La traite des êtres humains en ligne et facilitée par les technologies

Résumé et recommandations

GRETA
Groupe d'Experts
sur la lutte
contre la traite
des êtres humains

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

La traite des êtres humains en ligne et facilitée par les technologies

Résumé du rapport et recommandations

Rapport préparé par
Dr Paolo Campana
Professeur Agrégé, Université de Cambridge
Royaume-Uni

Avril 2022

Conseil de l'Europe

Les points de vue exprimés dans cet ouvrage n'engagent que le ou les auteurs et ne reflètent pas nécessairement la ligne officielle du Conseil de l'Europe.

Edition anglaise:
Online and technology-facilitated trafficking in human beings

Toute autre correspondance relative à ce document doit être adressée au secrétariat de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains
trafficking@coe.int

Photos: Shutterstock

Cette publication n'a pas fait l'objet d'une relecture typographique et grammaticale de l'Unité éditoriale du SPDP

Imprimé aux ateliers du Conseil de l'Europe

Table des matières

Abréviations utilisées dans le texte

ASW :	Adult Service Website / Site web du service pour adultes
CdE :	Conseil de l'Europe
CID :	Criminal Investigation Department / Département d'enquête criminelle
CSE :	Child Sexual Exploitation / exploitation sexuelle des enfants
CV :	Curriculum Vitae
EAW :	European Arrest Warrant / Mandat d'arrêt européen
ECE :	Equipe commune d'enquête
EIO :	European Investigation Order / Enquête européenne en matière pénale
FAI :	Fournisseur d'accès internet
GDPR :	General Data Protection Regulation / RGDP : Règlement général sur la protection des données
HDD :	Hard Disk Drive / Unité de disque dur
IA :	Intelligence artificielle
JIT :	Joint Investigation Team
JTA :	Joint Training Activities / Activités de formation conjointes
MLA :	Mutual Legal Assistance / Entraide judiciaire
ONG :	Organisation non-gouvernementale
OSINT :	Open Source Intelligence / Renseignements issus de sources ouvertes
TEH :	Traite des êtres humains
TIC :	Technologies de l'information et de la communication
TOR :	The Onion Router
UE :	Union éuropénne
VOIP :	Voice over Internet Protocol / Voix sur IP

Introduction

Internet et, plus généralement, les technologies de l'information et de la communication (TIC) contribuent largement à façonner notre vie. La pandémie de Covid-19 a fait ressortir à quel point internet et les TIC sont désormais présents dans nos activités et nos interactions sociales, et elle a même accéléré ce phénomène. La criminalité ne déroge pas à la règle et cela concerne aussi la traite des êtres humains.

Il est évident que les technologies posent de nouveaux défis et ouvrent de nouvelles perspectives aux services répressifs et aux Organisations non-gouvernementales (ONG). Cependant, la base d'informations factuelles sur la traite des êtres humains en ligne et facilitée par la technologie reste limitée et parcellaire. À l'heure actuelle, les informations disponibles les plus probantes proviennent d'une série d'études plutôt restreinte, généralement fondées sur un petit nombre d'entretiens avec des policiers et des personnes travaillant pour des ONG, souvent menés dans un nombre de pays très réduit, et sur quelques rapports d'organisations internationales. La présente étude ne se limite pas à quelques informations empiriques, mais présente une analyse de la traite en ligne et facilitée par la technologie fondée sur des informations factuelles recueillies de manière systématique auprès des États parties signataires de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains. Ces informations factuelles ont été complétées par des données provenant d'ONG qui viennent en aide aux victimes de la traite, et d'entreprises de technologie.

La présente étude s'inscrit dans un cadre relativement large. Elle évalue dans quelle mesure la technologie influe sur la traite des êtres humains et explore les modes opératoires des trafiquants en matière de traite en ligne et facilitée par la technologie. Son principal objectif consiste à explorer les difficultés juridiques et opérationnelles que les États parties et, dans une moindre mesure, les ONG rencontrent à chaque étape de la lutte contre la traite en ligne et facilitée par les TIC : la détection, les enquêtes et les poursuites, ou l'identification des victimes et la sensibilisation des groupes à risque. L'étude explore également une autre dimension capitale, à savoir les stratégies, les outils et les « bonnes pratiques » adoptés par les États parties et les ONG pour surmonter ces difficultés et renforcer leur action contre la traite en ligne et facilitée par la technologie. Le présent travail met en relief les similitudes entre les pays tout comme des expériences propres à chaque pays. Une attention particulière est portée à la formation, car il est tout aussi important d'investir dans le capital humain que dans les ressources technologiques.

