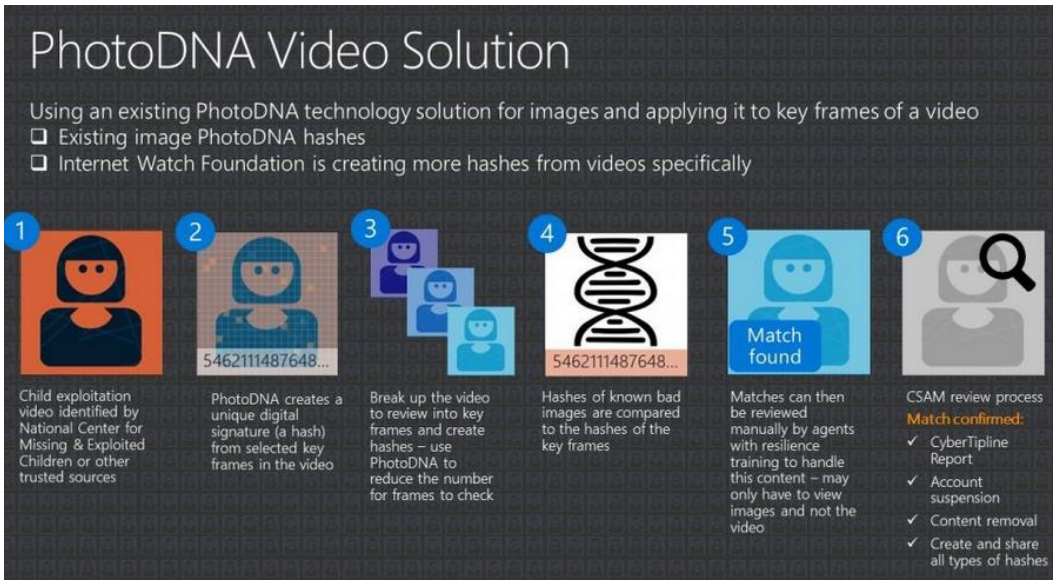
Cette technologie mesure le nombre de détails que partagent deux images ou vidéos et identifie ceux qui sont très similaires. Elle reconnaît les images même si elles ont été considérablement modifiées : orientation modifiée, retournement, étirement, gros plan, recadrage supérieur à 20 %, insertion d'une autre photo ou d'une vidéo, etc. Il est en outre possible de rechercher une correspondance exacte ou partielle, et, en option, de reconnaître le contenu d'une image ou d'une vidéo : bâtiments, pièces, objets identiques, image similaire incrustée dans une autre image ou vidéo. La limite de cette technologie, si l'on peut dire, est de reposer sur un algorithme très riche, susceptible d'être complexe à utiliser à grande échelle. L'algorithme le plus fréquent est SIFT (domaine public), employé par la technologie Videntifier[33] (breveté). Se servent notamment de cette technologie : INTERPOL,[34] Facebook (pour les droits d'auteur) et certains services de signalement, comme CyberTipline (pour les vidéos), ou Point de Contact.

Détection de vidéos

Les principes décrits ci-dessus (hachage de fichiers, vision par ordinateur à l'aide de descripteurs globaux / descripteurs locaux) permettent aussi d'identifier des vidéos, la principale différence entre l'identification d'images et de vidéos étant toutefois que cette dernière technologie fait appel à d'énormes ressources informatiques. Si l'algorithme et le système de la base de données ne sont pas conçus pour une efficacité maximale, la technologie de détection pourra fonctionner à petite échelle mais pas traiter d'importants volumes.

L'organigramme ci-après décrit la solution vidéo PhotoDNA de Microsoft, qui repose sur des descripteurs globaux[35].

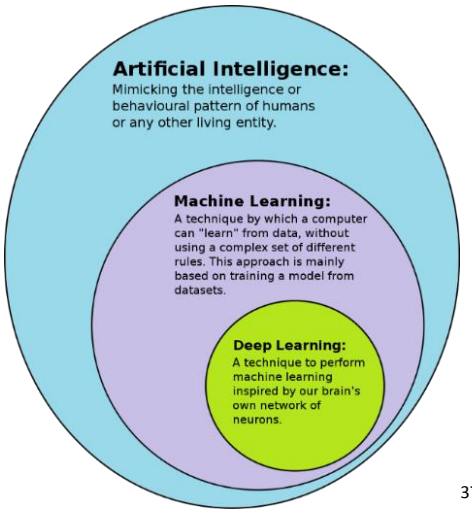
[30] https://www.youtube.com/watch?v=NORlSXfcWlo
[31] https://www.phash.org/
[32] https://about.fb.com/news/2019/08/open-source-photo-video-matching/
[33] http://www.videntifier.com/
[34] Organisation internationale de police criminelle (INTERPOL) Dirigée par son Secrétaire Général, INTERPOL dispose d'un personnel composé de policiers et de civils, d'un siège à Lyon, d'un complexe mondial pour l'innovation, à Singapour, et de plusieurs bureaux satellites dans diverses régions.
[35] https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/



2.1.3 Intelligence artificielle

La troisième technologie, et à ce jour la moins utilisée mais aussi la plus prometteuse dans la lutte contre l'exploitation et les abus sexuels d'enfants en ligne, est l'intelligence artificielle (IA). Mise au point dans les années 1950, cette technologie a évolué dans les années 1980 vers l'apprentissage automatique, où les algorithmes peuvent être « *entraînés* » à partir de jeux de données. Depuis les années 2010, elle a évolué vers un autre sous-domaine : l'apprentissage en profondeur[36].

Le schéma ci-dessous offre un aperçu simplifié des trois familles d'IA.



37

Comme l'IA imite le fonctionnement du cerveau humain, elle pourrait permettre à des ordinateurs de détecter de façon autonome des cas d'exploitation et d'abus sexuels d'enfants en ligne puis de les signaler aux autorités compétentes. Toutefois, la réglementation de l'utilisation de l'IA est un vaste domaine de recherche, complexe, qui fait appel à des mécanismes différents de ceux qui servent à

[36] https://master-iesc-angers.com/artificial-intelligence-machine-learning-and-deep-learning-same-context-different-concepts/
[37] https://en.wikipedia.org/wiki/Deep_learning#Deep_learning_revolution

contrôler la technologie de vision par ordinateur[38]. Deux éléments devraient entrer en ligne de compte :

- *La qualité du jeu de données* – L'origine du jeu de données, à savoir la façon dont il a été créé : est-ce qu'il concerne des conversations publiques ou privées, quelles organisations ont pris part à sa création, le secteur privé ou les forces de l'ordre en ont-ils rassemblé les éléments et gèrent-ils ce jeu de données ?
- *Les caractéristiques du jeu de données* – Contient-il uniquement des conversations textuelles ou aussi des métadonnées, par exemple la durée et la fréquence des communications, quelle langue a été choisie pour le jeu de données, contient-il d'autres informations contextuelles, par exemple la date de création d'un compte, l'activité d'un compte d'utilisateur, le recours à un VPN pour créer un compte ?

2.1.4 Enseignements aux fins du présent rapport

L'un des grands problèmes consiste à déterminer quels sont les moyens les moins restrictifs permettant de détecter les cas d'exploitation et d'abus sexuels d'enfants en ligne tout en protégeant dûment les victimes. Pour y répondre, il faut comprendre très précisément l'objectif recherché et l'environnement pour lequel telle ou telle technologie sera sélectionnée.

Les éléments ci-après pourraient permettre d'orienter ce processus :

- *La complexité de l'objectif* – Détecter une image identique connue est moins complexe que rechercher des images similaires. Détecter des images similaires associées à une image connue, montrant par exemple la même scène de crime, est moins complexe que de détecter une même personne. Plus l'objectif est complexe, plus la technologie à employer le sera aussi.
- *Complexité de la technologie* – Il est possible d'employer des technologies complexes pour atteindre des objectifs simples et d'employer par exemple la technologie de l'apprentissage en profondeur pour rechercher des images identiques alors que des solutions moins complexes conviendraient aussi.
- *Maturité de la technologie* – S'agissant de définir des garanties, il est plus sûr, pour les décideurs, d'opter pour une technologie bien éprouvée, bien documentée et stable. Il est en effet plus difficile de définir un niveau approprié de garanties lorsque d'une technologie en est aux premiers stades de son développement.
- *Complexité de l'environnement* – Le contexte dans lequel la technologie est déployée importe vraiment car une même technologie pourrait ne pas être déployable avec les mêmes garanties. Tout dépend principalement de l'audience cible du service : s'agit-il d'enfants uniquement, de professionnels, du public au sens large, d'adultes uniquement ; la technologie est-elle déployée dans un environnement public ou privé ; à quel endroit sera-t-elle déployée et quel y est le cadre juridique applicable ?

[38] https://www.forbes.com/sites/cognitiveworld/2020/05/23/towards-a-more-transparent-ai/

2.2 *Exemples concrets de l'utilisation de technologies automatisées pour détecter des cas d'exploitation et d'abus sexuels d'enfants en ligne*

Comme déjà indiqué, la technologie sera choisie dans une large mesure en fonction de l'objectif recherché. La distinction entre les différentes formes connues d'exploitation et d'abus sexuels d'enfants en ligne est liée soit au contenu, par exemple du matériel d'abus sexuels sur des enfants, soit au comportement, le « grooming » (sollicitation d'enfants à des fins sexuelles) étant par exemple ciblé, soit au fait que la technologie soit utilisée de façon proactive (prévention) ou réactive (détection).

Le tableau ci-après résume et schématise la façon dont les solutions technologiques décrites plus haut sont applicables aux principales formes d'exploitation et d'abus sexuels d'enfants en ligne. Il en ressort que la gamme de solutions technologiques applicable à la prévention des principales formes d'exploitation et d'abus sexuels d'enfants en ligne est pratiquement la même que celle qui est applicable à la détection. Le choix d'une solution technologique doit être fondé sur un examen approfondi de la question de savoir laquelle – dans la gamme – est la plus efficace pour l'objectif recherché. C'est ainsi que la disponibilité en ligne de matériel d'abus sexuels sur des enfants, qui est l'une des formes d'exploitation et d'abus sexuels d'enfants en ligne, peut être détectée à l'aide des trois familles d'outils de détection automatique : le hachage de fichiers, la vision par ordinateur et l'intelligence artificielle. Toutefois, ces outils peuvent avoir un mode d'application sensiblement différent en fonction de l'objectif visé.

Forme d'exploitation et d'abus sexuels d'enfants en ligne	**Prévention**	**Détection**
Disponibilité en ligne de matériel d'abus sexuels sur des enfants	Hachage de fichiers Vision par ordinateur, par ex. PhotoDNA Intelligence artificielle	Hachage de fichiers Vision par ordinateur, par ex. PhotoDNA Intelligence artificielle
« Grooming » (mise en confiance) / Sollicitation d'enfants à des fins sexuelles	Hachage de fichiers Vision par ordinateur, par ex. PhotoDNA Intelligence artificielle, par ex. outils « anti-grooming » (texte, métadonnées, contenu visuel)	Hachage de fichiers Vision par ordinateur, par ex. PhotoDNA Intelligence artificielle, par ex. outils « anti-grooming » (texte, métadonnées, contenu visuel)
Images et/ou vidéos sexuellement suggestives ou explicites d'enfants produites, partagées et reçues par des enfants	Hachage de fichiers Vision par ordinateur, par ex. PhotoDNA Intelligence artificielle, par ex. outils « anti-grooming » (texte, métadonnées, contenu visuel)	Hachage de fichiers Vision par ordinateur, par ex. PhotoDNA Intelligence artificielle, par ex. outils « anti-grooming » (texte, métadonnées, contenu visuel)
Contrainte et extorsion sexuelles	Hachage de fichiers Vision par ordinateur, par ex. PhotoDNA	Hachage de fichiers Vision par ordinateur, par ex. PhotoDNA

	Intelligence artificielle, par ex. outils « anti-grooming » (texte, métadonnées, contenu visuel)	Intelligence artificielle, par ex. outils « anti-grooming » (texte, métadonnées, contenu visuel)
Abus d'enfants en direct et à distance	La vision par ordinateur (avec descripteurs locaux) est susceptible d'aider à identifier une scène de crime (pièce ou bâtiment connus) Intelligence artificielle (texte, métadonnées, contenu visuel)	Hachage de fichiers La vision par ordinateur (avec descripteurs locaux) est susceptible d'aider à identifier une scène de crime (pièce ou bâtiment connus) Intelligence artificielle (texte, métadonnées, contenu visuel)

2.2.1 Activités axées sur le contenu

International Association of Internet Hotlines (INHOPE)

Les activités de l'International Association of Internet Hotlines (INHOPE), qui a été créée en 1999, offre un bon exemple d'utilisation des technologies de hachage de fichiers et de vision par ordinateur. INHOPE, qui réunit à l'heure actuelle 47 services de signalement dans le monde entier, est présente dans 43 pays. Chacun de ces services permet aux internautes de signaler en ligne, anonymement, du contenu qu'ils soupçonnent d'être illégal et tout particulièrement du matériel d'abus sexuels sur des enfants[39].

Afin de collecter, d'échanger et de classer les signalements de matériel d'abus sexuels sur des enfants, les services de signalement utilisent une plateforme sécurisée appelée ICCAM (en anglais, « *I see Child Abuse Material* » : je vois du matériel d'abus sur des enfants)[40], qui facilite en outre les technologies de hachage de fichiers d'images/de vidéo, d'empreinte numérique et d'indexation. Lorsqu'un service reçoit un signalement public, un analyste examine le matériel en question et s'il est établi que la page indiquée contient du matériel illégal, l'URL (Uniform Resource Locator)[41] est inscrite sur l'ICCAM, dont la principale caractéristique est l'automatisation. Le système qui indexe ensuite toutes les informations trouvées sur cet URL attribue une valeur de hachage à chacune des images/vidéos et il localise l'hébergeur. La valeur de hachage est comparée aux listes de valeurs de hachage des matériels d'abus sexuels sur des enfants répertoriés dans Baseline (liste de matériels illégaux à l'échelon international

[39] La description de cette procédure est tirée du rapport INHOPE 2020, (consultable à l'adresse : https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf).

[40] La plateforme ICCAM a été développée par INHOPE et Ziuz Forensics avec un financement de la Commission européenne dans le cadre des programmes Safer Internet et Connecting Europe Facility. Elle permet de mettre en place une collaboration multipartite entre les services de signalement, les forces de l'ordre (notamment INTERPOL) et le secteur privé.

[41] L'URL est une référence qui permet d'identifier une ressource du web par son emplacement et de préciser le protocole internet pour la récupérer. Voici ce à quoi peut ressembler une URL classique : http://www.example.com/index.html.

selon les critères d'INTERPOL)[42], et aux listes nationales (selon la législation nationale applicable dans le pays receveur et le pays hôte) pour que les matériels inédits ou déjà répertoriés puissent être repérés. Si le contenu est inédit (non trouvé dans une liste de valeurs de hachage), l'analyste peut alors classer chaque image/vidéo indexée séparément : dans Baseline, dans les bases nationales concernées de contenu illégal, ou en tant que contenu non illégal.

L'organigramme ci-après décrit la façon dont se déroule habituellement la suppression des matériels d'abus sexuels sur des enfants.

[42] Le système Baseline permet aux partenaires des secteurs public et privé de reconnaître, de signaler et de supprimer de leur réseau du matériel d'abus sexuels sur des enfants. Pour ce faire, ils doivent comparer les images et vidéos en question avec celles qui sont répertoriées dans la liste Baseline d'INTERPOL, qui contient la « *signature numérique* » de certaines des pires images et vidéos représentant des abus sexuels sur des enfants. Pour être incluses dans cette liste Baseline, les images et vidéos représentant des abus sexuels sur des enfants doivent être identifiées comme telles par un réseau d'enquêteurs spécialisés et remplir des critères précis en termes de gravité du contenu, par exemple la mise en scène d'enfants âgés de 13 ans ou moins. Ces critères stricts permettent de garantir que la liste Baseline répertorie uniquement les images et vidéos considérées comme illégales dans tout pays. Pour en savoir plus, voir : https://www.interpol.int/fr/Infractions/Pedocriminalite/Blocage-et-classement-de-contenu.

Ce processus automatique réduit la quantité de matériels d'abus sexuels sur des enfants auxquels les analystes sont exposés et il évite la duplication du travail. En 2020, par exemple, les signalements reçus par CyberTipline, un service de signalement aux États-Unis, comprenaient notamment 33,6 millions d'images, dont 10,4 millions inédites (détectées avec la vision par ordinateur sur base de descripteurs globaux), et 31,6 millions de vidéos, dont 3,7 millions inédites (détectées avec la vision par ordinateur sur base de descripteurs locaux)[43]. Selon le réseau INHOPE, 60 % de toutes les URL vérifiées en 2020 contenaient du matériel déjà analysé, ce qui signifie que le même contenu est diffusé et signalé à maintes reprises[44].

[43] https://www.missingkids.org/gethelpnow/cybertipline
[44] Rapport INHOPE 2020, p. 28.

La plupart du temps, le service qui reçoit le signalement informe les services répressifs locaux, il notifie le fournisseur d'hébergement et lui envoie une injonction de suppression[45] si le matériel est illégal. Toutes les images et les vidéos qui sont estampillées illégales à l'échelon international et à l'échelon national sont mises à la disposition d'INTERPOL via un portail ICCAM spécifiquement conçu à cet effet. INTERPOL télécharge alors ce matériel et le transfère dans sa base de données internationale sur l'exploitation sexuelle des enfants (ICSE)[46].

L'une des caractéristiques majeures des processus décrits ci-dessus est le niveau de connaissance des analystes des services de signalement, qui évaluent l'illégalité du contenu faisant l'objet d'un signalement, puis décident s'il faut ajouter le signalement à la plateforme ICCAM et – si le contenu est inédit (absent des listes de hachage) – ils classent l'image/la vidéo indexée dans Baseline, dans les bases nationales concernées ou en tant que contenu non illégal. Il s'agit d'une lourde responsabilité car si du contenu incorrectement classé sert de référence lors de futures vérifications, il peut renvoyer des faux positifs. Certains des services de signalement membres d'INHOPE, par exemple l'IWF, emploient une méthode de vérification dite des « *trois paires d'yeux* » : trois analystes dûment formés examinent et évaluent chaque image avant d'inclure son hachage dans la liste[47].

Rôle spécifique du National Center for Missing & Exploited Children (NCMEC, États-Unis)

La loi fédérale des États-Unis impose aux fournisseurs de services basés dans le pays de signaler à CyberTipline, le service de signalement du NCMEC, tout matériel apparent d'abus sexuels sur des enfants qu'ils découvrent dans leurs systèmes[48]. À ce jour, plus de 1 400 entreprises sont inscrites en tant que contributrices à CyberTipline[49] ; leurs signalements sont indispensables pour aider à soustraire des enfants à des situations dangereuses et empêcher une nouvelle victimisation.

En 2020, CyberTipline a reçu plus de 21,7 millions de signalements, soit 28 % de plus qu'en 2019 (où il y en avait eu 16,9 millions). Alors que la majorité (21,4 millions) des signalements provenait de fournisseurs de services électroniques (FSE), 303 299 émanaient du public, soit deux fois plus qu'en 2019 (où il y en avait eu 150 667)[50]. NCMEC estime que la hausse du nombre de signalements peut

[45] La procédure de notification et d'injonction de suppression (décrite dans le rapport d'INHOPE de 2020) vise à demander à un fournisseur d'hébergement ou à un moteur de recherche de retirer immédiatement ou de désactiver l'accès aux informations illégales, non pertinentes ou dépassées qu'ils hébergent sur leurs services. Les services de signalement d'INHOPE envoient des notifications et des injonctions de suppression aux fournisseurs d'hébergement lorsque quelqu'un leur envoie une URL contenant des images et des vidéos illégales, montrant des enfants victimes d'exploitation et abus sexuels.

[46] La base de données internationale sur l'exploitation sexuelle des enfants (ICSE) est un outil de renseignement et d'enquête avec lequel les enquêteurs spécialisés de plus de 60 pays peuvent échanger des informations sur des affaires d'abus pédosexuels. Cette base de données limite la duplication des initiatives et fait gagner un temps précieux aux enquêteurs qui peuvent savoir si certaines images ont déjà été découvertes ou identifiées dans un autre pays, ou si elles présentent des caractéristiques similaires à d'autres images. Forte de plus de 2,7 millions d'images et de vidéos, elle a permis d'identifier 23 500 victimes dans le monde. Pour en savoir plus, voir : https://www.interpol.int/fr/Infractions/Pedocriminalite/Base-de-donnees-internationale-sur-l-exploitation-sexuelle-des-enfants.

[47] https://annualreport2020.iwf.org.uk/tech/keyservices/hash

[48] 18 U.S.C. § 2258A

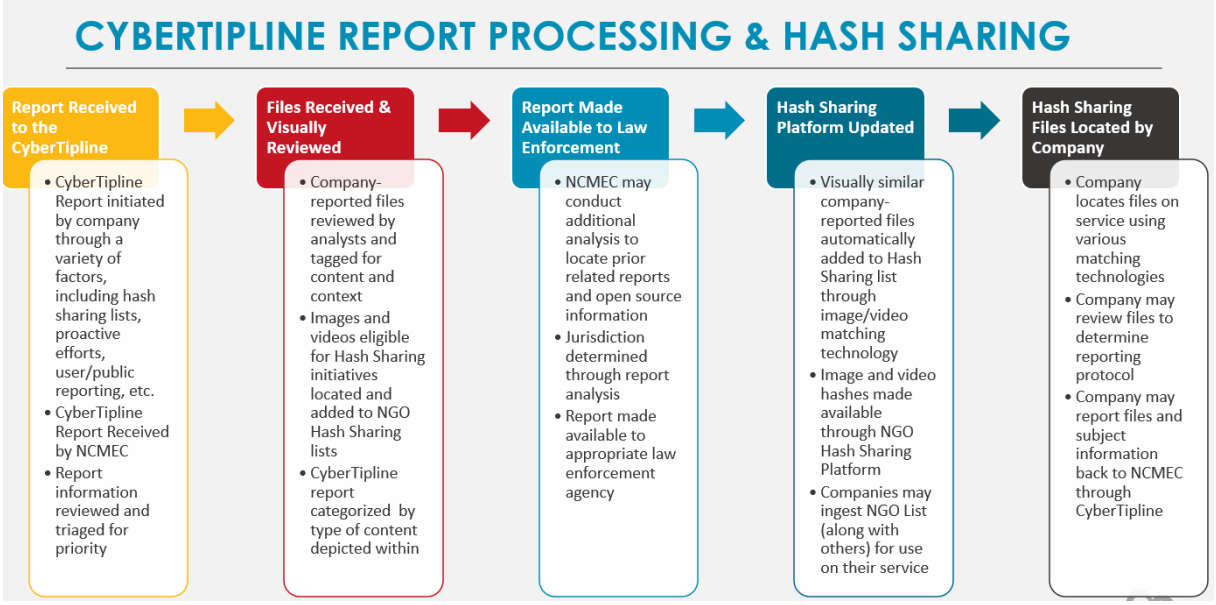
[49] https://www.missingkids.org/theissues/csam#bythenumbers

[50] https://www.missingkids.org/gethelpnow/cybertipline

indiquer plusieurs choses, dont l'augmentation du nombre d'utilisateurs sur une plateforme ou le degré de détermination d'un FSE à détecter et supprimer tout contenu illicite[51].

Plus de 30 sociétés ont accès à la plateforme du NCMEC, qui contient actuellement plus de 7,1 millions de hachages de matériels d'abus sexuels sur des enfants. L'IWF[52] et le Centre canadien pour la protection de l'enfance fournissent également (via la plateforme de hachages du NCMEC) une liste de hachages aux entreprises basées aux États-Unis. À titre d'exemple, la liste de hachages du NCMEC contient à elle seule 3,5 millions d'images et 385 000 vidéos. En outre, les entreprises elles-mêmes créent des listes de hachage de matériels d'abus sexuels sur des enfants et les partagent les unes avec les autres (via une plateforme que le NCMEC met à leur disposition), ce qui signifie que du matériel d'abus sexuels sur des enfants est souvent détecté et retiré avant que le public ou les services de signalement en aient découvert l'existence. Le NCMEC n'utilise alors pas la plateforme ICCAM car le contenu a déjà été supprimé d'internet.

L'organigramme ci-après décrit la façon dont CyberTipline traite habituellement les signalements et partage les hachages.



Service de vérification des hachages – Expertisebureau Online Kindermisbruik (EOKM, Pays-Bas)

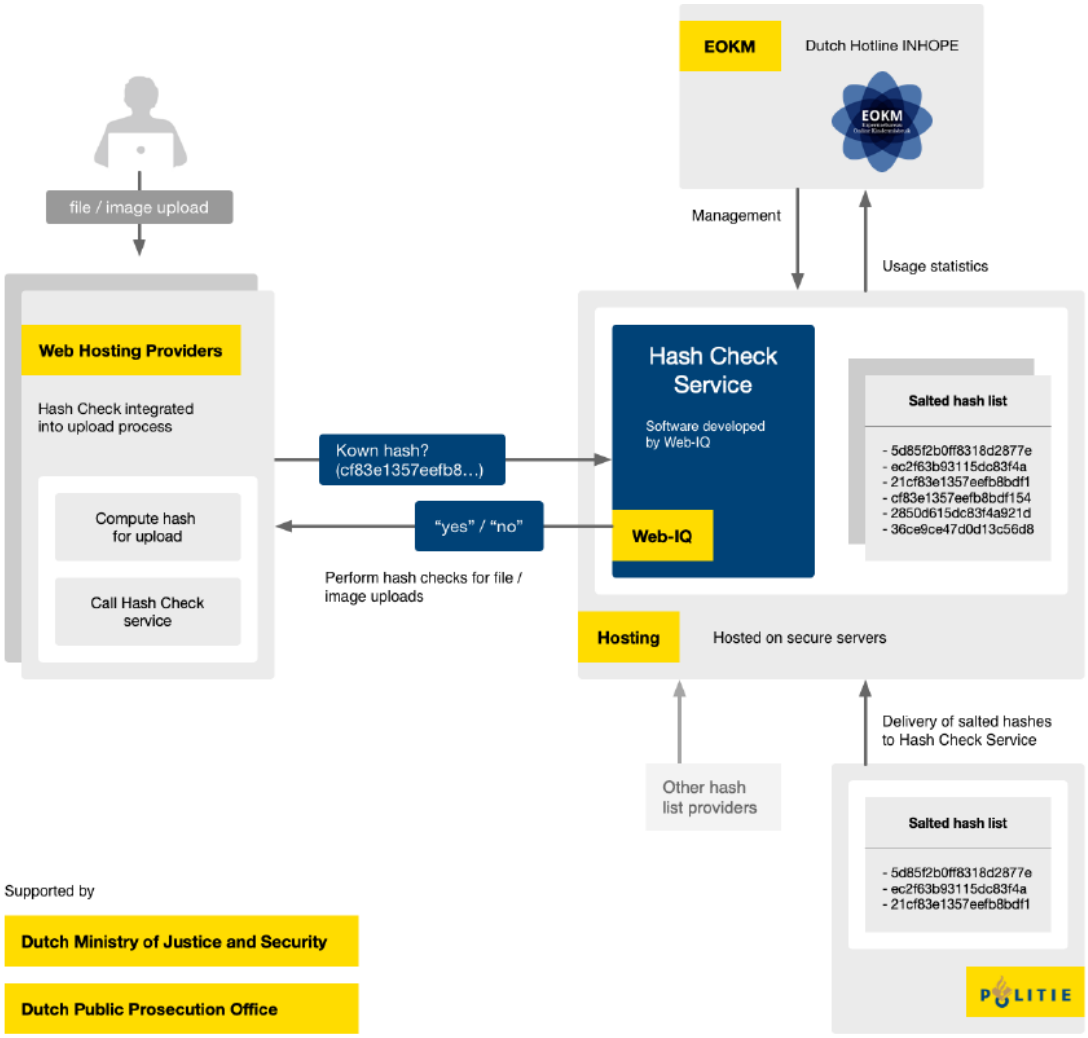
Le service de signalement néerlandais EOKM offre un autre exemple d'utilisation des technologies dont traite ce rapport. Depuis 2019, EOKM propose un service de vérification des hachages : il s'agit d'un outil qui comprend une base de données de plusieurs millions de hachages d'images d'exploitation sexuelle d'enfants. Via une interface de programme d'application, les utilisateurs peuvent vérifier si des images figurent dans la base de données. En 2020, le service de vérification des hachages a traité 18,2 milliards d'images, pour lesquelles il y a eu 7,4 millions de correspondances[53], ce qui a permis aux fournisseurs d'hébergement de supprimer les images de leurs serveurs.

[51] https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf
[52] https://www.iwf.org.uk/our-services/hash-list
[53] EOKM rapport 2020, p. 10, (consultable à l'adresse :

Selon EOKM, les chiffres sont élevés car de nombreux utilisateurs ont dès le départ vérifié tout leur matériel d'un coup pour voir s'il contenait des images illicites. La quantité d'images vérifiées devrait donc baisser à l'avenir. Toutefois, comme de nouveaux utilisateurs continuent de s'inscrire sur le service de vérification des hachages, il est difficile de faire des prévisions précises à ce stade[54].

Courant 2021, EOKM lancera deux nouveaux projets : le premier vise à en savoir plus sur le nombre de résultats positifs obtenus. Comme il s'agit de hachages et non réellement d'images, il n'est pour l'instant pas possible d'analyser suffisamment le type d'images trouvées : des données plus précises permettront donc d'obtenir de meilleures réponses. Le second est un projet pilote en collaboration avec Web-IQ[55] visant à analyser en quoi l'effet du serveur de vérification des hachages est différent pour les parties inscrites et pour celles qui ne le sont pas.

L'organigramme ci-après décrit le fonctionnement du service de vérification des hachages :



https://www.eokm.nl/wp-content/uploads/2021/04/EOKM-Jaarveslag-2020-DEF-ENG.pdf).

[54] Ibid.

[55] https://web-iq.com/

Internet Watch Foundation (IWF, R.-U.)

L'IWF a adopté une autre approche en matière d'utilisation de la technologie en question : au lieu d'offrir un service de vérification de hachages, elle partage sa liste de hachages avec ses membres dans le cadre d'une licence. Pour plus de facilité, chaque hachage est évalué au regard des normes internationales afin que les entreprises technologiques aient confiance dans les données qui leur sont fournies. L'IWF a mis au point une méthode efficace d'évaluation et de hachage de millions d'images d'abus sexuels sur des enfants : un outil d'évaluation d'images qui identifie les hachages et images multiples et les déduplique. Cela signifie qu'il peut en outre repérer les hachages ou les images d'autres organisations et les dédupliquer automatiquement avec ceux qui figurent déjà dans le système. Cette solution permet d'économiser du temps et de l'argent, et de protéger le bien-être de personnes qui auraient sinon dû voir ces images[56].

Exemples d'innovations

Ces dernières années, les services de signalement ont redoublé d'efforts et mené des recherches proactives lorsque la législation nationale les y autorisait. Il faut toutefois noter que les signalements par le public amènent surtout à découvrir du matériel inédit, tandis que ces recherches proactives visent surtout à aider à retirer du matériel déjà connu qui réapparaît sur internet[57].

Au sein du réseau d'INHOPE, seule l'IWF s'est investie dans la recherche proactive de matériels d'abus sexuels sur des enfants en ligne en 2020[58]. Cette tâche a été rendue possible par la création d'un robot d'indexation intelligent[59], contenant plus de 566 000 hachages d'images connues d'abus sexuels sur des enfants, qui a été déployé pour consulter méthodiquement des zones cibles sur internet. Ce robot d'indexation est utilisé à des fins tactiques dans une suite d'outils conçus pour trouver et supprimer les matériels d'abus sexuels sur des enfants et en perturber l'offre. Outre la création de signalements proactifs à l'intention des analystes de l'IWF, il sert aussi à vérifier les domaines d'un nombre croissant de Membres qui se sont engagés à prendre des mesures préventives pour empêcher leurs services d'être utilisés à des fins abusives. Il ressort des statistiques que les recherches proactives permettent d'identifier un bien plus grand nombre de matériels d'abus sexuels sur des enfants. En 2020, elles ont permis d'indexer 42 millions de pages web et plus d'un demi-milliard d'images. Les recherches proactives ont débouché sur 154 311 signalements, soit 52 % du nombre total de signalements reçus par IWF[60].

Autre exemple d'innovation dans le domaine considéré : le projet Arachnid[61], mené depuis 2016 par le Centre canadien. La plateforme détermine la présence de matériels d'abus sexuels sur des enfants dans une adresse URL en comparant les images qui s'y trouvent avec une banque de signatures

---

[56] Rapport IWF 2020, (consultable à l'adresse : https://annualreport2020.iwf.org.uk/tech/keyservices/hash).
[57] « *Study on framework of best practices to tackle child sexual abuse material online* », réalisée pour la Commission européenne par ICF S.A, Wavestone et Grimaldi Studio Legale, p. 5, (consultable à l'adresse : https://www.researchgate.net/publication/343813142_Study_on_Framework_of_best_practices_to_tackle_child_sexual_abuse_material_online_EXECUTIVE_SUMMARY_English).
[58] Rapport INHOPE 2020, p. 33.
[59] https://annualreport2020.iwf.org.uk/tech/new/crawlers
[60] Ibid.
[61] https://projectarachnid.ca/fr/#de-quoi-agit-il et https://www.protectchildren.ca/fr/zone-medias/communiques/2021/projet-arachnid-accessibilite-images-abus-pedosexuels

connues et déjà identifiées par des analystes comme constituant du matériel d'abus sexuels sur des enfants. Lorsque des matériels d'abus sexuels sur des enfants sont détectés, une demande de retrait est envoyée à l'hébergeur. Le projet Arachnid, qui traite des dizaines de milliers d'images par seconde, détecte du contenu à une vitesse largement supérieure à celle des méthodes traditionnelles permettant de détecter et de traiter ces matériels préjudiciables.

Le projet Arachnid détecte à l'heure actuelle plus de 100 000 images uniques par mois, qui doivent être vérifiées par un analyste et dont le nombre augmente tous les mois. Les conclusions du projet sont donc évidentes. Au 1er juin 2021, plus de 127 milliards d'images avaient été traitées, dont 39 millions retenues pour être soumises à un analyste, plus de 7,5 millions de demandes de retrait avaient été envoyées à des fournisseurs, dont 85 % au sujet de victimes inconnues des services de police[62]. Avec un tel nombre d'images retenues pour examen par un analyste, une collaboration avec des services de signalement du monde entier s'avérait nécessaire. En 2017, le Centre canadien a créé Arachnid Orb, un appareil grâce auquel les services de signalement d'autres pays peuvent collaborer dans le cadre du projet Arachnid. Arachnid Orb permet aux analystes du monde entier de mettre leurs compétences en commun afin de réduire les doubles emplois et d'en venir, à terme, à augmenter le nombre de demandes de retrait susceptibles d'être envoyées par l'entremise du projet Arachnid. À mesure que le nombre d'empreintes numériques vérifiées augmentera, le projet Arachnid deviendra de plus en plus efficace pour détecter les matériels d'abus sexuels sur des enfants et pour intervenir rapidement auprès des fournisseurs afin de leur demander de retirer ces photos et/ou ces vidéos nocives.

Au départ, la plateforme a été conçue pour explorer les liens trouvés sur des sites où la présence de matériels d'abus sexuels sur des enfants avait déjà été signalée à Cyberaide.ca, et pour détecter à quels endroits ces images et/ou vidéos étaient mises à la disposition du public. À l'heure actuelle, les activités d'exploration du projet Arachnid se poursuivent, mais celui-ci ne cesse d'évoluer et de s'adapter pour améliorer les capacités de lutte contre les matériels d'abus sexuels sur des enfants. Par exemple, « Shield » a été mis à la disposition des FSE dans le cadre du projet Arachnid pour améliorer et accélérer la détection de ces matériels préjudiciables, et pour en faciliter le retrait rapide.

Enfin, au sujet des initiatives en matière de partage des données de hachage, il convient de noter que la DG CONNECT a récemment attribué un marché (CNET/LUX/2020/OP/0059)[63] pour un projet dont le but est de faciliter l'élimination rapide des matériels en ligne d'abus sexuels sur des enfants. La solution de validation de principe, qui sera mise au point par les services de PwC UE[64] en coopération avec l'EOKM, European Service Network (ESN) et Web-IQ, devrait faciliter le retrait volontaire et rapide du matériel d'abus sexuels sur des enfants en améliorant l'interopérabilité, l'interconnectivité et la qualité des jeux de données. Précisément, elle contribuera à l'identification proactive de supports hébergés qui correspondent à du matériel connu d'abus sexuels sur des enfants. L'outil offre en outre la possibilité, moins invasive pour le secteur privé, de filtrer le matériel inacceptable à la source en l'analysant préventivement, au moment du téléchargement. Cela permet de mettre en place une base harmonisée et globale à partir de laquelle tous les acteurs concernés pourront recueillir, partager et utiliser les précieuses bases de données de hachage répertoriant tout le matériel connu d'abus sexuels

[62] Ibid.
[63] https://etendering.ted.europa.eu/cft/cft-display.html?cftId=6634&locale=fr
[64] https://www.pwc.com/gx/en/services/european-union.html

sur des enfants. Cette initiative vise en outre à renforcer la transparence des mesures de lutte contre l'offre en ligne de matériel d'abus sexuels sur des enfants.

Un dernier exemple d'innovation concerne l'utilisation, par l'IWF, de l'IA pour renforcer les capacités des analystes en créant un classificateur qui les aide à trier les images[65]. Cette technologie utilise l'apprentissage automatique pour indiquer quels signalements sont les plus susceptibles de contenir du matériel d'abus sexuels sur des enfants et lesquels pourraient ne pas en contenir. Cela permet aux analystes de classer leurs tâches par ordre de priorité et de se concentrer sur les signalements d'images montrant de très jeunes enfants victimes d'abus sexuels. Il faut toutefois souligner qu'en termes d'identification de victimes, il est indispensable que le contenu soit soumis à l'évaluation et au jugement d'humains, l'IA n'étant pas arrivée au stade où elle peut procéder à des distinctions granulaires[66]. Des projets similaires sont actuellement entrepris par d'autres acteurs, par ex. le projet APAKT, qui est mené par un service de signalement polonais : Dyżurnet.pl[67].

2.2.2 Activités axées sur le comportement

Outil « anti-grooming »

Pour réussir à lutter contre certaines des formes existantes d'exploitation et d'abus sexuels d'enfants en ligne, il faut faire appel à d'autres solutions technologiques et pas uniquement aux technologies axées sur le contenu qui sont décrites dans la section précédente. La technique récemment présentée de détection du « grooming », autrement dit de la sollicitation d'enfants à des fins sexuelles, fait appel à l'IA et cible les comportements, par exemple ceux qu'adoptent habituellement les prédateurs en ligne qui tentent d'attirer des enfants à des fins sexuelles. On peut déduire de la description officielle du fonctionnement de cette technique qu'elle n'utilise pas l'apprentissage en profondeur. Le jeu de données semble en effet trop réduit pour l'apprentissage en profondeur, qui requiert des milliards de données.

Le développement de cette technique/cet outil a démarré en novembre 2018 et depuis janvier 2020 c'est Thorn qui se charge de son adoption et des licences d'exploitation[68]. La technique peut être utilisée gratuitement par les entreprises technologiques proposant un service de messagerie instantanée qui cherchent à protéger les enfants face au risque de prédation en ligne sur leurs plateformes ; les forces de l'ordre et les organisations non gouvernementales (ONG) remplissant les conditions requises peuvent aussi s'en servir.[69] D'après le brevet de Microsoft pour la technologie de *« détection et de quantification du comportement des prédateurs sur les systèmes de communication », « la technique s'applique à l'historique des conversations par messagerie instantanée.* Elle évalue et « cote » les caractéristiques des conversations puis elle leur attribue un coefficient global de

[65] https://annualreport2020.iwf.org.uk/tech/new/classifiers et https://www.blog.google/around-the-globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online/
[66] Ibid.
[67] https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/4100,System-reagujacy-na-zagrozenia-bezpieczenstwa-dzieci-w-cyberprzestrzeni-ze-szcze.html?search=382648399
[68] Thorn : les défenseurs numériques des enfants, anciennement DNA Foundation, est une organisation internationale de lutte contre la traite des êtres humains qui combat l'exploitation sexuelle des enfants. Les principales activités de programmation de l'organisation sont axées sur la technologie internet et la façon dont elle facilite la pornographie enfantine et l'esclavage sexuel des enfants à l'échelle mondiale. L'organisation a été fondée par les acteurs américains Demi Moore et Ashton Kutcher.
[69] https://www.thorn.org/blog/what-is-project-artemis-thorn-microsoft-grooming/

probabilité. Celui-ci peut ensuite servir de déterminateur et être programmé par chacune des entreprises utilisatrices de la technique pour appeler l'attention de modérateurs humains sur une conversation. Les modérateurs humains sont ensuite en mesure de déceler des menaces imminentes et de les signaler aux forces de l'ordre ainsi que d'informer le NCMEC de tout cas de soupçon d'exploitation sexuelle d'enfants »[70].

Au moment de la rédaction du présent rapport, très peu d'informations avaient été publiées sur l'état du déploiement de cette technologie par le secteur privé et les forces de l'ordre. On sait que Microsoft utilise cette technique dans divers programmes de sa plateforme Xbox depuis plusieurs années et en étudie l'utilisation dans des services de messagerie instantanée, notamment Skype[71].

L'agent conversationnel reThink d'IWF

Dernier exemple de solutions technologiques ciblant les comportements en ligne : l'agent conversationnel interactif mis au point par l'IWF dans le cadre d'un projet sur deux ans financé par le fonds End Violence[72]. L'agent conversationnel vise à enrayer la demande de matériel en ligne d'abus sexuels sur des enfants en stoppant les personnes qui tentent d'avoir accès à ce type d'images et en les empêchant de commettre une infraction pénale. L'agent conversationnel reThink d'IWF interagira avec les utilisateurs d'internet qui semblent être à la recherche d'images d'abus sexuel d'enfants. Il tentera d'engager avec eux une conversation cordiale et positive puis, au moment opportun, les aiguillera vers l'aide et l'accompagnement dont ils ont besoin. Un pilote devrait être lancé fin 2021 et le projet devrait être entièrement opérationnel en 2022. Ce projet, dont on estime que le potentiel est énorme, contribuera à lutter de manière proactive contre l'exploitation et les abus sexuels d'enfants en ligne.

2.2.1 Enseignements aux fins du présent rapport

Les exemples concrets d'utilisation des technologies automatisées de détection de l'exploitation et des abus sexuels d'enfants en ligne permettent d'observer un élément important : la présence d'un décideur humain est une condition sine qua non du contrôle des solutions technologiques. L'intervention humaine reste primordiale à tous les niveaux, qu'il s'agisse de choisir les jeux de données qui serviront à entraîner les algorithmes ou de soumettre les contenus illicites qui font l'objet d'un signalement à des yeux humains pour analyse et décision.

Dans certains cas, comme dans celui du « grooming », avec le risque inhérent de prolifération sur toutes les plateformes offrant des services de messagerie instantanée, il est essentiel d'avoir recours aux technologies automatisées car elles sont actuellement les seules capables de contrôler d'énormes volumes de données et de porter secours à un enfant avant qu'il ne soit victime d'exploitation.

Si le fonctionnement de certaines entreprises du secteur privé suscite des inquiétudes à l'échelon mondial, il semblerait, selon divers spécialistes de la lutte contre l'exploitation et les abus sexuels d'enfants en ligne que celles-ci n'aient pas lieu d'être en ce qui concerne les mesures de hachage ou anti-grooming qui sont prises pour lutter contre ce phénomène. Dans leurs lettres aux députés du Parlement européen à propos de l'examen du projet de dérogation temporaire à certaines dispositions

[70] https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/
[71] Ibid.
[72] https://annualreport2020.iwf.org.uk/tech/new/chatbots

de la directive vie privée et communications électroniques, les représentants du NCMEC se sont exprimés comme suit : *« La technologie du hachage est utilisée dans la lutte contre l'exploitation et les abus sexuels d'enfants en ligne depuis près de 20 ans et, d'après l'expérience acquise, on peut affirmer que le hachage et les nouveaux indicateurs relatifs au « grooming » ne servent, lorsqu'ils sont utilisés dans la lutte contre ce phénomène, ni à suivre une activité en ligne sans rapport avec ce phénomène, ni à en établir le profil, et ils sont toujours associés à un certain niveau d'analyse humaine ou secondaire. La technologie de hachage qu'emploient des services pour détecter en ligne des abus sexuels d'enfants ne catalogue pas et ne comprend pas non plus les contenus qu'elle analyse : elle se contente de rechercher les images spécifiques d'abus sexuels d'enfants qu'elle a été entraînée à reconnaître. Tout autre contenu passe inaperçu : elle ne les reconnaît pas ni ne les catalogue. Les indicateurs anti-grooming fonctionnent de façon similaire à cette différence près que l'association de certains facteurs déclenche une alerte ».*

L'avis des spécialistes de la lutte contre l'exploitation et les abus sexuels d'enfants en ligne joue certes un rôle très important dans le discours public, mais une plus grande transparence dans l'utilisation des technologies de détection automatique améliorerait la mise au point des mécanismes de responsabilité. L'amélioration du niveau de transparence et de la responsabilité devrait passer avant tout par la cartographie des divers types d'applications existants et notamment par la description des rôles et responsabilités de tous les acteurs concernés.

3. CADRE JURIDIQUE

3.1 La directive vie privée et communications électroniques et le code des communications électroniques européen

Le contexte dans lequel se sont déroulés les débats au Parlement européen à propos du projet de dérogation temporaire à certaines dispositions de la directive vie privée et communications électroniques, évoqué au début de ce document, servira de point de départ à cette section consacrée à l'analyse du cadre légal applicable.

Le 10 septembre 2020, la Commission européenne a publié une « *Proposition concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des 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* »[73]. La Commission estimait qu'une telle dérogation était nécessaire car dès la mise en application du Code des communications électroniques européen (CCEE), à compter du 21 décembre 2020, les fournisseurs de certains services de communication en ligne, notamment de services de communications interpersonnelles non fondés sur la numérotation (par exemple téléphonie internet, messagerie instantanée et courrier électronique web), seraient alors couverts par la directive vie privée et communications électroniques[74].

[73] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020PC0568

[74] Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen. Journal officiel de l'Union européenne, L 321, 17/12/2018, (consultable à l'adresse : https://eur-lex.europa.eu/eli/dir/2018/1972/oj).