La présente étude répond à l'intérêt manifesté de longue date par le Conseil de l'Europe – et le GRETA – pour les liens existants entre les technologies et la traite des êtres humains. Outre une évaluation systématique de la base d'informations factuelles disponible à ce jour, elle vise à fournir aux membres du GRETA et à d'autres entités un outil pour effectuer de prochaines évaluations et suivre l'évolution des technologies et des comportements.

Méthodologie

Les informations factuelles mentionnées dans la présente étude ont été recueillies à l'aide d'un questionnaire novateur, comprenant des questions ouvertes et fermées. Ce questionnaire existe en trois versions : une version longue pour les États parties (40 questions) et deux versions plus courtes pour les ONG (14 questions) et les entreprises de technologie (11 questions). Pour concevoir ce questionnaire, une analyse contextuelle a été réalisée entre octobre et décembre 2020 à partir d'un large éventail de sources : des organisations internationales, des universités, des organisations non gouvernementales et des associations caritatives ainsi que des acteurs du secteur privé (pour en savoir plus, voir annexe A). Le questionnaire a été élaboré de janvier à mars 2021, en consultation avec le Conseil de l'Europe et les membres du GRETA. Les réponses de 40 États parties[1], 12 ONG[2] et 2 entreprises de TIC[3] ont été reçues entre juin et juillet 2021 (une réponse tardive est parvenue au Secrétariat du Conseil de l'Europe en septembre 2021). Des analyses ont ensuite été menées entre juin et septembre 2021. Le calendrier était relativement serré pour effectuer une étude couvrant un large éventail de questions, de pays et d'entités. L'étude offre l'évaluation détaillée d'une grande base d'informations factuelles, mais elle n'est en aucun cas exhaustive et présente certaines limites. Celles-ci sont décrites dans le texte, le cas échéant.

Enfin, la présente étude suit Mark Latonero (2012 : 9-10) dans sa définition des technologies de l'information et de la communication, en particulier « celles constituant des environnements numériques en réseau. Les technologies qui permettent aux utilisateurs d'échanger des informations numériques par réseau englobent l'internet, les réseaux sociaux en ligne et les téléphones portables ».

La technologie est partie pour durer – et avec elle, des changements structurels dans la façon dont les criminels agissent ; de nouvelles perspectives se dessinent et des vulnérabilités existantes s'aggravent. Il est donc nécessaire que les États parties s'adaptent et dotent leurs services répressifs et leur système de justice pénale de capacités en phase avec cet environnement en (constante) évolution. À cet effet, la présente étude propose des recommandations fondées sur des informations factuelles.

[1] L'Albanie, l'Arménie, l'Autriche, l'Azerbaïdjan, la Bosnie-Herzégovine, le Bélarus, la Belgique, la Bulgarie, la Croatie, Chypre, le Danemark, l'Estonie, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, l'Islande, l'Irlande, la Lettonie, la Lituanie, le Luxembourg, Malte, la République de Moldova, Monaco, le Monténégro, les Pays-Bas, la Macédoine du Nord, la Norvège, la Pologne, le Portugal, la Roumanie, Saint-Marin, la Slovaquie, la Slovénie, l'Espagne, la Suède, la Suisse, l'Ukraine et le Royaume-Uni.

[2] Astra (Serbie) ; Différents et égaux (Albanie) ; FIZ (Suisse) ; Hope Now (Danemark) ; Jesuit Refugee Service; (Macédoine du Nord) ; KOK (Allemagne) ; La Strada (République de Moldova) ; La Strada International (Europe); Centre pour les droits des migrants (Irlande) ; Praksis (Grèce) ; Schweizer Plattform gegen Menschenhandel (Suisse) ; Sustainable Rescue Foundation (Pays-Bas).

[3] Facebook et IBM.

Résumé du rapport

L'impact de la technologie sur la traite des êtres humains

L'impact de la technologie sur la traite des êtres humains est particulièrement préoccupant dans deux phases du processus de traite : le **recrutement** et l'**exploitation**. Les États parties ont fourni des informations qui mettent en lumière la place « grandissante » de la technologie dans le domaine de la traite, et la majorité d'entre eux qualifient aujourd'hui l'impact de la technologie sur la traite de « très important » ou d'« important ».

Les États parties ont mentionné l'**importance croissante** des contenus, annonces et sites/applications en ligne pour la recherche d'emploi, de même que l'importance croissante de la socialisation et des échanges personnels en ligne. Ces phénomènes **ouvrent des perspectives** pour les trafiquants et **accroissent les vulnérabilités existantes**. La technologie a changé la manière dont les gens entretiennent des relations et cela se répercute sur la criminalité, y compris la traite des êtres humains. Il s'agit d'un **changement structurel** auquel les services répressifs et les systèmes de justice pénale doivent s'adapter.