Le CCEE avait pour principale conséquence de modifier la situation juridique de certains services de communication en ligne. Avant son entrée en vigueur, ces services étaient couverts par la directive sur le commerce électronique, dont l'application est liée au pays d'origine, les fournisseurs de services établis dans un État membre étant libres d'offrir des services dans les autres États membres sans restriction[75]. Malgré certaines dérogations, notamment pour « *la prévention, les investigations, la détection et les poursuites en matière pénale, notamment la protection des mineurs* »[76], dans la plupart des États membres les textes permettant aux forces de l'ordre de solliciter des données auprès des fournisseurs de services étaient liés à leur statut de fournisseurs de « *services de communications électroniques* » et cette prérogative n'était donc généralement pas exercée à l'encontre des fournisseurs de communication en ligne[77]. Depuis l'entrée en vigueur du CCEE, ces fournisseurs de services sont désormais couverts par un régime réglementaire axé sur le principe du pays de destination, c'est-à-dire qu'ils sont soumis au droit de chacun des États membres dans lesquels ils proposent leurs services. De par cette évolution réglementaire, les fournisseurs de services de communication en ligne sont globalement couverts par les règles nationales de procédure pénale relatives à l'interception et aux données de communication ainsi qu'aux dispositions de la directive vie privée et communications électroniques, qui sont applicables aux fournisseurs de « *services de communications électroniques* ».

La proposition de dérogation temporaire était essentielle pour que les fournisseurs puissent continuer, après le 21 décembre 2020, de procéder volontairement à des activités impliquant l'utilisation de technologies automatisées pour détecter le matériel d'abus sexuels sur des enfants, le signaler et le retirer. La proposition était par ailleurs nécessaire pour que les États membres aient le temps d'adopter la législation sectorielle permettant de lutter plus efficacement contre l'exploitation et les abus sexuels d'enfants en ligne tout en respectant les droits fondamentaux, en particulier le droit au respect de la vie privée et la liberté d'expression.

Les enjeux inhérents à l'équilibre entre le respect de la vie privée et la protection des enfants qui sont évoqués dans la proposition de la Commission européenne, ont suscité un important débat entre plusieurs acteurs, notamment ceux qui sont très impliqués dans la lutte contre ce phénomène. Il convient de noter que des entreprises du secteur privé, par exemple Google, LinkedIn, Microsoft, Roblox et Yubo, se sont engagées publiquement à poursuivre leurs activités proactives de détection et de signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne pendant que l'UE examine la voie à suivre[78].

Trois avis sur ce point sont examinés ci-après : ceux du Contrôleur européen de la protection des données, de la commission des libertés civiles et du Comité économique et social européen.

[75] Directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), JO L 178 du 17/7/2000.
[76] Ibid., art. 3(4)(a)(i).
[77] I.e. *Google LLC c. Bundesrepublik Deutschland (C-193/18)* [2019] 1 W.L.R. 6044.
[78] https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

3.1.1 Contrôleur européen de la protection des données

Le Contrôleur européen de la protection des données (CEPD) a publié, le 10 novembre 2020, l'avis 7/2020 sur la proposition de la Commission européenne[79]. Il a indiqué ce qui suit : *« La confidentialité des communications est un élément essentiel des droits fondamentaux au respect de la vie privée et familiale »* et *« les mesures envisagées par la proposition constitueront une ingérence dans les droits au respect de la vie privée et à la protection des données des personnes concernées (utilisateurs, auteurs d'abus présumés et victimes) »*. Par ailleurs, le CEPD a estimé que *« l'analyse générale, indifférenciée et automatisée de toutes les communications textuelles transmises par l'intermédiaire de services de communications interpersonnelles non fondés sur la numérotation en vue de détecter de nouvelles infractions potentielles ne respecte pas les principes de nécessité et de proportionnalité. Même si la technologie utilisée se limite à l'utilisation d'« indicateurs clés », le CEPD estime que le déploiement d'une telle analyse générale et indifférenciée est excessif ».* Il fait en outre observer que *« l'analyse automatisée d'un discours ou d'un texte en vue d'identifier des cas potentiels de sollicitation d'enfants est susceptible de constituer une ingérence plus importante que la mise en correspondance d'images ou de vidéos sur la base de cas de pédopornographie précédemment confirmés ».*

En termes de nécessité et de proportionnalité, le CEPD a souligné qu'en « *l'absence d'une analyse d'impact accompagnant la proposition, la Commission n'a pas encore démontré que les mesures envisagées par cette proposition sont strictement nécessaires, efficaces et proportionnées pour atteindre l'objectif visé* ». Le CEPD a appelé la Commission, à fournir dans un premier temps, des informations supplémentaires pour permettre au co-législateur d'étudier si les mesures envisagées répondent effectivement aux exigences de nécessité, d'efficacité et de proportionnalité. Il a indiqué dans son avis qu'afin de pouvoir évaluer l'incidence d'une mesure sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, il était essentiel de déterminer précisément[80] :

- *la portée de la mesure*, y compris le nombre de personnes concernées et le risque éventuel d'« *intrusion collatérale* » (c'est-à-dire d'ingérence dans la vie privée de personnes autres que les personnes concernées par la mesure) ;
- *l'étendue de la mesure*, y compris la quantité d'informations collectées ; la durée de la collecte ; le besoin ou non, dans le cadre de la mesure examinée, de collecter et traiter des catégories particulières de données ;
- *le degré d'intrusion*, en s'interrogeant : sur la nature de l'activité sur laquelle porte la mesure (si elle affecte des activités soumises à une obligation de confidentialité telles que les relations entre un avocat et son client, les activités médicales) ; sur le contexte ; sur le fait qu'il puisse s'agir en réalité de profilage des individus concernés ; sur le fait que le traitement puisse supposer l'utilisation de systèmes de prise de décision automatisés (entièrement ou en partie) comportant un « *taux d'erreur* » ;
- si la mesure concerne des *personnes vulnérables* ou non ;

[79] Contrôleur européen de la protection des données, « *Avis 7/2020 sur la proposition de dérogations temporaires à la directive 2002/58/CE aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne* », (consultable à l'adresse : https://edps.europa.eu/system/files/2021-03/20-11-10_opinion_combatting_child_abuse_fr_3.pdf).
[80] Ibid.

- si la mesure porte également sur d'autres *droits fondamentaux.*

Le CEPD s'est en outre particulièrement inquiété du fait que la proposition n'expliquait pas le modèle de gouvernance des fournisseurs de services électroniques ayant recours à cette dérogation, et qu'elle ne précisait ni la manière dont ils effectueraient le signalement, ni à qui, ni qui serait chargé de la maintenance et de la mise à jour des bases de données pertinentes pour détecter les futurs cas d'exploitation et d'abus sexuels d'enfants en ligne. Le CEPD a par ailleurs recommandé que la validité de toute mesure transitoire ne dépasse pas deux ans.

3.1.2 Rapport de la commission des libertés civiles, de la justice et des affaires intérieures

La commission des libertés civiles, de la justice et des affaires intérieures (LIBE), du Parlement européen, a publié le 11 décembre 2020 un rapport sur la proposition de la Commission européenne[81]. Dans l'ensemble, la LIBE estime que « l*a proposition de règlement ne prévoit en soi aucune base juridique applicable au contrôle des communications par les fournisseurs. Au lieu de cela, elle prévoit une limitation de certains droits et obligations énoncés dans la directive 2002/58/CE et établit des garanties supplémentaires auxquelles doivent se conformer les fournisseurs s'ils souhaitent se fonder sur ce règlement* »[82].

La LIBE a par ailleurs précisé la portée des mesures et déclaré que la proposition de la Commission européenne « *ne devrait s'appliquer qu'aux vidéos ou images échangées via des services de messagerie et de courrier électronique ». En effet, [elle] ne devrait pas s'appliquer au contrôle des communications texte ou audio, qui reste entièrement soumis aux dispositions de la directive relative à la vie privée et aux communications électroniques ».* Compte tenu de son caractère temporaire, le champ d'application matériel du règlement devrait être limité à la définition établie de la « *pédopornographie* » dans la directive 2011/93/UE et du « *spectacle pornographique* » dans cette même directive (directive relative aux abus sexuels commis contre des enfants)[83].

La LIBE estime[84] qu'afin de garantir la proportionnalité de la limitation des droits fondamentaux, les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation désireux de se prévaloir de ce règlement devraient remplir certaines conditions :

- l'obligation de procéder à une analyse d'impact relative à la protection des données et à une consultation préalable, visées respectivement aux articles 35 et 36 du RGPD, avant de recourir à toute nouvelle technologie ;

---

[81] Parlement européen – Commission des libertés civiles, de la justice et des affaires intérieures (LIBE). *Rapport sur la proposition de règlement du Parlement européen et du Conseil concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des 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,* (COM(2020)0568 – C9-0288/2020 – 2020/0259(COD)), (consultable à l'adresse : https://www.europarl.europa.eu/doceo/document/A-9-2020-0258_FR.html).

[82] Comme indiqué au paragraphe a) de l'exposé des motifs.

[83] 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 (consultable à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32011L0093).

[84] Comme indiqué au paragraphe c) de l'exposé des motifs.

- utiliser l'article 6, paragraphe 1, point d) ou e), du RGPD comme base juridique ;
- une supervision et une intervention humaines sont garanties dans le cadre de tout traitement de données à caractère personnel et aucun résultat positif n'est transmis aux autorités répressives et aux organismes qui agissent dans l'intérêt public sans avoir été d'abord analysé par un humain ;
- des procédures et des mécanismes de recours appropriés sont en place ; aucune interférence dans les communications protégées par le secret professionnel ; une base juridique appropriée pour les transferts en dehors de l'UE conformément au chapitre V du RGPD ;
- recours effectifs mis en place par les États membres au niveau national.

En termes de délai, la LIBE estime que la période d'application du règlement de la Commission européenne devrait être limitée au 31 décembre 2022, et que si la future législation à long terme était adoptée et entrait en vigueur avant cette date, elle devrait entraîner l'abrogation dudit règlement.

3.1.3 Avis du Comité économique et social européen

Dans son avis publié le 11 janvier 2021, le Comité économique et social européen (CESE)[85] a souligné que, dans l'ensemble, il approuvait la proposition de règlement concernant une dérogation temporaire et strictement limitée à l'article 5, paragraphe 1, et à l'article 6 de la directive vie privée et communications électroniques. Il a déclaré que pour préserver la vie privée et protéger les données personnelles[86] :

- le traitement des données doit être proportionné et limité aux technologies bien établies régulièrement utilisées à cette fin par des services de communications interpersonnelles non fondés sur la numérotation avant l'entrée en vigueur du règlement,
- la technologie utilisée doit être conforme à l'état de la technique dans le secteur et être la moins intrusive possible dans la vie privée,
- la technologie utilisée doit être en elle-même suffisamment fiable, limiter autant que possible le taux d'erreurs et rectifier sans délai les erreurs occasionnelles qui pourraient survenir,
- la détection de la « *sollicitation d'enfants* » doit se limiter à l'utilisation d'« *indicateurs clés* »,
- le traitement se limite à ce qui est strictement nécessaire à cette fin, et les données sont effacées immédiatement, sauf si un abus sexuel contre des enfants en ligne a été détecté,
- le fournisseur a l'obligation de publier chaque année un rapport sur le traitement des données en question.

Le CESE n'était toutefois pas favorable à la durée d'application de la dérogation (jusqu'au 31 décembre 2025) et a déclaré que la Commission devrait veiller à ce que des garanties en matière de protection de la vie privée des enfants soient établies et mises en œuvre avant cinq ans.

---

[85] *Avis du Comité économique et social européen sur la proposition de règlement du Parlement européen et du Conseil concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des 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* (consultable à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020AE4192&rid=2).

[86] Ibid, paragraphe 2.5.

3.1.4 Enseignements aux fins du présent rapport

D'après les chiffres récemment publiés par le NCMEC, la situation examinée plus haut a eu des incidences sur le niveau de signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne. Le Centre a enregistré une baisse de 58 % des signalements de tels cas en provenance de l'UE depuis le 21 décembre 2020, date d'entrée en vigueur de la nouvelle réglementation[87].

Il est donc très important de noter que le 29 avril 2021, l'UE est parvenue à un accord provisoire sur la législation temporaire évoquée plus haut. Il a été convenu d'un certain nombre de garanties, et le processus d'adoption de la législation à long terme a démarré, la Commission européenne devant en rédiger un projet pour l'été 2021. Selon le communiqué de presse du Parlement européen[88], *« les modifications convenues prévoient une dérogation aux articles de la réglementation relative à la protection de la vie privée dans le secteur des communications électroniques qui portent sur la confidentialité des données relatives à la communication et au trafic, et elles permettent aux fournisseurs de services de courrier électronique web, de clavardage et de messagerie instantanée de détecter, de supprimer et de signaler volontairement les cas d'abus sexuel d'enfants en ligne ainsi que d'utiliser des technologies permettant de détecter la sollicitation d'enfants en ligne à des fins sexuelles. […] les négociateurs du Parlement se sont assurés que les autorités nationales chargées de la protection des données pourront exercer un contrôle renforcé des technologies utilisées, ils ont amélioré le mécanisme de plainte et les recours, et ils ont veillé à ce que les données traitées soient d'abord analysées par une personne avant de faire l'objet d'un signalement. Les fournisseurs de services devront par ailleurs améliorer les statistiques qu'ils communiquent. Cette législation temporaire devrait s'appliquer pendant maximum trois ans ou moins si de nouvelles règles, permanentes, sur la lutte contre les abus sexuels d'enfants en ligne devaient être approuvées dans l'intervalle* ».

Au moment de la rédaction du présent rapport, le texte définitif approuvé de la proposition de la Commission européenne n'avait pas encore été publié.

3.2 Comportement des fournisseurs de services

Cette section examine la nature juridique du fournisseur de services, les complexités juridictionnelles découlant de la fourniture de services transfrontaliers et la base légale concernant la surveillance et le signalement de la disponibilité en ligne de matériel d'abus sexuels sur des enfants.

3.2.1 La notion de « fournisseurs de services »

La Convention de Budapest définit la notion de « fournisseur de services » comme suit :

- toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

[87] https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

[88] Commission des libertés civiles, de la justice et des affaires intérieures. Communiqué de presse '*Provisional agreement on temporary rules to detect and remove online child abuse*', 30 avril 2021, (consultable, en anglais uniquement), à l'adresse : https://www.europarl.europa.eu/news/en/press-room/20210430IPR03213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse).

- toute *autre entité* traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs[89].

Cette définition était volontairement large pour s'appliquer non seulement aux fournisseurs classiques de services de télécommunication mais aussi à une large gamme de fournisseurs de services en ligne qui stockent du contenu pour leurs utilisateurs, par exemple les fournisseurs de médias sociaux[90]. La Convention de Budapest, qui va plus loin que le CCEE, pourrait s'appliquer à des entités qui fournissent ce qui s'appelle en droit de l'UE des « *services de la société de l'information* »[91] et des « *services de médias audiovisuels* »[92], à condition que soient proposés des « *services de communication ou d'autres services de traitement des données* »[93].

Il est par ailleurs important de noter que la définition du fournisseur de services qui est donnée à des fins réglementaires dans les textes nationaux relatifs à la fourniture de services n'est pas forcément alignée sur celle qui en est donnée en procédure pénale, laquelle peut être plus large que la définition réglementaire, comme c'est par exemple le cas au Royaume-Uni[94] et en Belgique[95].

3.2.2 Cadre juridique

Mettre en œuvre des systèmes de lutte contre l'exploitation et les abus sexuels d'enfants en ligne implique pour les fournisseurs de services deux activités principales : la détection (retrait compris) et le signalement. La détection implique le suivi et l'analyse des données des utilisateurs, habituellement rangées dans trois grandes catégories :

- *le contenu*, transmis ou au repos ;
- *les données relatives au trafic*, qui apportent des informations détaillées sur les activités de communication des utilisateurs[96] ;
- *les données relatives aux abonnés*, qui sont transmises au fournisseur de services lors de la création de la relation client[97].

[89] Article 1c.
[90] Rapport explicatif, paragraphe 27.
[91] Directive 2015/1535/UE prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, Journal officiel de l'Union européenne J L 241/1 du 17 septembre 2015 (consultable à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L:2015:241:FULL&from=RO).
[92] Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels ») (JO L 95/1 du 15 avril 2010, modifiée par la directive (UE) 2018/1808 (consultable à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32010L0013&lang1=FR&from=EN&lang3=choose&lang2=choose&_csrf=1606521a-f6c6-4bac-96d4-73d5aea78fe9).
[93] Rapport explicatif, paragraphe 27.
[94] Investigatory Powers Act 2016, s. 261(11) et (12). (consultable à l'adresse : https://www.legislation.gov.uk/ukpga/2016/25/section/261).
[95] Procureur-Generaal Bij Het Hof van Beroep te Gent c. Yahoo! Inc., Cour de cassation de Belgique, n° P.10.1347.N, 18 janvier 2011.
[96] Convention de Budapest, article 1d.
[97] Convention de Budapest, article 18, paragraphe 3.

La « *licéité* » du traitement des données est liée à des obligations négatives aussi bien qu'à des positives : négatives car le traitement ne doit violer aucune imposition légale comme la confidentialité et les interceptions illégales, et positives car un motif légal est requis conformément à la législation sur la protection des données[98]. La base légale sur laquelle repose le traitement peut en outre différer en fonction du type de données traitées[99].

Pour ce qui est du signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne, que ce soit auprès d'une autorité répressive publique ou d'un service de signalement autorisé, il peut correspondre grosso modo à l'un des quatre scénarios suivants :

1. *le signalement est volontaire* – un fournisseur de services peut effectuer un signalement sur base tout à fait volontaire. Il faudra généralement qu'il y soit autorisé par certaines des dispositions contractuelles régissant sa relation avec l'utilisateur. Toutefois, la validité de cette autorisation pourrait être contestée dans la mesure où le consentement de l'utilisateur à s'engager à respecter de telles conditions serait susceptible d'être invalidé en raison du statut de l'utilisateur (par exemple si c'est un enfant) ou de la façon dont le consentement a été obtenu, ou encore car la condition elle-même pourrait être déclarée contraire à des règles obligatoires ;
2. *le signalement volontaire est autorisé* – le signalement volontaire peut être autorisé par un cadre légal permettant expressément au fournisseur de services de divulguer les données concernées et précisant souvent dans quelles circonstances et conditions particulières il peut le faire tout en jouissant d'une immunité de responsabilité[100] ;
3. *le signalement est imposé par la loi* – un fournisseur de services peut signaler proactivement les cas qu'il détecte d'exploitation et d'abus sexuels d'enfants en ligne car la loi l'oblige à signaler un tel matériel et en cas de non-respect de cette obligation, sa responsabilité peut être engagée et il peut écoper d'une amende administrative ; il peut aussi être déclaré coresponsable (soit en qualité d'agent principal de l'infraction soit de complice)[101] ;
4. *le signalement est imposé par une autorité* – un fournisseur de services peut recevoir une demande de divulgation de données qui aura été autorisée par *un tribunal ou une autorité administrative indépendante*, dans le cadre d'une enquête sur une infraction pénale commise par un utilisateur.[102]

Pour ce qui est de faciliter le déploiement par les FSE de systèmes de détection automatique de l'exploitation et des abus sexuels d'enfants en ligne, ni le premier ni le quatrième scénario ne semblent fournir une base légale convenable. Dans le premier, la base légale relève avant tout du droit privé, ce qui pose d'importants risques aussi bien pour les intérêts des fournisseurs de services que pour les droits des utilisateurs. Le quatrième scénario est peut-être celui qui instaure le cadre juridique le plus solide mais le signalement est alors réactif, vu qu'il consiste à demander les données aux fournisseurs de services, ce qui est inadapté aux volumes de données concernés. Quant au troisième scénario, le fait que la divulgation des données soit un enjeu en termes de responsabilité du fournisseur de services

[98] RGPD, art. 6.
[99] Voir : directive vie privée et communications électroniques, art. 6 Données relatives au trafic.
[100] Voir : loi britannique de 2018 sur la protection des données, Sch. 2, Pt. 1, paragraphe 2.
[101] Voir : US (18 U.S.C. § 2258A) et droit italien.
[102] Tele2 Sverige AB c. Post-och Telestyrelsen [2017] 2 C.M.L.R 30. Voir aussi Szabó et Vissy c. Hongrie (2016) 63 E.H.R.R 3, paragraphe 77.

peut avoir des conséquences préoccupantes sur le comportement de celui-ci, qui risque alors de faire trop de signalements, avec toutes les répercussions négatives que cela pourrait avoir sur les utilisateurs, les services de signalement et les forces de l'ordre.

Si ces scénarios présentent les diverses possibilités à l'échelon national, les compétences juridictionnelles sont bien plus complexes dans un environnement transfrontière. Du point de vue du fournisseur de services, lorsqu'il est établi sur un territoire, le respect d'une obligation imposée sur un autre, sur lequel il offre des services, peut lui sembler « *volontaire* » ou du moins « *inopposable* »[103]. La réponse à la question de savoir s'il a raison ou pas, sur le fond ou sur la forme, peut exiger un règlement judiciaire, ce qu'aucune des parties ne pourrait souhaiter.

3.2.3 Proposition de règlement de l'UE relatif à la détection, à la suppression et au signalement des cas d'abus sexuels d'enfants en ligne

À propos du comportement des fournisseurs de services, il est très utile de présenter les scénarios que la Commission européenne a proposés dans l'initiative qu'elle a lancée pour définir les responsabilités de divers fournisseurs de services en ligne leur imposant de détecter les abus sexuels d'enfants en ligne ainsi que de signaler ce type de matériel aux pouvoirs publics.

En décembre 2020, la Commission européenne a lancé une consultation publique à propos d'une proposition de règlement du Parlement européen et du Conseil sur la détection, la suppression et le signalement du matériel d'abus sexuels sur des enfants en ligne. Selon l'analyse d'impact initiale relative à cette initiative, *« les actions menées dans l'UE pour lutter contre les abus sexuels d'enfants sont fragmentées, font double emploi et/ou sont insuffisantes dans certains domaines, comme le montre en particulier le suivi de la mise en œuvre de la directive relative aux abus sexuels commis contre des enfants. Ce sont en particulier les actions visant à prévenir ces abus dans l'UE, en ligne et hors ligne, qui sont insuffisantes, non coordonnées et d'une efficacité incertaine ; quant à l'efficacité de l'action que mènent les États membres pour venir en aide aux enfants victimes d'abus sexuels, elle est limitée car ils ne s'appuient pas systématiquement sur les meilleures pratiques et enseignements tirés dans d'autres États membres ou à l'échelon mondial* […] ». [104]

En s'appuyant sur des analyses plus approfondies, la Commission européenne proposera plusieurs types de législations possibles, axées en particulier sur les diverses mesures ci-après à l'échelon de l'UE :

- *Un cadre légal* instaurant une base juridique claire permettant aux fournisseurs de services d'opter pour des mesures *volontaires* visant à détecter, signaler et supprimer les abus sexuels d'enfants qui sont commis sur leurs services ainsi que *le matériel*, aussi bien *inédit* que *déjà connu*, et les *menaces par textos*. Ce cadre pourrait aussi déterminer auprès de quelle/quelles

[103] Le *Cloud Act* des États-Unis supprime par exemple la clause de « *blocage* » que prévoit le *Stored Communications Act* pour les demandes émanant des forces de l'ordre des pays avec lesquels les États-Unis ont conclu un accord bilatéral (18 U.S.C 2511(2)(j)). Il n'impose pas pour autant la divulgation de données.

[104] Analyse d'impact initiale. Règlement du Parlement européen et du Conseil sur la détection, la suppression et le signalement des cas d'abus sexuels d'enfants en ligne, et sur la création d'un centre de l'UE chargé de prévenir et de combattre les abus sexuels d'enfants en ligne (consultable à l'adresse : https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Lutte-contre-les-abus-sexuels-concernant-des-enfants-detection-suppression-et-signalement-des-contenus-illicites-en-ligne_fr).

autorité(s) publique(s) les signalements doivent être faits, que ce soit à l'échelon de l'UE ou à l'échelon national.

- *Un cadre légal* qui, en plus d'instaurer une base juridique claire comme dans la première possibilité, *contraindrait* les fournisseurs de services concernés à détecter, signaler et supprimer de leurs services tout *matériel connu d'abus sexuels sur des enfants.* Avec cette deuxième possibilité, les fournisseurs de services concernés pourraient aussi choisir d'adopter en outre des mesures visant à détecter, signaler et supprimer tout nouveau contenu et/ou menaces par textos mais *sans que ce soit pour autant obligatoire*.
- *Un cadre légal contraignant* les fournisseurs de services à détecter, signaler et supprimer de leurs services tout cas d'abus sexuel d'enfants, *qu'il s'agisse de matériel connu ou inédit ou de menaces par textos* comme le « grooming ». Comme avec la première possibilité, ce cadre pourrait aussi déterminer auprès de quelle/quelles autorité(s) publique(s) les signalements doivent être faits, que ce soit à l'échelon de l'UE ou à l'échelon national[105].

Suite à cette consultation publique, la Commission a reçu 41 avis[106] émanant de représentants des divers environnements concernés, notamment d'entités du secteur privé et d'ONG. Si les points de vue exprimés n'étaient ni homogènes ni univoques, ils montraient toutefois que la démarche suivie à l'échelon de l'UE pour prévenir et combattre l'exploitation et les abus sexuels d'enfants ne permet pas de lutter correctement contre les problèmes qui se posent et qu'il faut de toute urgence définir un cadre juridique cohérent dans l'UE.

3.2.4 Enseignements aux fins du présent rapport

Avec la libéralisation du secteur des communications ces 40 dernières années, associée à une évolution technologique rapide, par exemple avec l'informatique en nuage, la complexité du marché peut en outre poser d'autres difficultés empêchant de comprendre et de réglementer le comportement des fournisseurs de services. Le marché des communications est à la fois fortement interconnecté mais aussi très stratifié, avec des chaînes logistiques de très grande envergure, aussi bien du point de vue physique, que logique et opérationnel.

La complexité des chaînes logistiques peut avoir des incidences en termes de transparence, de légalité et de responsabilité. Si les dispositions légales ou réglementaires peuvent permettre de déterminer quel fournisseur de services est légalement responsable, le respect d'un devoir ou d'une obligation est susceptible d'être transféré à un autre fournisseur de services en application d'un contrat. L'attribution de responsabilités qui en résulte de par le mélange de mécanismes de droit public et de droit privé, peut obscurcir les questions de responsabilité pour les systèmes de détection automatique. Le point essentiel à retenir est que lorsqu'il est question du comportement d'un « *fournisseur de services* », l'idée d'une entité unique ne tient absolument pas compte de la complexité de la chaîne logistique de laquelle dépend le « service » lui-même.

Autre conséquence : les fournisseurs de services peuvent avoir accès aux marchés d'autres pays tout en opérant à partir d'un seul territoire. Du fait de cette souplesse, ils peuvent relever du ressort de

[105] Ibid.

[106] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Lutte-contre-les-abus-sexuels-concernant-des-enfants-detection-suppression-et-signalement-des-contenus-illicites-en-ligne/feedback_fr?p_id=16375286

diverses juridictions, à la fois celles du territoire sur lequel ils se trouvent mais aussi celles des territoires sur lesquels ils « *proposent leurs services* »[107]. Ce conflit de compétences a un « *coût* » pour le fournisseur de services, aussi bien en termes de respect de la loi, puisqu'il doit respecter plusieurs régimes législatifs et réglementaires différents, que de conflits de lois, puisqu'une mesure conforme à la loi d'un territoire est susceptible de constituer une infraction sur un autre. Si le respect de la loi peut être considéré comme un « *coût* » normal lié à l'exercice d'une activité économique, les conflits de lois peuvent avoir des incidences plus graves en ce sens qu'ils engagent la responsabilité du fournisseur de services, aussi bien en tant que personne morale qu'en tant que personne physique, et qu'il est difficile de s'assurer que l'ingérence dans l'exercice d'un droit est bien « *prévue par la loi* »[108].

3.3 Obligations positives au titre du droit international et européen des droits humains en matière de protection des enfants contre l'exploitation et les abus sexuels en ligne

Le droit international et européen des droits humains prévoit des droits dont l'exercice impose à divers acteurs aussi bien des obligations négatives que des positives. À l'échelon international, les acteurs concernés s'accordent maintenant globalement à dire que « *les droits ne sont pas juste des facultés individuelles subjectives imposant des limites à l'État ou à d'autres détenteurs d'obligations, ils sont liés à l'idée que les États ou d'autres acteurs ont le devoir de respecter et de protéger les droits et pas simplement de s'abstenir de les enfreindre* »[109]. Cette théorie de départ est au cœur de l'idée que les États doivent protéger les personnes risquant de subir un préjudice de la part d'acteurs de droit privé[110]. Par conséquent, les juridictions nationales, dans le monde entier, et les juridictions régionales des droits humains ont confirmé et renforcé au pénal le devoir de protection, notamment face à l'exploitation et aux abus sexuels d'enfants en ligne. S'il est nécessaire de surveiller en permanence de près cette tendance pour éviter des mesures « *trop coercitives* »[111], il est maintenant bien établi en droit international et européen des droits humains que les États ont le devoir de protéger les victimes ou victimes potentielles d'un préjudice.

3.3.1 Droits des enfants et obligations positives au titre du droit international et européen des droits humains

Nations Unies

Dans le système des Nations Unies, la protection face à l'exploitation et aux abus sexuels d'enfants en ligne repose avant tout sur la Convention des Nations Unies relative aux droits de l'enfant (CIDE). L'article 3 de la CIDE exige que *« dans toutes les décisions qui concernent les enfants, qu'elles soient le*

[107] Proposition de la Commission européenne concernant un règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM(2018) 225 définitif (17.4.2018), art. 1(1), (consultable à l'adresse : https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0002.02/DOC_1&format=PDF).

[108] Voir : CEDH, art. 8, paragraphe 2.

[109] L. Lazarus et al, *'The Evolution of Fundamental Rights Charters and Case Law'*, Parlement européen, Direction générale des politiques internes de l'Union, Direction des droits des citoyens et des affaires constitutionnelles, 2011, 34.

[110] Voir en général L Lazarus, '*The Right to Security*' in (ed), Max Planck Encyclopedia of Comparative Constitutional Law (Oxford University Press 2017).

[111] L Lavrysen and N Mavronicola (eds), '*Coercive Human Rights'*, Hart 2020.

fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale ». Il affirme en outre que « *les États parties s'engagent à assurer à l'enfant la protection et les soins nécessaires à son bien-être* », « *et ils prennent à cette fin toutes les mesures législatives et administratives appropriées* ». Au paragraphe 1, l'article 19 de la CIDE impose aux États de « *prendre toutes les mesures législatives adaptées pour protéger les enfants contre toutes les formes de violence physique ou psychologique, de brutalité ou d'atteinte à leur intégrité physique, […] de mauvais traitements ou d'exploitation, y compris d'abus sexuels* », et au paragraphe 2 il impose aux États de prendre des « *mesures de protection* » portant notamment […] sur « *d'autres formes de prévention, et aux fins d'identification, de rapport, de renvoi, d'enquête, […] et des procédures d'intervention judiciaire* ». L'article 34 de la CIDE exige que « *les États parties s'engagent à protéger l'enfant contre toutes les formes d'exploitation sexuelle et de violence sexuelle* ». Il leur impose de prendre « *toutes les mesures appropriées sur les plans national, bilatéral et multilatéral pour empêcher : a) Que des enfants ne soient incités ou contraints à se livrer à une activité sexuelle illégale ; b) Que des enfants ne soient exploités à des fins de prostitution ou autres pratiques sexuelles illégales ; c) Que des enfants ne soient exploités aux fins de la production de spectacles ou de matériel de caractère pornographique* ». Enfin, l'article 36 de la CIDE affirme que « *les États parties protègent l'enfant contre toutes autres formes d'exploitation préjudiciables à tout aspect de son bien-être* ».

La CIDE est complétée par le 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 (OPSC)[112] : un instrument qui appelle davantage l'attention sur l'obligation de l'État de prendre des mesures en matière de pénalisation, de prévention, d'enquête, de poursuites, de peines et de coopération internationale pour empêcher la vente d'enfants, la prostitution d'enfants et la pédopornographie aussi bien à l'intérieur de leurs frontières qu'à l'étranger[113].

La violence sexuelle, l'exploitation et les abus sexuels d'enfants sont par ailleurs traités dans des instruments complémentaires des Nations Unies, par exemple le « *Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée, visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants* »[114], ainsi que des textes du droit international souple, notamment : *l'Agenda des Nations Unies pour le développement durable*[115] *(objectifs 5, 8 et 16), la Déclaration et l'appel à l'action de Rio de Janeiro pour prévenir et éliminer l'exploitation sexuelle des enfants et des adolescents*[116], la publication récente intitulée

[112] Assemblée générale des Nations Unies, volume 2171, A-27531, adopté le 25 mai 2000 (en juillet 2019, 176 États avaient ratifié le Protocole facultatif ou y avaient adhéré)
https://www.ohchr.org/FR/ProfessionalInterest/Pages/OPSCCRC.aspx

[113] À sa 81e session (13-31 mai 2019), le Comité des droits de l'enfant (UNCRC) a adopté les lignes directrices sur la mise en œuvre de l'OPSC. Le rapport explicatif des lignes directrices sur la mise en œuvre de l'OPSC fait référence aux normes internationales et régionales relatives aux questions que traite l'OPSC, à diverses Observations générales sur la CIDE, et aux recommandations d'autres organes concernés, par exemple le Comité des Parties à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, autrement dit le « Comité de Lanzarote ».

[114] https://www.ohchr.org/fr/professionalinterest/pages/protocoltraffickinginpersons.aspx

[115] https://www.un.org/sustainabledevelopment/fr/objectifs-de-developpement-durable/

[116] https://www.ecpat.org/wp-content/uploads/2016/04/WCIII_Outcome_Document_Final.pdf

« *Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels* »[117], et la résolution de la Commission pour la prévention du crime et la justice pénale intitulée : « *Lutter contre l'exploitation et les abus sexuels d'enfants en ligne* »[118]. Par ailleurs, des orientations ont été données dans les rapports de la Rapporteuse spéciale des Nations Unies sur la vente et l'exploitation sexuelle d'enfants, y compris la prostitution des enfants et la pornographie mettant en scène des enfants et autres contenus montrant des violences sexuelles sur enfant[119].

Conseil de l'Europe

Convention de Lanzarote

Dans le système du Conseil de l'Europe, la Convention de Lanzarote oblige à ériger en infractions pénales toutes les formes d'abus sexuels à l'égard des enfants. En outre, elle « *constitue un cadre global et cohérent, couvrant la prévention, la coopération entre les différents acteurs, la protection et l'assistance apportées aux victimes, la criminalisation généralisée des diverses formes d'abus et d'exploitation, [et] des règles et instruments visant à faciliter les enquêtes, les poursuites et le droit procédural* ».

Plusieurs des articles de la Convention de Lanzarote sont liés au thème du présent rapport, en particulier les articles 18 (*abus sexuels*), 20 (*infractions se rapportant à la pornographie enfantine*), 21 (*infractions se rapportant à la participation d'un enfant à des spectacles pornographiques*), 22 (*corruption d'enfants*) et 23 (*sollicitation d'enfants à des fins sexuelles*). Toutes ces dispositions imposent aux États Parties de « *prendre les mesures législatives ou autres nécessaires pour ériger en infraction pénale les comportements prohibés ».* Il est précisé ce qui suit dans l'Avis interprétatif, évoqué dans l'introduction du présent document : « *les infractions mentionnées dans la Convention de Lanzarote restent érigées en infractions pénales par le droit interne de la même manière, quels que soient les moyens utilisés par les délinquants sexuels pour les commettre, que ce soit par l'utilisation des TIC ou non, même lorsque le texte de la Convention de Lanzarote ne mentionne pas expressément les TIC* »[120].

Par ailleurs, l'Avis interprétatif appelle les États Parties à « *assurer une réponse appropriée aux développements technologiques et utiliser tous les outils, mesures et stratégies appropriés pour prévenir et combattre efficacement les infractions sexuelles à l'encontre d'enfants qui sont facilitées par l'utilisation des TIC* » ; à allouer des ressources aux autorités responsables des enquêtes et des poursuites « *pour que les enquêtes et les poursuites en matière d'infractions sexuelles commises à*

---

[117] *Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels*, adoptées par l'Interagency Working Group (Groupe de travail interinstitutionnel), Luxembourg, 28 janvier 2016 (consultable à l'adresse : http://luxembourgguidelines.org/fr/version-francaise/).

[118] https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_28/ECN152019_L3REv1_eV1903716.pdf

[119] Voir le rapport récemment publié par la Rapporteuse spéciale sur la vente et l'exploitation sexuelle d'enfants, y compris la prostitution des enfants et la pornographie : « *Vente et exploitation sexuelle d'enfants* », A/HRC/43/40, 21 janvier 2020. Voir aussi : Rapporteuse spéciale sur la vente et l'exploitation sexuelle d'enfants, y compris la prostitution des enfants et la pornographie : *« 25 ans de lutte contre la vente et l'exploitation sexuelle d'enfants : relever les nouveaux défis* », 2016 (consultable, en anglais uniquement, à l'adresse : https://www.ohchr.org/Documents/Issues/Children/SR/25YearsMandate.pdf).

[120] Avis interprétatif, paragraphe 12.

l'encontre d'enfants facilitées par l'utilisation des TIC soient efficaces »[121] ; et à « *encourage[r] le secteur privé travaillant dans le domaine des TIC à contribuer à la prévention et à la lutte contre l'exploitation et les abus sexuels des enfants qui sont facilités par l'utilisation des TIC* »[122].

Particulièrement intéressant aux fins du présent rapport, l'article 10, paragraphe b), de la Convention de Lanzarote exige « *des mécanismes de recueil de données ou des points d'information, au niveau national ou local et en coopération avec la société civile, permettant, dans le respect des exigences liées à la protection des données à caractère personnel, l'observation et l'évaluation des phénomènes d'exploitation et d'abus sexuels concernant des enfants* ». L'Avis interprétatif encourage par conséquent « la coopération entre les pouvoirs publics compétents, la société civile et le secteur privé afin de mieux prévenir et combattre l'exploitation et les abus sexuels des enfants qui sont facilités par l'utilisation des TIC ».

Les exigences de la Convention de Lanzarote en matière *d'enquête, de poursuites et de droit procédural* entrent également en ligne de compte dans le présent rapport. Aux termes de l'article 30, paragraphe 5, les États Parties prennent « *les mesures législatives ou autres nécessaires pour, conformément aux principes fondamentaux de son droit interne : garantir des enquêtes et des poursuites efficaces des infractions établies conformément à la présente Convention, permettant, s'il y a lieu, la possibilité de mener des enquêtes discrètes ; permettre aux unités ou services d'enquêtes d'identifier les victimes des infractions établies conformément à l'article 20, notamment grâce à l'analyse des matériels de pornographie enfantine, tels que les photographies et les enregistrements audiovisuels, accessibles, diffusés ou transmis par le biais des technologies de communication et d'information* ».

Enfin, l'article 38 de la Convention de Lanzarote, qui présente également un intérêt aux fins du présent rapport, définit des principes généraux et des mesures de coopération internationale. Au paragraphe 3, il prévoit une base juridique pour l'entraide judiciaire en matière pénale ou d'extradition. L'Avis interprétatif appelle en outre les États à coopérer « afin de faire face au caractère transnational fréquent des infractions sexuelles commises à l'encontre d'enfants facilitées par l'utilisation des TIC»[123].

D'autres instruments du Conseil de l'Europe viennent compléter la Convention de Lanzarote en ce sens qu'ils prévoient certaines protections, à savoir, notamment : l'article 7 de la Charte sociale européenne (*protection spéciale contre les dangers physiques et moraux auxquels les enfants et les adolescents sont exposés*)[124], l'article 17 de la Charte sociale révisée (*droit des enfants à une protection sociale, juridique et économique appropriée*) et son article 17, paragraphe 1, alinéa b (*obligation de prendre toutes les mesures nécessaires et appropriées pour protéger les enfants et les adolescents contre la négligence, la violence ou l'exploitation*), les *Lignes directrices sur une justice adaptée aux enfants*,

[121] Ibid, paragraphe 14.
[122] Ibid, paragraphe 17.
[123] Ibid, paragraphe 19.
[124] Conseil de l'Europe, Série des traités européens – n° 35, Turin 18 octobre 1961. Selon le Comité européen des droits sociaux, cette disposition protège les enfants contre « *toutes les formes d'exploitation sexuelle à des fins commerciales* » à savoir : « *la prostitution enfantine, la pornographie impliquant des enfants et la traite des enfants* » (Comité européen des droits sociaux, Les droits des enfants dans la Charte sociale européenne, Document d'information).

adoptées par le Comité des Ministres du Conseil de l'Europe en novembre 2010[125], et la Convention d'Istanbul[126]. Plus récemment, le Comité des Ministres du Conseil de l'Europe a publié la « *Recommandation sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique* », soulignant les obligations des États et des acteurs non étatiques (notamment les entreprises) et qui affirment le droit des enfants « *d'être protégés contre toute forme de violence, d'exploitation et d'abus dans l'environnement numérique* »[127]. Les Lignes directrices reconnaissent notamment que *« toutes les mesures de protection devraient tenir compte de l'intérêt supérieur de l'enfant et du développement de ses capacités, et ne pas restreindre indûment l'exercice d'autres droits »*[128].

Convention de Budapest

La Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest)[129] revêt un intérêt particulier aux fins du présent rapport. Son article 9 impose aux Parties d'ériger en infractions pénales les comportements « *se rapportant à la pornographie enfantine* », qui vont de la production, de l'offre et de la diffusion, au fait de se procurer ou de procurer et de posséder ce type de matériel. Qui plus est, la Convention de Budapest prévoit les pouvoirs et procédures en matière d'enquête et de conservation des preuves non seulement liées à des actes de cybercriminalité mais aussi à toute infraction dont les éléments de preuve sont stockés au moyen d'un système informatique. Les mêmes dispositions s'appliquent en matière de coopération internationale.

Les Parties à la Convention de Budapest négocient actuellement – dans le cadre du Comité de la Convention sur la cybercriminalité (T-CY) – un deuxième protocole additionnel, relatif au renforcement de la coopération et de la divulgation des preuves électroniques. Le projet de texte[130] a été approuvé le 28 mai 2021 par le T-CY. Ce protocole offrira des outils novateurs, qui n'existaient pas encore dans les accords de droit pénal international, notamment la coopération directe avec les fournisseurs de services situés sur le territoire d'un autre État Partie pour la divulgation des données relatives aux abonnés (article 7), avec les entités fournissant des services d'enregistrement de noms de domaine pour la communication d'informations sur la personne ayant enregistré un nom de domaine (article 6) ; la divulgation accélérée de données informatiques stockées en situation d'urgence (article 9) et une demande d'entraide urgente (article 10) ; et la protection des données transférées en vertu de ce protocole (article 14).

Le deuxième protocole additionnel présente un intérêt à plusieurs titres pour ce qui concerne les mesures de lutte contre le matériel d'abus sexuels sur des enfants mais aussi le présent rapport. Premièrement, la Convention de Budapest compte actuellement 66 États Parties, dont les États-Unis, où sont basés bon nombre de fournisseurs de services. Deuxièmement, les dispositions de cette

[125] Voir aussi : Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (Convention d'Istanbul) ; Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains ; et Convention de Budapest.
[126] Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (Convention d'Istanbul), consultable à l'adresse : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/210).
[127] CM/Rec(2018)7.
[128] Ibid, paragraphe 50, p. 7. On trouvera davantage d'informations dans l'annexe.
[129] https://rm.coe.int/168008156d
[130] https://rm.coe.int/t-cy-2020-7-fr-pdp-protocol-v3t-approuve-par-le-tcy-/1680a2bb10

Convention relatives aux pouvoirs et procédures et à la coopération internationale sont applicables aux enquêtes et à la collecte de preuves électroniques, non seulement pour les infractions se rapportant à la pornographie enfantine (article 9 de la Convention de Budapest) mais aussi les autres infractions couvertes par la Convention de Lanzarote. Troisièmement, il est possible de coopérer directement avec des fournisseurs de services pour obtenir des informations sur les abonnés (article 18 de la Convention de Budapest et articles 6 et 7 du futur protocole), afin d'identifier les utilisateurs d'une adresse IP, d'une adresse e-mail ou d'un compte sur des médias sociaux, ou la personne ayant enregistré un nom de domaine. Quatrièmement, le nouveau protocole comportera des mesures d'urgence qui permettront de venir en aide à des enfants victimes. Par conséquent, en bref, les mesures que contiennent la Convention de Budapest et son nouveau protocole permettront en outre d'assurer le suivi des signalements de matériel d'abus sexuels sur des enfants envoyés par des fournisseurs de services.

La négociation de ce deuxième protocole a par ailleurs toutefois fait ressortir la nécessité d'adopter des garanties, en particulier dans le cadre de la coopération transfrontalière. Les diverses mesures qu'énonce le protocole s'appliquent par exemple uniquement à des enquêtes et poursuites pénales spécifiques et ne prévoient pas une surveillance générale des communications. Par ailleurs, les États Parties devront établir une base juridique en droit interne pour l'exécution des mesures que prévoit le protocole. À cet égard, le protocole permet aux États Parties de formuler une série de réserves et de déclarations pour satisfaire aux exigences spécifiques de leur droit interne. Ils peuvent par exemple exiger d'être notifiés lorsqu'un autre État Partie envoie directement une injonction à un fournisseur de services sur leur territoire. D'autres garanties sont prévues : limitation de l'utilisation, exigence de confidentialité ou motifs de refus ; des modalités précises en matière de protection des données à caractère personnel (article 14) ont été prévues pour veiller à ce que le transfert international de données à caractère personnel bénéficie d'une norme de protection jugée appropriée par tous les États Parties, notamment les membres de l'Union européenne. Enfin, les fournisseurs de services et les entités proposant des services d'enregistrement de noms de domaine répondront aux injonctions ou demandes relevant du deuxième protocole additionnel, qui précise en outre quels renseignements ces injonctions ou demandes doivent donner et quelles informations complémentaires elles doivent fournir.

Union européenne

Dans l'Union européenne, le point de départ en matière de protection contre l'exploitation et les abus sexuels d'enfants en ligne est l'article 24 de la Charte des droits fondamentaux de l'Union européenne (Charte de l'UE). L'article 24 de la Charte de l'UE indique dans son paragraphe 1 que « *les enfants ont droit à la protection et aux soins nécessaires à leur bien-être* », et dans son paragraphe 2, que « *dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale* ». Les « *droits de l'enfant* » sont en outre expressément protégés au titre de l'article 3, paragraphe 3, du Traité de l'Union européenne. Par ailleurs, l'article 83, paragraphe 1, du Traité sur le fonctionnement de l'UE range « *l'exploitation sexuelle des femmes et des enfants* » parmi les « *infractions pénales […] particulièrement graves revêtant une dimension transfrontière résultant du caractère ou des incidences de ces infractions ou d'un besoin particulier de les combattre sur des bases communes* ».

Directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie

À l'heure actuelle, l'instrument législatif majeur de l'UE au sujet de l'exploitation et des abus sexuels d'enfants en ligne est la directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie (directive relative aux abus sexuels commis contre des enfants), que le Parlement européen et le Conseil ont adoptée le 13 décembre 2011[131]. Ce texte vise à *protéger les droits de l'enfant* et à veiller à ce que « *l'intérêt supérieur de l'enfant* » soit une « *considération primordiale* » des « *autorités publiques ou des institutions privées* »[132]. Par ailleurs, il « *établit des règles minimales relatives à la définition des infractions pénales et des sanctions dans le domaine des abus sexuels et de l'exploitation sexuelle des enfants, de la pédopornographie et de la sollicitation d'enfants à des fins sexuelles. Il introduit également des dispositions afin de renforcer la prévention de ce type de criminalité et la protection de ceux qui en sont victimes* »[133]. La directive relative aux abus sexuels commis contre des enfants a été « *le premier instrument juridique global de l'UE* » couvrant « *la prévention, les enquêtes et les poursuites concernant les infractions, ainsi que l'assistance et la protection des victimes* »[134]. Elle affirme dès le départ que les abus sexuels et l'exploitation sexuelle des enfants, en ligne et hors ligne, « *constituent des violations graves des […] droits de l'enfant à la protection et aux soins nécessaires à son bien-être* »[135]. Elle affirme expressément que « *l'intérêt supérieur de l'enfant doit être une considération primordiale* », conformément à l'article 24, paragraphe 2, de la Charte de l'UE, et à l'article 3 de la CIDE[136].

L'article 25 de la directive relative aux abus sexuels commis contre des enfants, qui impose aux États membres deux obligations majeures, est une disposition importante qui présente un très grand intérêt aux fins du présent rapport. L'article 25, paragraphe 1, impose aux États membres de prendre « *les mesures nécessaires pour faire rapidement supprimer les pages internet contenant ou diffusant de la pédopornographie qui sont hébergées sur leur territoire* » et de s'efforcer « *d'obtenir la suppression*

[131] La directive relative aux abus sexuels commis contre des enfants découle en partie du programme de Stockholm visant à lutter contre les « *menaces transnationales* » pesant sur la sécurité intérieure de l'UE, et elle contribue au projet de reconnaissance mutuelle conforme à l'article 83, paragraphe 1, du TFUE (Le Programme de Stockholm — Une Europe ouverte et sûre qui sert et protège les citoyens, 2010 /C 115/01, 4 mai 2010). Elle coïncide en outre avec la réalisation du Programme de l'UE en matière de droits de l'enfants (*Programme de l'Union européenne en matière de droits de l'enfant*, Bruxelles, 15 février 2011, COM/2011/0060 final). Le *Programme* a réaffirmé l'engagement de l'UE en faveur de l'élimination de toutes les formes de violence à l'égard des enfants, notamment la violence sexuelle (p. 7). Parallèlement, des objectifs complémentaires ont été fixés dans le cadre du *Programme de l'UE pour un internet plus sûr*, dont l'une des activités vise à « réduire le volume de contenus illicites distribués en ligne et à s'attaquer d'une manière adéquate aux comportements préjudiciables en ligne, en se concentrant notamment sur la distribution en ligne de matériel pédopornographique » (Proposition de décision du Parlement européen et du Conseil instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication, 27 février 2008, COM/2008/0106 final). Cette évolution au sein de l'UE a suscité une réforme décisive de la décision-cadre 2004/68/JAI et l'adoption de la directive relative aux abus sexuels commis contre des enfants (voir considérants 6 et 48 de la directive en question).

[132] Considérants 1, 2 et 6 de la directive relative aux abus sexuels commis contre des enfants.

[133] Article 1 de la directive relative aux abus sexuels commis contre des enfants.

[134] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « *Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants* », 24 juillet 2020 COM(2020) 607 final (stratégie de lutte contre les abus sexuels commis contre des enfants).

[135] Considérant 1 de la directive relative aux abus sexuels commis contre des enfants.

[136] Assemblée générale des Nations Unies, résolution 44/25 du 20 novembre 1989.

des pages hébergées en dehors de celui-ci ». Le paragraphe 2 de cet article est quant à lui une clause facultative autorisant les États membres à « *bloquer l'accès* » à ces pages. Il exige que des mesures soient « *établies par le biais de procédures transparentes* » et fournissent « *des garanties suffisantes, en particulier pour veiller à ce que les restrictions soient limitées à ce qui est nécessaire et proportionnées, et que les utilisateurs soient informés de la raison de ces restrictions* ». Il exige en outre que « *ces garanties incluent aussi la possibilité d'un recours judiciaire* ». Il est par ailleurs indiqué dans le 47e considérant de la directive relative aux abus sexuels commis contre des enfants que le respect de l'article 25 ne doit pas forcément passer par des mesures législatives. *« […] Les mesures prises par les États membres conformément à la présente directive pour supprimer ou, le cas échéant, bloquer les sites internet contenant de la pédopornographie pourraient se fonder sur diverses formes d'action publique, comme des mesures législatives, non législatives, judiciaires ou autres. Dans ce contexte, la présente directive s'entend sans préjudice des mesures volontaires adoptées par le secteur de l'internet afin de prévenir tout détournement de leurs services ou du soutien que les États membres peuvent apporter à de telles mesures ».*

En 2016, la Commission européenne et le Conseil ont publié un rapport évaluant la mise en œuvre de l'article 25 de la directive relative aux abus sexuels commis contre des enfants (le rapport sur l'article 25)[137]. Il y est indiqué que « *la coopération entre le secteur privé, y compris l'industrie et la société civile, et les autorités publiques, notamment les services répressifs et le pouvoir judiciaire, est cruciale pour mettre en œuvre les mesures prévues à l'article 25* »[138]. Par ailleurs « *les mesures non législatives sont donc considérées comme transposant la directive de manière satisfaisante si elles permettent d'atteindre dans la pratique les résultats visés à l'article 25.* »[139]. Après un tour d'horizon des mesures de transposition adoptées, le rapport sur l'article 25 conclut qu'il faut encourager les États membres à en faire concrètement davantage pour respecter cet article. Les « *principaux défis* » recensés consistent à supprimer le matériel d'abus sexuels sur des enfants et à ce que des garanties soient fournies lorsque l'accès par les internautes à des pages internet est bloqué. Le rapport a donc appelé à renforcer la collaboration entre les multiples acteurs concernés à l'échelon de l'UE[140].

La résolution du Parlement européen relative aux abus sexuels commis contre des enfants « *déplore que seule la moitié des États membres aient incorporé dans leur législation des dispositions permettant de bloquer l'accès* » et appelle à davantage utiliser « *les mesures de retrait* », qui « *sont plus efficaces* »[141]. En outre, elle invite instamment les États membres et les institutions de l'UE à coopérer avec le secteur de l'internet, Europol/le Centre européen de lutte contre la cybercriminalité, Eurojust, Interpol et des pays tiers, et dans le cadre de diverses initiatives telles que celles d'INHOPE et de Connecting Europe Facility, pour atteindre les objectifs de l'article 25[142].

[137] Rapport de la Commission au Parlement européen et au Conseil évaluant la mise en œuvre des mesures visées à l'article 25 de la directive 2011/93/UE du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, COM(2016) 872 final, Bruxelles 16 décembre 2016 (rapport sur l'article 25).
[138] Rapport sur l'article 25, p. 4.
[139] Ibid.
[140] Ibid.
[141] Résolution du Parlement européen du 14 décembre 2017 sur la mise en application de la 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 (2015/2129(INI)) (résolution du Parlement européen relative aux abus sexuels commis contre des enfants), paragraphes 40 et 44.
[142] Résolution du Parlement européen relative aux abus sexuels commis contre des enfants, paragraphes 45, 46, 47, 48, 49.

Plus récemment, ces appels ont donné lieu à l'adoption de la Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants[143], et ils ont été réaffirmés dans l'initiative de la Commission européenne intitulée : « *Delivering for children: an EU Strategy on the Rights of the Child »*[144]*.* Il ressort de ces deux documents que la directive relative aux abus sexuels commis contre des enfants devra être modifiée ou remplacée afin de rester adaptée à la lutte contre l'exploitation et les abus sexuels d'enfants en ligne, en particulier compte tenu du fait que « *les auteurs d'abus ne cessent de perfectionner leur utilisation des technologies et leurs capacités techniques, notamment en matière de* ***chiffrement*** *et d'****anonymat*** »[145].

3.3.2 Jurisprudence en matière de protection des enfants contre l'exploitation et les abus sexuels en ligne

Cette section se concentrera plus précisément sur la jurisprudence relative aux obligations positives des États en matière de protection des enfants contre l'exploitation et les abus sexuels en ligne.

Cour européenne des droits de l'homme (la Cour)

Depuis le milieu des années 1980, la Cour juge qu'il existe des obligations positives relatives aux abus sexuels d'enfants, et elle en a énoncé plusieurs[146]. Ces obligations découlaient au départ de l'article 8[147] de la CEDH. Dans *MC c. Bulgarie*[148], toutefois, le viol ainsi que l'exploitation et les abus sexuels ont été considérés comme des violations de l'interdiction absolue des traitements inhumains et dégradants qui est énoncée à l'article 3 de la CEDH. Depuis lors, dans la jurisprudence relative à l'exploitation et aux abus sexuels concernant les enfants, les cas d'abus graves sont considérés comme des violations de l'article 3 de la CEDH, tandis que la Cour peut aussi traiter les moins graves comme des violations de l'article 8.

À mesure que les sensibilités ont évolué à l'égard de la gravité des abus sexuels concernant les enfants, la Cour a interprété de façon plus restrictive la marge d'appréciation des États quant au respect de leurs obligations positives. C'était déjà évident dans l'arrêt *KU c. Finlande*, dans lequel elle décrivait l'exploitation et les abus sexuels d'enfants en ligne comme « un type odieux de méfaits qui fragilisent

---

[143] Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants, Bruxelles, 24 juillet 2020 COM(2020) 607 final, (consultable à l'adresse : https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_fr.pdf).

[144] Commission européenne, La stratégie de l'UE sur les droits de l'enfant, réf. : Ares(2020)3149750 – 17 juin 2020, (consultable à l'adresse : https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12454-Strategie-de-l'UE-sur-les-droits-de-l'enfant-2021-2024-_fr).

[145] Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants, p. 6, caractères gras dans la version originale.

[146] X et Y c. les Pays-Bas, requête n° 8978/80, 26 mars 1985 ; Stubbings c. Royaume-Uni, requête n° 22083/93, 22 octobre 1996 ; MC c. Bulgarie, requête n° 39272/98, 4 décembre 2003 ; K.U. c. Finlande, requête n° 2872/02, 2 mars 2009 ; O'Keeffe c. Irlande [GC], n° 35810/09, CEDH 2014 ; Y. c. Slovénie, n° 41107/10, § 101, CEDH 2015 ; M.G.C c. Roumanie, n° 61495/11, 15 mars 2016 ; Trabajo Rueda c. Espagne, requête n° 32600/12, 30 mai 2017 ; A et B c. Croatie, GC, requête n° 7144/15, définitif le 4/11/2019 ; X et autres c. Bulgarie, GC, requête n° 22457/16, 2 février 2021.

[147] X et Y c. les Pays-Bas, requête n° 8978/80, 26 mars 1985, voir paragraphe 23 ; Stubbings c. Royaume-Uni, requête n° 22083/93, 22 octobre 1996, paragraphes 62 - 64.

[148] MC c. Bulgarie, requête n° 39272/98, 4 décembre 2003.

les victimes »[149]. La Cour s'est de plus en plus appuyée sur la Convention de Lanzarote et sur la CIDE, en particulier au sujet de « *la protection de l'intérêt supérieur de l'enfant* », pour préciser la teneur des obligations de protection et d'enquête en ce qui concerne les abus sexuels d'enfants[150].

Ces trois dernières années, la Grande Chambre de la Cour s'est penchée sur les obligations positives des États en ce qui concerne les abus sexuels commis à l'égard d'enfants dans deux arrêts majeurs : *A et B c. Croatie* (2019) et *X et autres c. Bulgarie* (2021)[151]. Ces arrêts marquent l'aboutissement de plus de 25 ans de jurisprudence de la Cour dans ce domaine et donnent des orientations faisant autorité quant aux obligations qui incombent aux États membres en la matière.

Dans *A et B c. Croatie*[152], la Cour devait se prononcer sur la décision prise face à l'agression sexuelle présumée d'une victime âgée de quatre ans et demi par son père. Elle a d'abord dû vérifier si le cadre juridique régissant l'action des autorités en matière d'enquête et de poursuites dans les affaires d'abus sexuels d'enfants était satisfaisant. Ensuite, elle s'est concentrée sur la question de savoir « *si les autorités compétentes avaient rapidement et dûment mené une enquête approfondie* ». Pour terminer, elle a vérifié « *si les autorités avaient suffisamment protégé le droit de la requérante au respect de sa vie privée et tout particulièrement de son intégrité personnelle, en tenant compte de la vulnérabilité de la requérante due à son jeune âge et aux abus sexuels présumés, et si l'intérêt supérieur de l'enfant avait été leur considération primordiale* ». Le problème n'était donc « *pas uniquement l'efficacité de l'enquête mais aussi l'absence ou l'insuffisance présumées des mesures visant à protéger, dans le cadre des poursuites pénales, les droits de l'enfant qui avait été la victime présumée d'abus sexuels* »[153].

La Cour a noté que l'article 3 (combiné à l'article 8) de la CEDH « *impose à l'État de protéger l'intégrité physique et psychologique d'une personne* », d'autant plus que « *les enfants et toute autre personne vulnérable ont tout particulièrement droit à une protection efficace* »[154]. La Cour a jugé qu'en vertu de l'article 3 « l*es autorités avaient une obligation positive* » et notamment « *le devoir de mettre en place et d'appliquer un cadre juridique approprié pour protéger les victimes contre les actes de violence commis par des particuliers* »[155] ainsi que celle de « *mener une enquête effective* »[156]. Par conséquent, les États membres doivent « *veiller à ce qu'il existe en droit pénal des dispositions permettant de dûment punir les abus sexuels commis à l'égard d'enfants et à ce qu'elles se traduisent concrètement par des enquêtes et des poursuites effectives* »[157]. Pour ce qui concerne la marge d'appréciation de l'État lorsqu'il s'acquitte de ses obligations, la GC a noté que « *lorsqu'un volet particulièrement important de l'existence ou de l'identité d'une personne est en jeu, où lorsque les activités considérées portent sur les aspects les plus intimes de la vie privée, la marge d'appréciation de l'État est alors réduite* »[158].

---

[149] K.U. c. Finlande, requête n° 2872/02, 2 mars 2009, paragraphe 46.
[150] Söderman c. Suède, requête n° 5786/08, 12 novembre 2013, paragraphes 80 - 82.
[151] A et B c. Croatie, GC, requête n° 7144/15, définitif le 4 novembre 2019 ; X et autres c. Bulgarie, GC, requête n° 22457/16, 2 février 2021.
[152] MC c. Bulgarie, requête n° 39272/98, 4 décembre 2003. Voir aussi : O'Keeffe c. Irlande [GC], n° 35810/09, CEDH 2014 ; Y. c. Slovénie, n° 41107/10, § 101, CEDH 2015 ; M.G.C c. Roumanie, n° 61495/11, 15 mars 2016.
[153] A et B c. Croatie, paragraphe 105.
[154] Paragraphe 106, citant O'Keeffe c. Irlande paragraphe 144 ; X et Y c. les Pays-Bas, paragraphes 23-24 et 27, et M.C. c. Bulgarie, paragraphe 150.
[155] Paragraphe 107, citant Söderman c. Suède [GC], n° 5786/08, paragraphe 80, CEDH 2013 et autres références.
[156] Paragraphe 108.
[157] Paragraphe 110, citant MC c. Bulgarie, paragraphe 153.
[158] A et B c. Croatie, paragraphe 113.

La GC a conclu son appréciation générale par les paragraphes importants ci-après, montrant la position actuelle de la Cour et, sur base notamment de la Convention de Lanzarote, le poids qu'elle accorde aux obligations positives relatives aux abus sexuels d'enfants[159] :

> *La Cour rappelle que dans les affaires d'abus sexuels, les enfants sont particulièrement vulnérables […] La Cour rappelle aussi que le droit à la dignité humaine et à l'intégrité psychologique requiert une attention particulière lorsqu'un enfant est victime de violence […] Elle rappelle que selon les obligations incombant à l'État au titre des articles 3 et 8 de la Convention dans de tels cas, où un enfant est impliqué ou concerné en tant que victime présumée d'abus sexuels, il faut que le droit de l'enfant de voir son intérêt supérieur primer soit respecté […] et les autorités nationales doivent dûment tenir compte de la vulnérabilité propre à cet enfant et de ses besoins.*
>
> *Au vu de ce qui précède, la Cour estime que les États sont obligés, en vertu des articles 3 et 8, d'adopter des dispositions permettant d'ériger en infractions pénales les abus sexuels d'enfants et de les appliquer en procédant à des enquêtes et des poursuites effectives […] prenant ainsi en considération la vulnérabilité particulière des enfants, leur dignité et leurs droits en tant qu'enfants et que victimes. En outre, ces obligations découlent d'autres instruments internationaux, comme la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels et la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique […]*

Dans *X et autres c. Bulgarie*[160], la GC a estimé que l'État avait échoué à protéger des enfants d'un orphelinat de Bulgarie, avant leur adoption en Italie, contre des abus sexuels, et à enquêter sur les faits. Les faits de l'espèce exigeaient une coopération internationale entre les autorités italiennes et bulgares dans le cadre de l'enquête sur les abus présumés. La GC a présenté une synthèse de la jurisprudence de la Cour et énoncé les principes généraux applicables, faisant écho à ceux qu'elle avait définis dans *A et B c. Croatie*. Sur cette base, la GC a affirmé ce qui suit[161] :

> *« Il ressort de la jurisprudence de la Cour […] que les obligations positives qui pèsent sur les autorités en vertu de l'article 3 de la Convention comportent, premièrement, l'obligation de mettre en place un cadre législatif et réglementaire de protection, deuxièmement, dans certaines circonstances bien définies, l'obligation de prendre des mesures opérationnelles pour protéger des individus précis face à un risque de traitements contraires à cette disposition et, troisièmement, l'obligation de mener une enquête effective sur des allégations défendables d'infliction de pareils traitements. De manière générale, les deux premiers volets de ces obligations positives sont qualifiés de « matériels », tandis que le troisième correspond à l'obligation positive « procédurale » qui incombe à l'État ».*

À propos de l'exigence d'effectivité de l'enquête pénale, la GC a indiqué que celle-ci pouvait « *inclure dans certaines circonstances pour les autorités qui en sont chargées une obligation de coopérer avec les autorités d'un autre État, impliquant une obligation de solliciter une assistance ou une obligation de prêter son assistance* ». Notant en outre que la nature et l'étendue de cette obligation de coopération dépendront inévitablement des circonstances de chaque espèce, la GC a ajouté que « *les États concernés doivent prendre toutes les mesures raisonnables envisageables pour coopérer les uns avec les autres et épuiser de bonne foi les possibilités que leur offrent les instruments internationaux applicables relatifs à l'entraide judiciaire et à la coopération en matière pénale* ». Par ailleurs, la Cour

[159] A et B c. Croatie, paragraphes 111 et 112.
[160] X et autres c. Bulgarie, GC, requête n° 22457/16, 2 février 2021.
[161] Ibid, paragraphe 178.

« *vérifie normalement dans ce contexte si l'État défendeur a fait usage des possibilités que lui offraient ces instruments* »[162].

De plus, la Cour a noté que l'obligation positive découlant de l'article 3 de la CEDH, qui commande l'instauration d'un cadre législatif et réglementaire « *efficace* » permettant de mettre les individus suffisamment à l'abri des abus sexuels et dont l'application soit « *effective* » en pratique, est renforcée « par les articles 18 à 24 de la Convention de Lanzarote »[163]. En outre, « *à cet égard, la Cour rappelle que la Convention doit s'appliquer en accord avec les principes du droit international, en particulier ceux relatifs à la protection internationale des droits de l'homme* » (179)[164]. Enfin, l'influence générale des principes fondateurs de la Convention de Lanzarote dans l'interprétation des obligations positives a été réaffirmée par la GC dans la conclusion de son analyse des normes juridiques applicables :

> *Il ressort enfin de la jurisprudence de la Cour que, dans les cas où des enfants ont été potentiellement victimes d'abus sexuels, le respect des obligations positives découlant de l'article 3 requiert, dans le cadre des procédures internes engagées, la mise en œuvre effective du droit des enfants à ce que leur intérêt supérieur prime, ainsi que la prise en compte de leur particulière vulnérabilité et de leurs besoins spécifiques (A et B c. Croatie, précité, § 111, et M.M.B. c. Slovaquie, n° 6318/17, § 61, 26 novembre 2019 ; voir également M.G.C. c. Roumanie, précité, §§ 70 et 73). Ces exigences sont également énoncées dans d'autres instruments internationaux pertinents en l'espèce, tels que la CIDE, la Convention de Lanzarote et les instruments adoptés dans le cadre de l'Union européenne (voir les paragraphes 124-127 et 135-137 ci-dessus).* ***D'une manière plus générale, la Cour estime que l'obligation procédurale de mener une enquête effective découlant de l'article 3 de la Convention doit être interprétée, lorsque des abus sexuels sur des mineurs sont potentiellement en jeu, à la lumière des obligations découlant des autres instruments internationaux applicables et, plus particulièrement, de la Convention de Lanzarote***.[165]

Cour de justice de l'Union européenne (CJUE)

La CJUE a rarement eu l'occasion d'examiner la question de l'exploitation et des abus sexuels d'enfants en ligne. Néanmoins, deux arrêts relatifs aux infractions interdites par la directive relative aux abus sexuels commis contre des enfants montrent le poids qui est accordé aux droits des enfants victimes d'abus sexuels, d'exploitation et de pornographie.

Le premier arrêt, *P.I c. Oberbürgermeisterin der Stadt Remscheid*[166], a été prononcé peu après l'adoption de ladite directive. Il s'agissait de savoir si l'infraction d'exploitation sexuelle commise à l'encontre d'enfants par une personne du cercle de confiance tel que défini aux articles 3 et 9 de la directive relative aux abus sexuels commis contre des enfants, était suffisamment grave pour tomber sous le coup de la notion de « *raisons impérieuses de sécurité publique* », susceptible de justifier une mesure d'éloignement au sens de l'article 28, paragraphe 3, de la directive 2004/38/CE. Dans son arrêt, la CJUE a souligné la gravité des infractions à la directive relative aux abus sexuels commis contre des enfants et estimé que ces infractions constituaient « *une atteinte particulièrement grave à un intérêt fondamental de la société, susceptible de représenter une menace directe pour la tranquillité et*

[162] Ibid, paragraphe 191.
[163] Ibid, paragraphe 179.
[164] Ibid.
[165] Ibid, paragraphe 192.
[166] P.I. c. Oberbürgermeisterin der Stadt Remscheid, affaire C-348/09, 22 mai 2012.

la sécurité physique de la population », et présentaient « *des caractéristiques particulièrement graves* »[167]. Pour arriver à cette conclusion, la CJUE a indiqué que l'exploitation sexuelle des enfants faisait partie « *des domaines de criminalité particulièrement grave revêtant une dimension transfrontalière dans lesquels l'intervention du législateur de l'Union est prévue* », conformément à l'article 83, paragraphe 1, du TFUE[168]. La CJUE a par ailleurs rappelé le premier considérant de la directive relative aux abus sexuels commis contre des enfants, qui souligne que les abus sexuels et l'exploitation sexuelle des enfants constituent des violations graves des droits de l'enfant à la protection et aux soins nécessaires à son bien-être, tels qu'ils sont consacrés dans la CIDE et dans la Charte des droits fondamentaux de l'Union européenne[169]. Enfin, elle s'est appuyée sur l'interdiction dans ladite directive des peines minimales[170] :

> *« La gravité de ce type d'infractions ressort également de l'article 3 de la directive 2011/93, qui dispose, à son paragraphe 4, que le fait de se livrer à des activités sexuelles avec un enfant qui n'a pas atteint la majorité sexuelle doit être passible d'une peine maximale d'au moins cinq ans d'emprisonnement, alors que, en vertu du paragraphe 5, sous i), du même article, le fait de se livrer à de telles activités en abusant d'une position reconnue de confiance, d'autorité ou d'influence sur un enfant doit être passible d'une peine maximale d'au moins huit ans d'emprisonnement. Selon le même paragraphe 5, sous iii), cette peine doit être de dix ans au moins en cas d'usage de la contrainte, de la force ou de menaces. Conformément à l'article 9, sous b) et g), de la même directive, doivent être considérées comme aggravantes les circonstances que l'infraction a été commise par un membre de la famille de l'enfant, une personne qui cohabite avec l'enfant ou une personne ayant abusé de sa position reconnue de confiance ou d'autorité et la circonstance que l'infraction a été commise en ayant recours à des actes de violence grave ou a causé un préjudice grave à l'enfant ».*

En quelques mots, l'arrêt *P.I c. Oberbürgermeisterin der Stadt Remscheid* réaffirme la gravité des crimes énumérés dans la directive relative aux abus sexuels commis contre des enfants et les considère comme des atteintes graves aux droits fondamentaux des enfants.

Le deuxième arrêt portant sur l'exploitation et les abus sexuels d'enfants en ligne est l'arrêt *La Quadrature du Net et autres c. Premier ministre et autres*, prononcé par la GC le 6 octobre 2020[171]. Dans cette affaire, la directive relative aux abus sexuels commis contre des enfants a été évoquée à propos de la question de « *la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique* »[172].

À propos de la conservation des données relatives à l'adresse IP, la CJUE a noté qu'eu égard au caractère grave de l'ingérence dans les droits consacrés aux articles 7 et 8 de la Charte de l'UE, « *seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence* ». La CJUE a

---

[167] Ibid, paragraphe 28

[168] Ibid, paragraphe 25.

[169] Ibid, paragraphe 26 : *« En exprimant ledit objectif, le premier considérant de la directive 2011/93 souligne que les abus sexuels et l'exploitation sexuelle des enfants constituent des violations graves des droits fondamentaux, en particulier des droits de l'enfant à la protection et aux soins nécessaires à son bien-être, tels qu'ils sont consacrés dans la Convention des Nations unies relative aux droits de l'enfant du 20 novembre 1989 et dans la Charte des droits fondamentaux de l'Union européenne ».*

[170] Ibid, paragraphe 27.

[171] La Quadrature du Net et autres c. Premier ministre et autres, affaires jointes C-511/18, C-512/18 et C-520/18, 6 octobre 2020.

[172] Ibid, paragraphe 152.

estimé que les mesures prises conformément à la directive relative aux abus sexuels commis contre des enfants entraient dans cette catégorie et relevaient de l'article 15, paragraphe 1, de la directive vie privée et communications électroniques, « *pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données* »[173].

Le raisonnement de la CJUE dans cette affaire donne de précieux indices sur le poids à attribuer aux impératifs de protection contre l'exploitation et les abus sexuels d'enfants en ligne, qui vont à l'encontre des droits relatifs à la protection des données :

> 154. *Or, aux fins de la conciliation nécessaire des droits et des intérêts en cause […], il y a lieu de tenir compte du fait que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. À cela s'ajoute le fait que la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte que la détection des infractions commises en ligne peut, de ce fait, comme l'ont indiqué plusieurs gouvernements dans leurs observations soumises à la Cour, s'avérer impossible sans avoir recours à une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58. Tel peut notamment être le cas, ainsi que l'ont fait valoir ces gouvernements, des infractions particulièrement graves en matière de pédopornographie, telles que l'acquisition, la diffusion, la transmission ou la mise à disposition en ligne de pédopornographie, au sens de l'article 2, sous c), de la 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.*
>
> *155. Dans ces conditions, s'il est vrai qu'une mesure législative prévoyant la conservation des adresses IP de l'ensemble des personnes physiques propriétaires d'un équipement terminal à partir duquel un accès à Internet peut être effectué viserait des personnes qui ne présentent, de prime abord, pas de lien, […], avec les objectifs poursuivis et que les internautes disposent, […], du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée, une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données.*
>
> *156. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence. En outre, la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi. Enfin, une mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées ».*

3.3.3 Enseignements aux fins du présent rapport

L'évolution de la jurisprudence internationale relative aux obligations positives au fil des dernières décennies est allée de pair avec un renforcement des normes et instruments juridiques internationaux

[173] Ibid, paragraphe 155.

et régionaux. Cela a permis de mettre en place un ensemble d'obligations en matière de droits humains, tirées de textes internationaux et européens, en vertu desquelles les États doivent ériger en infraction pénale toute violation des droits fondamentaux des personnes, enquêter sur ces violations, engager des poursuites et en sanctionner les auteurs. Outre la protection du droit à la vie, à la sécurité et contre la violence fondée sur le genre, la protection des enfants contre les abus sexuels est l'un des objectifs essentiels de ce domaine du droit.

L'intérêt supérieur de l'enfant, considération primordiale de tous les pouvoirs publics, et la protection contre la violence, l'exploitation et les abus sexuels, sont inscrits dans la CIDE et dans son Protocole facultatif concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants. Ces instruments sont le fondement d'autres instruments de droit international, plus récents, ayant pour objet de protéger les droits fondamentaux des enfants[174]. Au Conseil de l'Europe, la Convention de Lanzarote est le traité spécialisé phare qui « *constitue sans doute la norme internationale la plus élevée pour ce qui est de la protection des enfants contre l'exploitation et les abus sexuels* »[175]. Cet instrument vient compléter une série de normes du Conseil de l'Europe, en particulier la Convention de Budapest, dont l'objet est la protection des enfants contre l'exploitation et la violence sexuelles aussi bien hors ligne qu'en ligne[176]. Dans le droit de l'UE, l'article 24 de la Charte de l'UE, et l'article 3, paragraphe 3, du Traité de l'UE, garantissent les droits de l'enfant et le principe selon lequel « *les enfants ont droit à la protection et aux soins nécessaires à leur bien-être* »[177]. Par ailleurs, l'article 83, paragraphe 1, du TFUE range « *l'exploitation sexuelle des femmes et des enfants* » parmi les « *infractions pénales […] dans des domaines de criminalité particulièrement grave revêtant une dimension transfrontière* ». Enfin, la directive relative aux abus sexuels commis contre des enfants est un instrument législatif spécialement conçu pour intégrer dans le droit de l'UE les protections prévues dans la Convention de Lanzarote. Comme la Convention de Lanzarote, la directive relative aux abus sexuels commis contre des enfants comprend des obligations spécifiques incombant à l'État et destinées à protéger les enfants contre l'exploitation et les abus sexuels en ligne.

Dans la jurisprudence de la Cour, la protection des enfants contre l'exploitation et les abus sexuels est une obligation positive découlant des articles 3 et 8 de la CEDH. La portée et la structure de cette obligation générale ont été définies au fil de 25 ans de jurisprudence et leur évolution a suivi celle des normes internationales et européennes. La Cour souligne que la réalisation de cette obligation générale doit être « *concrète et effective* ». Les États doivent par conséquent atteindre concrètement l'objectif qu'ils se sont fixés et pas juste théoriquement ou de façon illusoire. Comme récemment

[174] Protocole visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, additionnel à la Convention des Nations Unies contre la criminalité transnationale (15 novembre 2000) ; Agenda des Nations Unies pour le développement durable (objectifs 5, 8 et 16) ; Déclaration et appel à l'action de Rio de Janeiro pour prévenir et éliminer l'exploitation sexuelle des enfants et des adolescents (2008) ; *Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels* ; Conseil économique et social des Nations Unies, Commission pour la prévention du crime et la justice pénale : « *Lutter contre l'exploitation et les abus sexuels d'enfants en ligne* » (24 mai 2019).

[175] Proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels d'enfants en ligne et à la pédopornographie, abrogeant la décision cadre 2004/68/JAI /* COM/2010/0094 final, p. 2.

[176] Article 7 de la Charte sociale européenne ; article 17 de la Charte sociale européenne révisée ; Lignes directrices du Conseil de l'Europe sur une justice adaptée aux enfants (2010) ; Recommandation sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique (CM/Rec(2018)). Voir annexe.

[177] Article 24, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne.

indiqué dans deux arrêts de principe[178], cette obligation entraîne « le devoir de mettre en place et d'appliquer un cadre juridique approprié pour protéger les victimes contre les actes de violence commis par des particuliers ». Il en découle que les États doivent adopter des dispositions de droit pénal permettant de dûment sanctionner les abus sexuels d'enfants, cela se traduisant concrètement par des enquêtes et des poursuites effectives. En outre, les États sont tenus de coopérer avec les autorités d'autres États pour solliciter une entraide ou prêter assistance, et d'épuiser « *de bonne foi* » les possibilités que leur offrent tous « *les instruments internationaux applicables relatifs à l'entraide judiciaire et à la coopération en matière pénale* »[179].

La CJUE reconnaît le poids de l'interdiction des abus sexuels d'enfants dans le droit de l'UE et précise que la gravité de l'infraction constitue « *une atteinte particulièrement grave à un intérêt fondamental de la société* »[180], pose des « *menaces graves contre la sécurité publique* »[181], et « *présente des caractéristiques particulièrement graves* »[182]. La CJUE, qui estime que les abus sexuels d'enfants sont une atteinte grave à leurs droits fondamentaux, a intégré leur protection contre l'exploitation et les abus sexuels en ligne dans le principe de l'intérêt supérieur de l'enfant tel qu'il est énoncé dans l'article 24 de la Charte de l'UE, dans la CIDE et dans la directive relative aux abus sexuels commis contre des enfants[183].

Il ressort clairement de la jurisprudence concernant les obligations positives que les États ont une marge d'appréciation quant aux moyens de respecter les obligations de protection. Lorsque la marge d'appréciation des États est réduite parce que liée à un droit absolu, il y a une forte présomption que l'obligation positive doive être respectée grâce à des moyens pratiques, effectifs et adéquats. C'est clairement le cas avec le respect de la protection contre l'exploitation et les abus sexuels d'enfants en ligne, qui ont toujours été jugés comme une atteinte aux droits les plus fondamentaux garantis dans les textes internationaux et européens portant sur les droits humains. Si, dans ce contexte, la portée de la marge d'appréciation de l'État est restreinte[184], la Cour n'a toutefois pas encore exigé des États qu'ils adoptent un système obligatoire de signalement par les parties de droit privé. Par ailleurs, il ressort clairement de la jurisprudence de la Cour et de celle de la CJUE qu'il ne peut pas être imposé aux États d'aller à l'encontre de l'exercice des droits, concurrents, au respect de la vie privée et à la protection des données[185]. Les États membres doivent par conséquent trouver le meilleur équilibre possible entre le respect des obligations négatives liées au respect de la vie privée et à la protection des données tout en satisfaisant aux normes minimales qu'entraînent les obligations positives qui leur incombent.

[178] A et B c. Croatie, GC, requête n° 7144/15, définitif, 4 novembre 2019 ; X et autres c. Bulgarie, GC, requête n° 22457/16, 2 février 2021.
[179] X et autres c. Bulgarie, paragraphe 191.
[180] P.I. v Oberbürgermeisterin der Stadt Remscheid, paragraphe 28
[181] La Quadrature du Net et autres c. Premier Ministre et autres, paragraphe 152.
[182] P.I. v Oberbürgermeisterin der Stadt Remscheid, paragraphe 28.
[183] P.I. v Oberbürgermeisterin der Stadt Remscheid, paragraphe 32.
[184] K.U. c. Finlande, requête n° 2872/02, 2 mars 2009 ; Söderman c. Suède, requête n° 5786/08, 12 novembre 2013 ; A et B c. Croatie, requête n° 7144/15, définitif le 4/11/2019 ; X et autres c. Bulgarie, GC, requête n° 22457/16, 2 février 2021.
[185] CJUE : La Quadrature du Net et autres c. Premier ministre et autres ; la Cour : Trabajo Rueda c. Espagne, requête n° 32600/12, 30 mai 2017.

3.4 Conditions et garanties en matière de protection des données

La détection et le signalement volontaires, par les fournisseurs de services, des cas d'exploitation et d'abus sexuels d'enfants en ligne se caractérisent souvent par la restriction illicite du droit des personnes au respect de la vie privée, cette restriction étant donc inacceptable car contraire à la législation applicable en matière de protection des données. Bien que ce traitement de données entraîne incontestablement une ingérence prononcée dans les droits au respect de la vie privée et à la protection des données à caractère personnel, cette section offre des orientations quant à la question de savoir dans quelles conditions et avec quelles garanties en matière de protection des données la détection et le signalement volontaires pourraient avoir lieu. Elle offre plus précisément des orientations quant au contenu (images, vidéos et texte) ou aux données relatives au trafic qui sont susceptibles d'être analysés aux fins de la détection automatique des cas d'exploitation et d'abus sexuels d'enfants en ligne, et du signalement volontaire de ces cas aux autorités compétentes en matière pénale et/ou à des services de signalement autorisés ou autres organisations luttant contre ce phénomène dans l'intérêt public. La protection des données et les garanties évoquées ci-après visent les fournisseurs de services, comme indiqué dans l'introduction du présent rapport, c'est-à-dire les fournisseurs de services de communications, dont ceux qui offrent des services de communications interpersonnelles non fondés sur la numérotation, mais aussi les intermédiaires offrant des services publics de stockage, de transmission ou de communication d'informations via internet (hébergement, transmission, espace de stockage (cloud) avec téléchargement de contenu). Par ailleurs, sans s'écarter du thème global du présent rapport, cette section se concentre sur la mise en place volontaire, par les fournisseurs de services, d'un mécanisme de détection et de signalement volontaires des cas d'exploitation et d'abus sexuels d'enfants en ligne qui soit principalement fondé sur l'intérêt public, tel que décrit dans les cadres juridiques applicables en vigueur.

3.4.1 Jurisprudence de la Cour relative à l'article 8 de la CEDH

Les conditions dans lesquelles les exceptions peuvent être légalement appliquées ont été d'abord définies par la Cour dans des affaires relatives à la surveillance des communications par l'État, par exemple dans l'affaire *Malone c. Royaume-Uni*, pour la prévisibilité des mesures[186], *Huvig c. France* et *Kruslin c. France*, pour l'exigence de règles suffisamment claires[187], *Weber & Saravia c. Allemagne* pour les garanties minimales,[188] et *Zakharov c. Russie* et *Szabó c. Hongrie* pour le soupçon raisonnable, la nécessité absolue et l'autorisation judiciaire[189]. Dans des affaires comme *K.U c. Finlande*, « les obligations positives », en vertu desquelles l'État doit prévoir des moyens efficaces pour protéger les enfants contre l'exploitation et les abus sexuels en ligne, se sont vues accorder un poids considérable face aux conditions de protection de la confidentialité des communications[190]. Mais dans *Trabajo Rueda c. Espagne,* la Cour a jugé que les mesures prises pour rechercher et saisir des preuves afin de lutter contre l'exploitation et les abus sexuels d'enfants en ligne étaient disproportionnées et entraînaient une violation de l'article 8, et, dans *Benedik c. Slovénie*, elle a jugé que le respect des

[186] Malone c. Royaume-Uni, requête n° 8691/79, 2 août 1984.
[187] Kruslin c. France, requête n° 11801/85, 24 avril 1990 ; Huvig c. France, requête n° 11105/84, 24 avril 1990.
[188] Weber et Saravia c. Allemagne, requête n° 54934/00, 29 juin 2006.
[189] Zakharov c. Russie, requête n° 47134/06, 4 décembre 2015 ; Szabó et Vissy c. Hongrie, requête n° 37138/14, 6 juin 2016.
[190] K.U. c. Finlande, requête n° 2872/02, 2 mars 2009. Voir aussi la section 3.3 plus haut sur les obligations positives de protection contre l'exploitation et les abus sexuels d'enfants en ligne.

garanties procédurales et la recevabilité des preuves en justice primaient par rapport aux poursuites engagées dans des cas d'exploitation et d'abus sexuels d'enfants en ligne[191].

3.4.2 Protection générale des données par le Conseil de l'Europe

Les règles et garanties en matière de protection des données qui sont évoquées ci-après et sur lesquelles les fournisseurs de services peuvent s'appuyer lorsqu'ils détectent et signalent volontairement des cas d'exploitation et d'abus sexuels d'enfants en ligne, sont fondées sur les obligations découlant de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, ci-après : Convention 108, telle qu'elle sera modifiée par l'entrée en vigueur du protocole d'amendement STCE n° 223 (ci-après, Convention 108+)) : il s'agit du cadre général du Conseil de l'Europe en matière de protection des données. Ces textes sont en outre conformes à d'autres cadres potentiellement applicables en matière de protection des données, par exemple ceux de l'Union européenne. Les lignes directrices ne s'appliquent que si des données à caractère personnel sont réellement traitées lorsque des cas d'exploitation et d'abus sexuels d'enfants en ligne sont détectés et signalés puis le matériel supprimé ou lors de toute autre procédure ultérieure connexe. Il est important de noter que bien que le recours aux technologies de hachage pour la pseudonymisation non réversible d'images et de vidéos soit considéré comme une garantie importante – en vue de la comparaison anonymisée de ce matériel avec du matériel d'exploitation et d'abus sexuels d'enfants déjà vérifié qui figure dans des registres ou des bases de données fiables et de qualité – les processus de détection n'en sont pas pour autant dispensés de respecter les exigences découlant de la législation sur la protection des données. Le hachage n'est qu'une technique de protection de la vie privée et l'anonymisation des données à caractère personnel, par exemple dans du contenu tel que des images et des vidéos, implique elle-même le traitement de données à caractère personnel, qui restent soumises à la législation sur la protection des données. En outre, tout signalement fondé sur une correspondance trouvée par comparaison ou fondé sur un soupçon raisonnable après détection d'une tendance (par l'IA) dans des données textuelles ou des données relatives au trafic, à l'aide, dans certains cas, des données d'historique, impliquera le transfert de données à caractère personnel (informations sur l'utilisateur ou l'IP) et sera donc soumis à la loi sur la protection des données.

Base juridique

Pour que les fournisseurs de services présents dans les États membres du Conseil de l'Europe puissent détecter automatiquement et signaler volontairement les cas d'exploitation et d'abus sexuels d'enfants en ligne lorsque cela implique le traitement de données à caractère personnel, cela doit se faire dans le respect des conditions énoncées à l'article 8 de la CEDH ainsi que des règles applicables à l'échelon national en matière de protection des données, en ce compris les obligations découlant de la Convention 108+.

Si l'article 11 de la Convention 108+ autorise des exceptions à un nombre limité de principes en matière de protection des données, dans le respect de conditions strictes, aucune exception n'est autorisée aux paragraphes 2 et 3 de l'article 5 de la Convention 108+, qui exige que tout traitement de données repose sur un fondement légitime prévu par la loi.

[191] Trabajo Rueda c. Espagne, requête n° 32600/12, 30 mai 2017 ; Benedik c. Slovénie, requête n° 62357/14, 8 avril 2015.

Si le paragraphe 3 de l'article 5 de la Convention 108+ exige que les données à caractère personnel faisant l'objet d'un traitement soient traitées licitement, le paragraphe 2 limite quant à lui la base sur laquelle les fournisseurs de services pourraient s'appuyer pour détecter automatiquement et signaler volontairement des cas d'exploitation et d'abus sexuels d'enfants en ligne : ce serait soit sur la base du *consentement* libre, spécifique, éclairé et non-équivoque des utilisateurs concernés, soit « en vertu d'autres fondements légitimes prévus par la loi », ce qui, d'après le paragraphe 46 du rapport explicatif de la Convention 108+ englobe notamment le traitement de données b) réalisé pour les *intérêts légitimes* prédominants du responsable du traitement ou d'un tiers ou c) pour des motifs d'intérêt public[192].

Le bien-fondé des trois motifs permettant de procéder à la détection automatique des cas d'exploitation et d'abus sexuels d'enfants en ligne et à leur signalement volontaire est examiné ci-après.

Consentement

À la question de savoir si les fournisseurs de services peuvent simplement s'appuyer sur le *consentement* de l'utilisateur pour procéder à la détection automatique et au signalement volontaire des cas d'exploitation et d'abus sexuels d'enfants en ligne – par exemple en indiquant dans leurs termes et conditions que lorsque l'utilisateur accepte ceux-ci, il accepte que le contenu de ses communications ou les données relatives au trafic soient automatiquement analysés à des fins de détection et de signalement aux autorités, à des centres de signalement autorisés ou à d'autres organisations agissant dans l'intérêt public – la réponse doit être forcément négative. Afin de pouvoir être considéré comme une base valide pour le traitement des données à caractère personnel, le consentement de l'utilisateur doit non seulement être spécifique et éclairé (comme ce pourrait être le cas s'il était énoncé comme indiqué ci-dessus dans les termes et conditions) mais il doit aussi être donné *librement*. Selon le paragraphe 42 du rapport explicatif de la Convention 108+, « *le consentement doit représenter la libre expression d'un choix intentionnel […] qui indique clairement dans ce contexte spécifique l'acceptation du traitement des données à caractère personnel proposé* », de telle sorte que le « *consentement ne doit pas être considéré comme libre si [la personne concernée] n'a pas de véritable choix ou de liberté de choix* ». Lorsque l'acceptation des termes et conditions est obligatoire, la personne n'a par définition ni véritablement le choix ni la liberté de choix. Par ailleurs, comme les actes d'exploitation et d'abus sexuels d'enfants en ligne qui ont été détectés doivent être signalés – éventuellement par l'intermédiaire de services de signalement autorisés ou d'autres organisations agissant dans l'intérêt public – aux autorités compétentes en matière pénale afin que celles-ci puissent enquêter et engager des poursuites, le consentement obligatoire de l'utilisateur peut d'autant moins être accepté comme base légale du traitement des données.

Intérêt légitime

La question de savoir si les fournisseurs de services peuvent baser leurs activités de traitement de données aux fins de la détection automatique et du signalement volontaire des cas d'exploitation et d'abus sexuels d'enfants en ligne, sur des « intérêts légitimes prédominants » (voir paragraphe 46 du

[192] Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223), Strasbourg, 10 octobre 2018, paragraphe 46.

rapport explicatif de la Convention 108+), qu'il s'agisse de leurs intérêts en tant que responsable du traitement des données ou de ceux d'un tiers, est plus complexe.

Si les autorités compétentes en matière pénale, auxquelles les cas d'exploitation et d'abus sexuels d'enfants en ligne doivent être signalés ou divulgués volontairement, ont un intérêt à recevoir de telles informations, l'intérêt des « tiers » (en ce qui concerne les enquêtes et les poursuites) aura du mal à servir de base légitime aux termes de l'article 5, paragraphe 2, de la Convention 108+. Il vaudra mieux dans ce cas que les États membres fassent reposer le traitement des données à caractère personnel sur l'intérêt public, comme évoqué plus bas.

Pour ce qui concerne l'intérêt légitime des fournisseurs de services, la réponse dépend des règles nationales qui leur sont applicables et/ou de la question de savoir s'ils remplissent les conditions requises pour être considérés comme des fournisseurs de services de communication électronique. Dans l'UE, par exemple, les fournisseurs de services de communication électronique sont *impérativement obligés* de veiller à la confidentialité du contenu des communications et des données connexes relatives au trafic, en application des articles 5 et 6 de la directive vie privée et communications électroniques, dont *aucune* dérogation n'est autorisée sur la base de leur propre intérêt légitime. Conformément à l'article 15 de la directive vie privée et communications électroniques, leurs obligations découlant des articles 5 et 6 *ne* peuvent être limitées *que* sur la base de mesures *législatives* adoptées par les États membres. Par conséquent, les fournisseurs qui relèvent du champ d'application géographique et matériel de la directive vie privée et communications électroniques, qui, depuis le 21 décembre 2021, couvre les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation, sont uniquement autorisés à analyser automatiquement les contenus pour y rechercher des cas d'exploitation et d'abus sexuels d'enfants en ligne, et à signaler ces derniers s'ils peuvent se prévaloir d'une base légale adoptée dans l'intérêt public. Une telle base légale doit servir à atteindre les objectifs des instruments internationaux applicables, comme la Convention de Lanzarote (voir plus bas), et être conforme aux dispositions spécifiques qu'ils contiennent. Lorsque les fournisseurs de services sont impérativement obligés d'analyser les contenus à la recherche de cas d'exploitation et d'abus sexuels d'enfants en ligne, les modalités de ces régimes obligatoires offrent une base légale.

Quant aux fournisseurs de services qui ne sont pas soumis à une telle obligation, ils peuvent légalement se prévaloir de leur propre intérêt légitime pour mettre en place un système de détection automatique et de signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne, par exemple au titre des conditions et limitations. S'il est économiquement légitime pour les fournisseurs de services de souhaiter éviter que leurs services véhiculent du contenu et du matériel qu'ils jugent nocifs, ou s'ils ne souhaitent pas faciliter la disponibilité en ligne d'un tel matériel (susceptible, en plus d'être illicite, de relever de l'exploitation et des abus sexuels d'enfants en ligne), cela ne les autorise pas à se réserver le droit, sans conditions ni limites (par ex. dans leurs termes et conditions), d'analyser automatiquement le contenu des communications ou les données relatives au trafic pour détecter de tels contenus ou matériels et pour les supprimer ou, dans les cas d'exploitation et d'abus sexuels d'enfants en ligne, de les signaler.

L'analyse automatique et le signalement sont des opérations de traitement des données qui, même si elles sont fondées sur l'intérêt légitime de l'entreprise du fournisseur de services, exigent de ménager un équilibre. Selon le paragraphe 48 du rapport explicatif de la Convention 108+, « *la légitimité d'une finalité dépendra des circonstances, le but étant de garantir dans chaque cas un juste équilibre entre*

les droits, libertés et intérêts en jeu : le droit à la protection des données à caractère personnel, d'une part, et la protection d'autres droits, d'autre part. Un juste équilibre doit ainsi être ménagé entre les intérêts de la personne concernée et ceux du responsable du traitement ou de la société ». Le paragraphe 46 du rapport explicatif de la Convention 108+, déjà cité plus haut, est encore plus strict en ce sens qu'il exige que l'intérêt légitime du contrôleur des données soit « prédominant », ce qui signifie qu'il doit l'emporter sur les intérêts ou les libertés et les droits fondamentaux des personnes dont les données sont concernées, et notamment leur droit à la protection des données, au respect de la vie privée et à la confidentialité de leur correspondance. L'analyse des contenus visant à détecter des cas d'exploitation et d'abus sexuels d'enfants en ligne et le signalement de ces derniers touchent l'ensemble des utilisateurs, dont le contrôle systématique et généralisé des contenus et des données relatives au trafic ne sera acceptable que s'il est encadré par des conditions et garanties strictes en matière de respect de la vie privée.

Utilité publique

Selon le paragraphe 47 du rapport explicatif de la Convention 108+, le traitement des données fondé sur des motifs d'intérêt public doit être prévu par *la loi* et peut, entre autres, être réalisé à des fins de prévention, d'enquête, de détection et de poursuites d'infractions pénales, par exemple l'exploitation et les abus sexuels d'enfants en ligne. Comme indiqué plus haut, un cadre légal fondé sur l'intérêt public offrira à de nombreux fournisseurs, en fonction des règles auxquelles ils sont soumis à l'échelon national, l'assise juridique la plus solide pour l'analyse automatique des contenus et matériels à la recherche de cas d'exploitation et d'abus sexuels d'enfants en ligne et pour d'éventuels signalements volontaires. Il est par conséquent fortement recommandé aux États membres du Conseil de l'Europe, conformément à leurs obligations positives énoncées dans la jurisprudence de la Cour[193], qui découlent des articles 3 et 8 de la CEDH et visent à protéger les enfants contre l'exploitation et les abus sexuels en ligne, d'établir un cadre juridique ad hoc, fondé sur l'intérêt public et permettant aux fournisseurs de services de détecter automatiquement et de signaler volontairement les cas d'exploitation et d'abus sexuels d'enfants en ligne, dans le respect d'un certain nombre de conditions et garanties. Dans ce contexte, la définition de cet intérêt public pourrait reposer sur les normes communes qu'énonce la Convention de Lanzarote.

Données sensibles

Lorsque des images et des vidéos sont analysées pour détecter des cas d'exploitation et d'abus sexuels d'enfants en ligne et que cette opération dévoile la vie et les préférences sexuelles des personnes, et notamment d'enfants, les données concernées devraient être considérées comme étant sensibles. Cela signifie, conformément à l'article 6 de la Convention 108+, que le traitement des données ne sera autorisé que si des garanties appropriées inscrites dans la loi viennent compléter celles que prévoit la Convention 108+. Ces garanties devraient protéger les personnes concernées contre les risques que le traitement de leurs données pourrait entraîner pour leurs intérêts, leurs droits et leurs libertés fondamentales.

La protection des intérêts, des droits et des libertés fondamentales des enfants oblige les fournisseurs de services, dans le cadre des activités qu'ils mènent pour détecter automatiquement, supprimer et signaler volontairement les cas d'exploitation et d'abus sexuels d'enfants en ligne, à éviter toute

[193] Voir la Section 3.3 ci-dessus.

ingérence inutile dans les droits des adolescents qui arborent un comportement sexuellement explicite, et notamment dans leur droit au respect de la vie privée et dans l'exploration de leur sexualité, qui fait partie de ce dernier. Malgré les défis technologiques et juridiques qui se posent pour distinguer qualitativement les images, la protection du droit des enfants au respect de la vie privée devrait comprendre celle du droit à découvrir leur identité sexuelle dans un environnement sûr et privé. Par ailleurs, les fournisseurs de services devraient protéger l'épanouissement de l'identité et des expériences sexuelles des enfants ainsi que l'intimité des photos ou vidéos explicites dans lesquelles ils se représentent et qu'ils envoient à d'autres enfants, où, lorsqu'ils ont atteint l'âge du consentement sexuel en droit national, qu'ils partagent plus largement. Les fournisseurs de services devraient aussi éviter de signaler aux autorités compétentes en matière pénale des cas de sollicitation lorsque les utilisateurs et les personnes représentées ont atteint l'âge du consentement sexuel prévu en droit national.

Par ailleurs, la comparaison des images et des vidéos devrait se faire sans que les données biométriques soient traitées par des moyens techniques et légaux permettant l'identification ou l'authentification uniques d'une personne physique. Il faut, à cet effet, analyser les données traitées pour déterminer s'il s'agit de données biométriques.

3.4.3 Conditions et garanties[194]

Indépendamment du fait que d'autres garanties importantes doivent être adoptées, notamment en matière d'État de droit, de droit pénal et de procédure, les conditions et garanties ci-après sont des normes minimales relatives à la protection des données, sans préjudice de l'application de l'article 8 de la CEDH, des règles de droit interne applicables à la protection des données et des obligations liées à la Convention 108 et, dès son entrée en vigueur, à la Convention 108+.

Il faut par ailleurs noter qu'outre les règles de détection automatique et de signalement volontaire des cas d'exploitation et d'abus sexuels d'enfants en ligne susceptibles d'être fondées sur un intérêt légitime, aucune exception à la Convention 108+ n'est autorisée (voir plus haut). Lorsque le traitement des données est fondé sur un tel intérêt, la règle devrait être celle de l'équilibre entre, d'une part, l'intérêt légitime prédominant du contrôleur des données et, d'autre part, les droits et intérêts des personnes dont les données sont concernées, sous réserve que les garanties appropriées soient en place. Les exceptions de l'article 11 de la Convention 108+ ne seront autorisées que si elles sont énoncées dans une loi et si elles ne portent que sur un nombre limité de principes en matière de

[194] Tirées à la fois de la Convention 108+ et de la proposition de règlement du Parlement européen et du Conseil concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des 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, les conditions et garanties suggérées renvoient à des extraits de la proposition de règlement et notamment aux modifications proposées par la LIBE dans la version la plus récente consultable en ligne au moment de la rédaction du présent rapport : Conseil de l'Union européenne, proposition de règlement du Parlement européen et du Conseil concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des 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. État d'avancement des réunions techniques avec le Parlement européen et des débats sur les modifications proposées, Bruxelles, 26 janvier 2021, 5616/21.

protection des données. Quoi qu'il en soit, toute restriction doit reposer sur des motifs d'intérêt public inscrit dans la législation, poursuivre une finalité légitime et constituer « *une mesure nécessaire et proportionnée dans une société démocratique* », conformément à la jurisprudence de la Cour en matière de protection des données.

Limites poursuivant une finalité stricte

Selon l'article 5, paragraphe 4, alinéa b, de la Convention 108+, les données à caractère personnel qui sont traitées par les fournisseurs de services lorsqu'ils analysent les communications et les données correspondantes relatives au trafic, ne doivent l'être qu'à la seule finalité de détecter les cas d'exploitation et d'abus sexuels d'enfants en ligne pour les supprimer et/ou procéder à leur signalement ou leur divulgation volontaires aux autorités compétentes en matière pénale et/ou aux services de signalement autorisés ou à d'autres organisations agissant dans l'intérêt public pour lutter contre ce phénomène.

Quantité minimale de données et proportionnalité

Les données à caractère personnel qui sont traitées à des fins de détection et de signalement ou divulgation volontaires doivent être limitées au strict nécessaire, conformément à l'article 5, paragraphe 4, alinéa b, de la Convention 108+, afin que la proportionnalité, qui est l'un des principes majeurs de la protection des données, soit respectée.

Protection des données dès la conception

Comme défini à l'article 10, paragraphe 2, de la Convention 108+, les fournisseurs de services doivent concevoir le traitement des données de façon à éviter ou à limiter le risque d'ingérence dans les droits et dans les libertés fondamentales des personnes dont les données sont concernées. Par conséquent, les technologies qu'ils utilisent pour la détection automatique :

- doivent être les moins intrusives possibles en matière de vie privée et correspondre à l'état de la technique dans le secteur ;
- doivent, lorsqu'elles servent à analyser le contenu d'images ou de vidéos, utiliser de préférence le hachage pour la pseudonymisation non réversible d'images et de vidéos en vue de leur comparaison anonymisée avec du matériel d'exploitation et d'abus sexuels sur des enfants qui a été vérifié et qui figure dans des registres ou des bases de données fiables et de qualité ;
- sont incapables, lorsqu'elles sont utilisées pour analyser des communications contenant du texte, d'en comprendre la teneur et peuvent seulement être en mesure de détecter des tendances indiquant d'éventuels cas d'exploitation et d'abus sexuels d'enfants en ligne, à l'aide des principaux indicateurs pertinents et des facteurs de risque recensés objectivement ;
- doivent être suffisamment fiables pour limiter le taux d'erreur et éviter de renvoyer des faux positifs, qu'il s'agisse de contenus ou de tendances (c.-à-d. identification ou suspicion erronées de cas d'exploitation et d'abus sexuels d'enfants en ligne), et doivent correspondre dans toute la mesure du possible à l'état de la technique dans le secteur, et, si de telles erreurs se produisent, leurs conséquences doivent être rectifiées sans attendre ;

- ne doivent pas, lorsque c'est techniquement possible, entraîner une ingérence dans toute communication protégée par le secret professionnel, par exemple entre des médecins et leurs patients, des journalistes et leurs sources, ou des avocats et leurs clients.

Analyse d'impact

Les fournisseurs de services doivent analyser l'impact que le traitement des données est susceptible d'avoir sur les droits et sur les libertés fondamentales des personnes concernées avant de lancer ce processus, et doivent avoir indiqué que ce traitement n'entraînerait pas un risque élevé pour les droits et les libertés fondamentales de ces personnes, ou qu'ils ont pris des mesures pour atténuer le risque.

Transparence

Les fournisseurs de services doivent faire savoir dans leurs termes et conditions, aux personnes dont les données sont concernées, qu'ils limitent la confidentialité de leurs communications et des informations correspondantes relatives au trafic uniquement aux fins de la détection des cas d'exploitation et d'abus sexuels d'enfants en ligne, en vue de leur suppression et/ou du signalement ou de la divulgation volontaires de tels cas aux autorités compétentes en matière pénale et/ou à des services de signalement autorisés ou autres organisations luttant contre ce phénomène dans l'intérêt public.

Par ailleurs, en cas de résultat positif suite à la comparaison avec du matériel d'exploitation et d'abus sexuels sur des enfants qui a été vérifié et qui figure dans des registres ou des bases de données fiables et de qualité, ou en cas de soupçon raisonnable suite à la détection d'une tendance (au moyen de l'IA) dans du contenu textuel ou dans des données relatives au trafic, sur base, dans certains cas, des données d'historique, les personnes concernées doivent recevoir les informations suivantes :

- les autorités compétentes en matière pénale et les services de signalement autorisés, ou autres organisations luttant dans l'intérêt public contre les cas d'exploitation et d'abus sexuels d'enfants en ligne, avec lesquels leurs données à caractère personnel ont été partagées ;
- les possibilités d'indemnisation par les fournisseurs de services ;
- la possibilité de déposer une plainte auprès des autorités de contrôle compétentes, et d'intenter un recours judiciaire, et l'identité desdites autorités.

La communication desdites informations peut être retardée si elle est susceptible de nuire à une enquête en cours, auquel cas ce retard ne devra pas dépasser le strict nécessaire et les personnes concernées devront être informées sans attendre une fois l'enquête achevée.

Signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne après une détection automatique

Comme le signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne susceptible d'intervenir suite à une détection automatique peut considérablement affecter la personne dont les données sont concernées, il ne sera jamais uniquement fondé sur le résultat de la procédure automatique. Les fournisseurs de services doivent veiller à ce que le traitement automatique des données à caractère personnel fasse l'objet d'une intervention et d'un contrôle humains. Par ailleurs, aucun signalement ou aucune divulgation aux autorités compétentes en matière pénale et/ou à des services de signalement autorisés ou autres organisations luttant dans l'intérêt public contre

l'exploitation et les abus sexuels d'enfants en ligne, ne peut intervenir tant qu'un résultat positif ou un soupçon légitime n'a pas été analysé et confirmé par un humain.

Sécurité des données

Les fournisseurs de services doivent établir des procédures internes pour prévenir les abus ainsi que l'accès, l'utilisation, la suppression ou les transferts non autorisés.

Conservation limitée

Si aucun cas d'exploitation et d'abus sexuels d'enfants en ligne n'a été détecté et confirmé, toutes les données relatives au contenu et au trafic, et tous les résultats obtenus à la suite du traitement doivent être effacés immédiatement après avoir été traités.

Lorsque des cas d'exploitation et d'abus sexuels d'enfants en ligne ont été détectés et confirmés, les données strictement nécessaires relatives au contenu et au trafic et les données à caractère personnel générées par le traitement sont conservées uniquement aux fins des objectifs énumérés ci-après et seulement pendant le délai strictement nécessaire, après quoi elles devront être supprimées immédiatement et de façon permanente :

- pour signaler et transférer des données dans un délai raisonnable aux autorités compétentes en matière pénale et/ou à des services de signalement autorisés ou autres organisations luttant dans l'intérêt public contre l'exploitation et les abus sexuels d'enfants en ligne ;
- pour bloquer le compte de l'utilisateur concerné ou pour suspendre un service qui lui est proposé ;
- pour créer un hachage aux fins de comparaisons futures, lorsque les données à caractère personnel sont incontestablement liées à des cas d'exploitation et d'abus sexuels d'enfants en ligne ;
- pour qu'une plainte puisse être déposée ainsi qu'aux fins des sanctions et/ou recours judiciaires et extrajudiciaires.

Mécanismes de plainte et recours effectifs

Sans préjudice de leur droit de recours en cas de violation des règles de protection des données, les utilisateurs qui ont eu à pâtir de l'utilisation de technologies spécifiques pour le traitement de données à caractère personnel aux fins de la détection, de la suppression ou du signalement de cas d'exploitation et d'abus sexuels d'enfants en ligne, doivent avoir la possibilité de déposer plainte contre les mesures prises par un fournisseur de services et ont droit à un recours effectif si le matériel supprimé ou signalé ne constitue pas un tel cas. Par conséquent, les fournisseurs de services doivent mettre en place des mécanismes de plainte accessibles et effectifs et les membres du Conseil de l'Europe doivent quant à eux adopter des procédures de recours effectives, notamment dans les cas où :

- le contenu des utilisateurs a été supprimé ou leur compte a été bloqué, ou bien le service qui leur est proposé a été suspendu ;
- le contenu ou l'identité des utilisateurs ont été signalés aux autorités compétentes en matière pénale et/ou à des services de signalement autorisés ou autres organisations luttant dans l'intérêt public contre l'exploitation et les abus sexuels d'enfants en ligne.

Flux transfrontières d'informations

Durant le processus automatique de comparaison du contenu d'images ou de vidéos avec des registres ou bases de données externes et/ou le signalement ou la divulgation de cas d'exploitation et d'abus sexuels d'enfants en ligne aux autorités compétentes en matière pénale et/ou à des services de signalement autorisés ou autres organisations agissant dans l'intérêt public, les fournisseurs de services doivent pleinement respecter les conditions applicables aux flux transfrontières de données à caractère personnel, par exemple celles qui sont énoncées dans le chapitre III de la Convention 108+.

Ils pourraient donc se prévaloir de l'article 14 de la Convention 108+ une fois que le protocole d'amendement STCE n° 223 entrera en vigueur, et envoyer des données à caractère personnel sans autres conditions à d'autres Parties à ce protocole si aucune des exceptions énoncées à l'article 14, paragraphe 1, ne s'applique à ce transfert de données précis. Comme ça ne sera guère le cas dans l'immédiat ni certainement avant 2023, ni probablement non plus après cette date pour l'ensemble des grands territoires impliqués dans les transferts de données aux fins de la lutte contre l'exploitation et les abus sexuels d'enfants en ligne, l'article 14, paragraphe 3, de la Convention 108+ pourrait aussi s'appliquer à un fournisseur de services souhaitant envoyer des données à caractère personnel à un autre État ou territoire.

Bien que ça ne soit pas encore contraignant, « un niveau approprié de protection fondé sur les dispositions de la présente Convention est garanti » lors du transfert et dans l'État destinataire, lequel devrait rassurer suffisamment toute partie privée pour pouvoir coopérer et envoyer des données avec l'une des méthodes décrites ci-après. Selon l'article 14, paragraphe 3, de la Convention 108+, « un niveau de protection des données approprié peut être garanti par : a) les règles de droit de cet État ou de cette organisation internationale, y compris les traités ou accords internationaux applicables ; ou b) des garanties ad hoc ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables, adoptés et mis en œuvre par les personnes impliquées dans le transfert et le traitement ultérieur des données ». Il faut par conséquent poursuivre le travail d'analyse et, s'il y a lieu, mettre en place de telles garanties provisoires.

Les termes et conditions de l'article 14 du deuxième protocole additionnel à la Convention de Budapest (voir section 3.3.1 plus haut) pourraient également jouer un rôle capital dans la décision à prendre au sujet de la condition a (déterminer si le droit d'un pays offre un niveau de protection des personnes approprié lors des transferts transfrontières de données). Conformément à la Convention 108+ – et tout particulièrement à la première exception décrite sous son article 11, paragraphe 1 – et au système de protection des données de l'Union européenne et des États Parties à la Convention de Budapest (dont les États-Unis, le Canada, l'Australie et le Japon), ces termes et conditions pourraient être examinés lorsqu'un État s'engage dans une coopération en matière de justice pénale impliquant le traitement de preuves électroniques et qu'il cherche à mettre en place un niveau de protection approprié durant le transfert de données entre autorités dans le cadre des enquêtes en cours sur des données déjà disponibles et souvent détenues par des fournisseurs de services. Le deuxième protocole additionnel à la Convention de Budapest sera ouvert à la signature au printemps 2022. Le mécanisme de transfert qu'il permettra de mettre en place dès son entrée en vigueur impliquera pour les fournisseurs de services que le pays où ils sont établis prendra une série de mesures, notamment législatives, dès la ratification du texte, et qu'ils devront continuer de respecter les règles de protection des données de ce pays. Il est donc probable que les entités privées se prévaudront pendant un certain temps de la condition b (niveau de protection approprié avec des garanties ad hoc ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables).

Pour contribuer à la vérification du niveau de protection qu'un État ou une organisation internationale pourraient garantir en droit, les acteurs intéressés, entités privées ou publiques mondiales, pourraient être invités, et soutenus à cet effet, à étoffer les « registres d'importateurs de données » et les « pôles de signalement par pays » déjà utilisés ou à en mettre en place. Parmi ces outils, il y a des listes de pays, établies sur la base d'une analyse juridique approfondie, vers lesquels des données à caractère personnel pourraient être envoyées sans réduire le niveau de protection de ces données qu'assure le pays où le fournisseur de services est installé ou offre ses services. Les analyses réalisées par des entités publiques, par exemple les décisions de la Commission européenne relatives à l'adéquation du niveau de protection des données, ou les évaluations que réalise le Comité de la Convention 108 au sujet des pays qui demandent à adhérer au texte, ou, à l'avenir, les évaluations du niveau de protection offert conformément à l'article 23, alinéas e et f, pourraient aussi fournir des orientations.

S'agissant de la conformité à la condition b de l'article 14, paragraphe 3, de la Convention 108+, il existe déjà plusieurs possibilités susceptibles d'offrir des orientations quant aux modalités de transfert de données à caractère personnel d'un territoire à l'autre avec le même niveau de protection offert, notamment : les clauses contractuelles types pour le transfert de données à caractère personnel entre pays de l'UE et pays tiers, clauses qui peuvent aussi être utilisées en toute sécurité dans un contexte non-UE ou pas exclusivement UE ; les dispositions des Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, et les Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance, adoptées par le Comité européen de la protection des données.

Toutefois, les clauses contractuelles types et les recommandations doivent être analysées à la lumière de l'arrêt de la CJUE *Commissaire à la protection des données c. Facebook Irlande et Maximilian Schrems* (*« Schrems II »*)[195]. L'arrêt *Schrems II*, qui invalide une deuxième fois l'instrument de transfert bilatéral entre l'Union européenne et les États-Unis, porte sur deux exigences spécifiques. La première est l'existence nécessaire de recours juridiques et donc de droits effectifs et opposables à un recours devant un tribunal indépendant et impartial. La deuxième, qui concerne l'ampleur de certains programmes de surveillance, est l'absence de limites d'accès par les autorités nationales aux données à caractère personnel, ce qui porte atteinte au principe de la stricte nécessité. Il ressort de l'arrêt qu'un nouvel accord, plus durable et viable, qui est en cours de négociation entre l'Union européenne et les États-Unis, pourrait aussi avoir des incidences sur les transferts de données aux fins de la lutte contre l'exploitation et les abus sexuels d'enfants en ligne, et qu'il a déjà eu des conséquences directes sur les clauses contractuelles types actualisées que la Commission européenne a récemment publiées (4 juin 2021)[196]. Par ailleurs, cet arrêt a déjà incité le Comité européen de la protection des données à résumer les exigences essentielles qu'un contrôleur de données doit respecter lors d'un transfert de données à caractère personnel d'un État membre de l'UE vers un État non-membre de l'UE. Les conditions sont très similaires à celles qu'énonce l'article 11 de la Convention 108+, sur la base de la jurisprudence de la Cour décrite plus haut.

[195] Commissaire à la protection des données c. Facebook Irlande et Maximilian Schrems, affaire C-311/18, 16 juillet 2020.

[196] Clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers | Commission européenne (europa.eu)

Divers modèles qui ont été créés (et publiés) dans le secteur, par exemple les « analyses d'impact du transfert des données », mérite également un examen plus poussé. La méthode utilisée pour procéder à ces analyses ne peut pas être décrite ici dans son intégralité mais certains de ses éléments clés pourraient jeter les bases de nouvelles réflexions. Généralement, une fois toutes les opérations de transfert cartographiées, des solutions techniques sont recommandées à titre de garanties venant s'ajouter à celles dont les transferts sont déjà assortis (concernant la sécurité des données, la qualité des données, la transparence, la base juridique appropriée, la diligence requise avec les données sensibles, les exigences en matière de responsabilité, etc.). Il s'agit par exemple du cryptage avec la clé que détient le personnel du pays expéditeur, et du fait de rapatrier les transferts stratégiques. En outre, les analyses recommandent habituellement que l'entreprise établisse des règles contraignantes, pour validation par l'autorité locale de protection des données et, *in fine*, par le CEPD. Enfin, pour le long terme, les analyses recommandent de faire en sorte que le stockage et l'hébergement des données soient locaux pour pouvoir utiliser des solutions techniques plus astucieuses, par exemple des services du Cloud facilités par des fournisseurs locaux, une chaîne de blocs, les fiducies de données, etc.

3.4.4 Enseignements aux fins du présent rapport

La détection automatique et le signalement volontaire des cas d'exploitation et d'abus sexuels d'enfants en ligne ont des incidences sur la confidentialité du contenu des communications et sur les données connexes relatives au trafic, or les fournisseurs de services doivent veiller à cette confidentialité. La détection et le signalement entraînent une ingérence dans le droit au respect de la vie privée et de la vie familiale, et dans la protection des données à caractère personnel des personnes concernées, à savoir, notamment, les utilisateurs, parmi lesquels les contrevenants potentiels, mais aussi les enfants qui apparaissent dans le matériel d'exploitation et d'abus sexuels en ligne et qui doivent aussi avoir la possibilité de communiquer en toute confidentialité avec un adulte de confiance, avec les organisations actives dans la lutte contre ce phénomène, et avec leur avocat.

Bien que le recours aux technologies de hachage pour la pseudonymisation non réversible d'images et de vidéos – en vue de leur comparaison anonymisée avec du matériel d'exploitation et d'abus sexuels sur des enfants qui a été vérifié et qui figure dans des registres ou des bases de données fiables et de qualité – soit considéré comme une garantie importante, les processus de détection n'en sont pas pour autant dispensés de respecter les exigences découlant de la législation sur la protection des données. Le hachage n'est qu'une technique de protection de la vie privée et l'anonymisation des données à caractère personnel, par exemple dans du contenu tel que des images et des vidéos, implique elle-même le traitement de données à caractère personnel, qui restent soumises à la législation sur la protection des données. En outre, tout signalement fondé sur une correspondance trouvée par comparaison ou fondé sur un soupçon raisonnable après détection d'une tendance (par l'IA) dans des données textuelles ou des données relatives au trafic, à l'aide, dans certains cas, des données d'historique, impliquera le transfert de données à caractère personnel (informations sur l'utilisateur ou l'IP) et sera donc soumis à la loi sur la protection des données.

4. PRINCIPALES CONCLUSIONS ET RECOMMANDATIONS

Par rapport à la fin des années 1990, il existe à l'heure actuelle au moins deux fois plus de formes d'exploitation et d'abus sexuels d'enfants. À cause de l'utilisation prédominante des technologies de l'information et de la communication (TIC), les enfants peuvent être confrontés en grande partie aux mêmes risques en ligne que hors ligne. L'appel à une action concertée visant à les protéger contre l'exploitation et les abus sexuels en ligne est encore plus fort vu les effets que la pandémie de covid-19 a eus sur les principales menaces liées à ce phénomène.

> ***Recommandation n° 1 : pour réussir à prévenir et combattre les formes actuelles d'exploitation et d'abus sexuels d'enfants en ligne, les pouvoirs publics doivent suivre l'évolution technologique constante dans ce domaine et y réagir, celle-ci étant notamment facilitée par l'utilisation prédominante des TIC, qui ne cessent d'évoluer. Le recours à des technologies automatisées dans la lutte contre l'exploitation et les abus sexuels d'enfants en ligne est en l'occurrence essentiel.***

Il y a un décalage entre le recours aux technologies de détection automatique et le niveau des informations publiées sur l'adoption de ces technologies. En raison de ce manque d'informations, les décideurs et les régulateurs ont du mal à se faire une opinion correcte sur la façon de réglementer ces technologies et à proposer des garanties adéquates.

> ***Recommandation n° 2 : pour assurer un juste équilibre entre le respect de la vie privée et la protection des enfants contre l'exploitation et les abus sexuels, il est de la plus haute importance de favoriser un dialogue entre les entreprises du secteur privé et les décideurs/régulateurs. Ce dialogue devrait avant tout viser principalement à dûment garantir la transparence quant au choix technologique et aux processus dont la technologie choisie est assortie.***

Actuellement, le niveau insuffisant de transparence quant à la qualité et à la taille des listes de hachage du matériel connu d'abus sexuels sur des enfants limite dans une certaine mesure le potentiel de telle ou telle solution technologique en termes de retrait rapide dudit matériel.

> ***Recommandation n° 3 : les initiatives destinées à améliorer la coordination dans ce domaine devraient être répertoriées et soutenues car elles sont indispensables à la fiabilité des bases de données de référence. À ce propos, il est en outre nécessaire de veiller à davantage de clarté sur la façon dont les mécanismes de responsabilité sont gérés, notamment le recrutement et la formation des personnes employées par les entreprises du secteur privé pour analyser du contenu illicite, comme le matériel d'abus sexuels sur des enfants.***

S'agissant de définir des garanties, il est plus sûr, pour les décideurs et les régulateurs, d'opter pour une technologie bien éprouvée, bien documentée et stable. Toutefois, face aux défis que pose actuellement la lutte contre l'exploitation et les abus sexuels d'enfants en ligne, il pourrait être judicieux ou nécessaire d'utiliser des technologies plus puissantes qui en sont aux premiers stades de développement.

Recommandation n° 4 : pour mieux préserver l'équilibre entre respect de la vie privée et protection des enfants contre l'exploitation et les abus sexuels, il faudrait définir le niveau approprié de garanties le plus tôt possible durant le processus de développement d'une technologie. Les décideurs et les régulateurs devraient se concentrer tout particulièrement sur le jeu de données qu'utilise cette technologie pour définir des associations complexes d'algorithmes.

Chaque outil de détection des cas d'exploitation et d'abus sexuels d'enfants en ligne est différent et comporte ses propres objectifs. Pour définir les moyens de détection les moins restrictifs, il faut bien comprendre l'objectif de chaque technologie et l'environnement pour lequel elle est choisie.

Recommandation n° 5 : pour améliorer le respect de la vie privée tout en donnant la priorité à la protection des enfants contre l'exploitation et les abus sexuels, il est nécessaire de favoriser les solutions technologiques qui sont les plus efficaces pour les objectifs recherchés.

Le nombre d'experts dans chacun des domaines concernés étant limité, les débats ont lieu en vase clos alors que la controverse suscitée par la proposition de la Commission européenne a montré qu'il fallait proposer des solutions efficaces pour prévenir et combattre l'exploitation et les abus sexuels d'enfants en ligne.

Recommandation n° 6 : il faudrait recenser et soutenir les initiatives axées sur un dialogue transversal.

Il convient de noter que diverses instances internationales, la Cour européenne des droits de l'homme et la Cour de justice de l'UE accordent une grande importance à la nécessité de protéger les enfants contre les infractions à caractère sexuel, tout comme la Convention de Lanzarote et la directive relative aux abus sexuels commis contre des enfants, lorsqu'il s'agit de concilier le droit des enfants à une protection et le droit à la protection des données.

Recommandation n° 7 : il faut dûment tenu compte, dans le débat législatif à venir, de l'importance accordée en droit international et européen des droits humains aux obligations positives dans la lutte contre l'exploitation et les abus sexuels d'enfants en ligne, ainsi qu'à l'intérêt supérieur de l'enfant.

Les textes juridiques, en évolution constante, qui régissent à l'heure actuelle les technologies de détection automatique n'abordent pas suffisamment les défis que pose le fait de chercher à protéger les enfants contre l'exploitation et les abus sexuels en ligne et à prévenir ce phénomène tout en veillant au maximum au respect de la vie privée dans les communications en ligne.

Recommandation n° 8 : compte tenu des lacunes juridiques actuelles, les États membres du Conseil de l'Europe devraient examiner la nécessité de définir un cadre juridique harmonisé et durable, susceptible d'offrir une sécurité juridique aux fournisseurs de services en tenant compte des progrès technologiques futurs.

Il ressort de l'analyse des normes du Conseil de l'Europe relatives à la protection des données et de la jurisprudence de la Cour en la matière, qu'un cadre juridique ad hoc fondé sur l'intérêt public offrirait l'assise juridique la plus solide pour la détection automatique des cas d'exploitation et d'abus sexuels d'enfants en ligne, les signalements volontaires et les flux transfrontières de données à caractère

personnel, et que la définition de l'intérêt public pourrait reposer sur les normes communes qu'énonce la Convention de Lanzarote.

> ***Recommandation n° 9 : les États membres du Conseil de l'Europe sont vivement encouragés, conformément aux obligations positives qui leur incombent de protéger les enfants contre l'exploitation et les abus sexuels en ligne, à mettre en place un cadre juridique axé sur l'intérêt public selon la Convention de Lanzarote, qui permettrait aux fournisseurs de services de détecter automatiquement, de supprimer et de signaler les cas d'exploitation et d'abus sexuels d'enfants en ligne puis de transférer des informations sur ces cas tout en respectant les conditions et garanties énumérées dans la section 3.4 en matière de protection des données et de respect de la vie privée.***

5. GLOSSAIRE

IA – Intelligence artificielle

VO – Vision par ordinateur

CE – Commission européenne

CEPD – Contrôleur européen de la protection des données

CCEE – Code des communications électroniques européen

CESE – Comité économique et social européen

EOKM – Expertisebureau Online Kindermisbruik

ESN – European Service Network

EUROPOL – Agence de l'Union européenne pour la coopération des services répressifs

HF – Hachage de fichiers

SVH – Service de vérification des hachages

ICCAM – « I see Child Abuse Material »

IP - Protocole internet

ICSE – Base de données internationale sur l'exploitation sexuelle des enfants

TIC – Technologies de l'information et de la communication

INHOPE – International Association of Internet Hotlines

INTERPOL – Organisation internationale de police criminelle

IOCTA – Évaluation de la menace que représente la criminalité organisée sur l'internet

IWF – Internet Watch Foundation

LIBE – Commission des libertés civiles, de la justice et des affaires intérieures

MVNO – Opérateur de réseau mobile virtuel

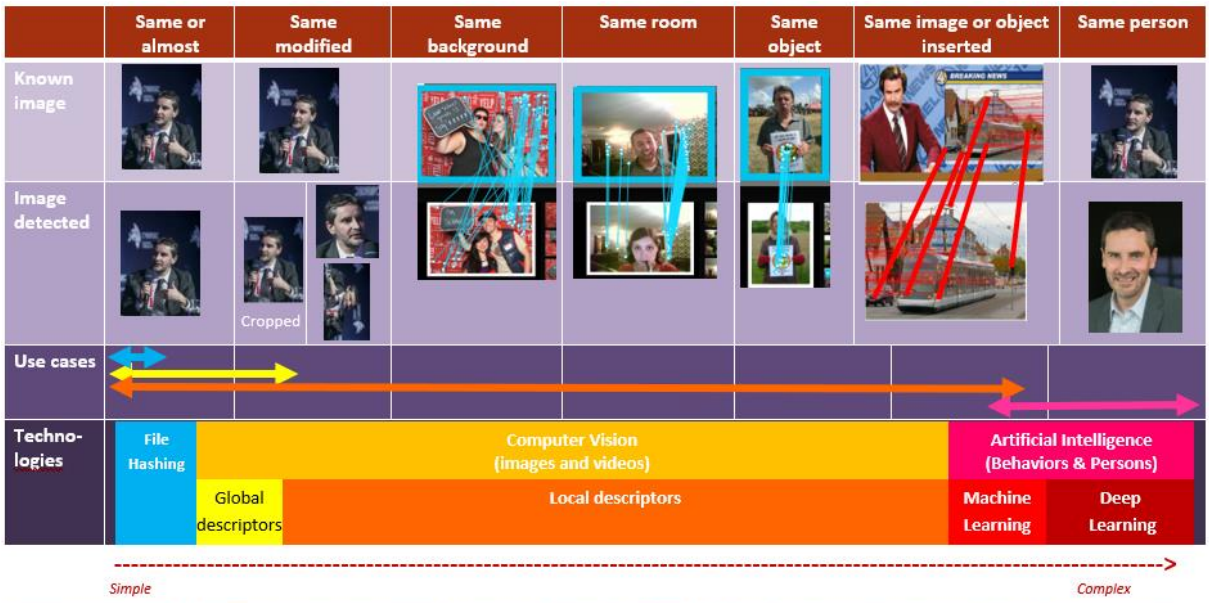
NCMEC – National Center for Missing & Exploited Children

OPSC – 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

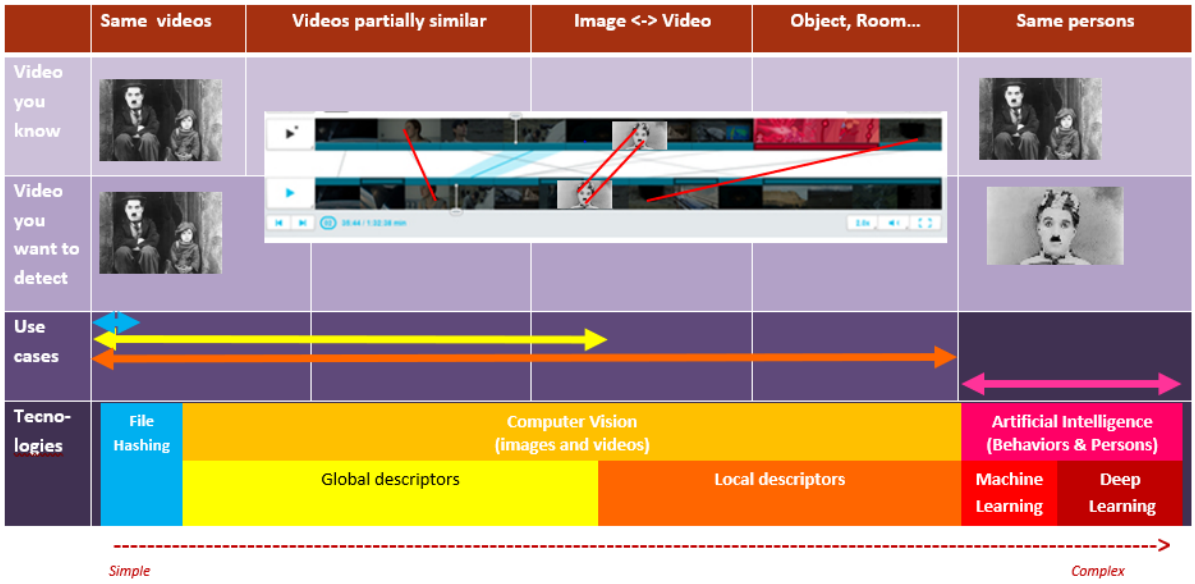
OTT – Services par contournement

6. ANNEXE

1. Tour d'horizon schématique des technologies de détection du contenu visuel dans des images et des vidéos.



How to read this diagram: File hashing technology applies only to detect the same file, this is why the arrow in blue applies only to detect "same or almost". As the file hashing technology cannot detect images with minor changes (change of 1 pixel), the arrow is short. "Global descriptors" applies well to detect same images and can also detect images with partially the same content. "Local descriptors" is efficient to detect all the scenarios (same, similar, modified etc.). "Artificial intelligence" can cover many use cases, more than what is shown on this diagram, but it is also more complex to use than computer vision technology.



How to read this diagram: Same as in section 3. The range of application of each of these technologies is indicative. Also, the range is not indicative of the level of adoption. For instance, file hashing is shown with the smallest range on this table, but it is in practice much more broadly used than the other technologies.

2. Sources complémentaires :

- https://www.culture.gouv.fr/ ou https://www.culture.gouv.fr/Sites-thematiques/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique/Travaux/Missions/Mission-du-CSPLA-sur-les-outils-de-reconnaissance-des-contenus-proteges-par-les-plateformes-de-partage-en-ligne-etat-de-l-art-et-propositions – Rapport publié en 2020 par le ministère français de la Culture à propos de la directive sur le droit d'auteur ; la vision par ordinateur y est décrite comme une technologie mature et abordable pour les organisations de toute taille.
- Lignes directrices concernant l'application du 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 ; dispositions sur le « recueil de données » et la « prévention ».

- **B. Recueil de données**
- 20. Le Comité engage vivement les États parties à se doter d'un mécanisme chargé de recueillir des données sur toutes les situations relevant du Protocole facultatif, d'analyser les informations ainsi obtenues, de suivre l'évolution des situations observées et de réaliser des études d'impact.
- Il est important que la collecte d'informations soit le fruit d'une collaboration entre toutes les parties intéressées, notamment les bureaux nationaux de statistique et les organismes de protection de l'enfance, et que les données soient centralisées afin qu'il n'y ait pas d'incohérences ou de contradictions dans les informations dont disposent les différents organismes publics. Le Comité recommande en particulier aux États parties :
- a) De ventiler les données pour faire apparaître comment différents groupes d'enfants sont touchés par les infractions visées. Au minimum, les données devraient être ventilées par sexe et âge de la victime et par type d'exploitation ;
- b) De recueillir des données sur la manière dont les enfants accèdent aux médias numériques et sociaux et les utilisent, sur les incidences que ces médias ont sur leur vie et leur sécurité, et sur les facteurs qui influent sur leur capacité de faire face aux dangers que l'utilisation des TIC leur font courir ;
- c) De recueillir des données sur le nombre d'infractions signalées, le nombre de personnes poursuivies, déclarées coupables et condamnées, et aussi, de préférence, sur les réparations accordées, en les ventilant par nature de l'infraction (infractions commises en ligne et infractions commises hors ligne), catégorie à laquelle l'auteur appartient, relation entre l'auteur et la victime, et sexe et âge de la victime ;
- d) De faire en sorte, si les données sont recueillies au niveau régional ou local (par exemple, par les municipalités), que les mêmes indicateurs et le même système soient utilisés.
- 21. Les données devraient toujours être recueillies dans le respect du droit des enfants à la vie privée.

- **C. Prévention de la vente et de l'exploitation sexuelle d'enfants en ligne**
- 37. Les États parties devraient prendre des mesures pour prévenir et combattre la vente, l'exploitation sexuelle et les abus sexuels sur enfants commis en ligne. Ils devraient notamment s'assurer que les lois et politiques nationales couvrent comme il se doit toutes les manifestations de la vente, de l'exploitation sexuelle et des abus sexuels dont les enfants peuvent être victimes, y compris les infractions commises au moyen des TIC ou facilitées par ces technologies.
- 38. Les États parties devraient faire des analyses et mener des recherches sur les infractions commises en ligne, suivre l'évolution du problème afin de mieux le comprendre et décider des mesures à prendre en étroite collaboration avec les industries et les organisations concernées.
- …
- 41. Étant donné que les images, vidéos et autres contenus représentant des abus pédosexuels peuvent rester en ligne indéfiniment, le Comité appelle l'attention des États parties sur le fait que la diffusion de ce type de matériel, outre qu'elle prolonge le tort causé aux victimes, contribue à présenter l'enfant comme un objet sexuel et risque de conforter les personnes qui ont une attirance sexuelle pour les enfants dans l'idée que cette attirance est « normale » puisque beaucoup la partagent. Le Comité demande donc instamment aux États parties de veiller, dans le cadre de leurs mesures de prévention, à ce que les fournisseurs d'accès à Internet contrôlent ce qui est publié en ligne et bloquent et suppriment les contenus incriminés.
- 42. Le Comité appelle l'attention des États parties sur la nécessité de lutter contre la pratique du « sexting » (envoi à des tiers de messages sexuellement explicites et autoproduits au moyen d'un téléphone portable) par les enfants. Dans bien des cas, c'est la pression de leurs pairs qui pousse les jeunes à se livrer à cette pratique, que les adolescents considèrent de plus en plus comme « normale ». Or, si en soi le sexting n'est pas nécessairement illégal, ni même répréhensible, il n'est pas sans risques. Les contenus sexualisés envoyés par « sexto » peuvent facilement se propager en ligne et hors ligne sans le consentement de l'enfant ou contre son gré, peuvent être très difficiles à faire disparaître, et sont susceptibles d'être utilisés à des fins d'intimidation et d'extorsion sexuelle, et donc d'avoir sur l'enfant des conséquences graves et traumatisantes pouvant aller jusqu'au suicide. Le sexting doit faire l'objet d'une attention particulière, et le Comité engage les États parties à se doter d'une législation qui protège clairement les enfants et à mettre l'accent sur la prévention en sensibilisant ceux-ci aux graves conséquences que peut avoir la diffusion d'images d'autrui et de soi-même.

- La Recommandation Environnement numérique (CM/Rec(2018)7, paragraphes 51 à 66) comprend les mesures ci-après relatives aux matériels d'abus sexuels sur des enfants :

Mesures relatives aux matériels d'abus sexuels sur des enfants

61. Les interventions en matière de politiques relatives aux matériels d'abus sexuels d'enfants devraient être axées sur les victimes, la priorité absolue devant être d'identifier, de localiser et de protéger les enfants qui figurent sur ce type de matériels, et de leur proposer des services de réadaptation.

62. Les États devraient mener une action de surveillance permanente pour vérifier si des matériels d'abus sexuels d'enfants sont hébergés sur le territoire relevant de leur juridiction et la manière dont ils sont hébergés, et charger leurs services répressifs d'établir des bases de données d'empreintes numériques ou « *hashes* » , dans le but d'accélérer l'identification et la localisation des enfants victimes d'exploitation ou d'abus sexuels, et d'appréhender les auteurs de ces actes.

63. Les États devraient amener les entreprises commerciales à apporter une assistance technique aux services répressifs, notamment en fournissant l'équipement et l'aide technique nécessaires, pour les aider à identifier les auteurs de crimes contre les enfants et à rassembler les preuves nécessaires pour les poursuites pénales.

64. Compte tenu des technologies existantes et sans préjudice de la responsabilité des intermédiaires internet, et de leur exemption des obligations générales de surveillance, les États devraient exiger des entreprises commerciales qu'elles prennent des mesures raisonnables, proportionnées et efficaces pour s'assurer que leurs réseaux ou services en ligne ne sont pas détournés à des fins criminelles ou à d'autres fins illégales pouvant nuire aux enfants, en relation, par exemple, avec la production, la diffusion, l'offre, la publicité ou le stockage en ligne de matériels d'abus sexuels d'enfants ou d'autres formes d'abus en ligne sur des enfants.

65. Les États devraient obliger les entreprises commerciales concernées à recourir à des listes d'empreintes numériques pour s'assurer que leurs réseaux ne sont pas détournés pour stocker ou diffuser des images d'abus sexuels d'enfants.

66. Les États devraient obliger les entreprises commerciales et les autres parties prenantes concernées à prendre rapidement toutes les mesures nécessaires pour garantir la disponibilité des métadonnées relatives à tout contenu ayant trait à l'exploitation et aux abus sexuels concernant des enfants trouvé sur des serveurs locaux, à les tenir à la disposition des services répressifs, à supprimer ces contenus et à restreindre l'accès à ces contenus localisés sur des serveurs situés hors de leur juridiction en attendant qu'ils soient supprimés.