La technologie peut intervenir pendant la phase de **recrutement** en facilitant l'identification et la localisation des victimes potentielles ainsi que la prise de contact. Différents mécanismes entrent en jeu selon la forme d'exploitation.

S'agissant du **recrutement aux fins d'exploitation sexuelle**, plusieurs États parties ont observé l'existence d'offres d'emploi liées à la traite et détecté des recrutements par le biais de plateformes de réseaux sociaux et d'applications de rencontre. Une stratégie courante est la méthode des loverboys). Il s'agit d'une méthode de recrutement en ligne selon laquelle le trafiquant repère et contacte une victime potentielle sur une plateforme en ligne et apprend à connaître ses loisirs et centres d'intérêt ainsi que sa situation personnelle et familiale. Le

trafiquant offre ensuite empathie et soutien à la victime potentielle dans le cadre d'une relation romantique, dans le but de gagner sa confiance et de prendre le contrôle sur elle.

Dans plusieurs pays, de nombreux cas de **chantage** à l'encontre des victimes ont été constatés. Cela se fait souvent en recueillant au départ des données « compromettantes » sur les victimes – par exemple, en demandant à la personne des photographies ou des vidéos d'elle-même nue – puis en utilisant ces données pour la contraindre se livrer à la prostitution.

Pendant la **phase d'exploitation**, la technologie peut faciliter la **commercialisation** des services sexuels fournis par les victimes de la traite. Plusieurs pays font mention de sites internet utilisés pour proposer des services sexuels. Parmi les annonces figurent des services fournis par des victimes de la traite. En outre, si les vidéos diffusées en direct sont souvent liées à des abus sexuels sur des enfants, une poignée de pays a suggéré qu'elle pouvait concerner des victimes de traite d'âge adulte.

De plus, la technologie peut être utilisée pour **coordonner des activités.** Elle permet essentiellement de séparer le lieu où l'activité sexuelle est pratiquée de celui où la coordination se déroule. Cela a des implications importantes pour les services répressifs.

Certains pays ont démontré l'existence d'outils technologiques employés par les trafiquants pour **surveiller et contrôler** les victimes pendant la phase d'exploitation. Le chantage et l'utilisation d'informations compromettantes à l'encontre des victimes peuvent également servir à exercer un contrôle durant cette phase.

Les **nouvelles tendances** relevées par plusieurs pays en matière d'exploitation sexuelle englobent l'essor des « webcams en direct » et des applications de chat vidéo « prépayées », et le recours croissant à des applications pour contrôler les victimes. Ces webcams et ces applications de chat vidéo peuvent être utilisées pour diffuser en direct des actes sexuels réalisés par des victimes de traite. Quelques pays ont noté que la pandémie de Covid-19 avait augmenté les possibilités pour les trafiquants d'établir des contacts en ligne avec des personnes vulnérables.

Dans le contexte de la traite aux fins d'**exploitation par le travail**, des données fournies par des États parties montrent que les technologies de l'information et de la communication (TIC) sont surtout employées pour **recruter** des victimes, en particulier au moyen d'**offres d'emploi en ligne.** Ces offres ne sont pas seulement publiées dans des sites spécifiquement consacrés à l'emploi, mais également diffusées et transmises par la voie des réseaux sociaux dans des groupes spécialisés dans la recherche d'emploi et des groupes d'entraide en ligne. Plusieurs pays ont souligné l'importance des pages web destinées à favoriser les échanges d'informations entre travailleurs migrants comme espace de recrutement ciblé par les trafiquants.

Une **nouvelle tendance** à propos de l'exploitation par le travail, relevée par certains pays, concerne la hausse des recrutements par le biais d'internet et des réseaux sociaux. Cette tendance aurait été accélérée par l'épidémie de Covid-19. Si la technologie ne semble pas jouer un rôle notable dans la phase d'exploitation, certains pays ont souligné que l'« économie à la tâche » et, particulièrement, les plateformes de livraison augmentent les possibilités d'exploiter les victimes de traite.

Rien ne prouve que le ***dark web*** joue un rôle très important dans les affaires de traite où les victimes sont adultes (la diffusion de matériels relatifs à l'exploitation sexuelle d'enfants dépasse le cadre de la présente étude). Les **cryptomonnaies** ne semblent pas non plus très employées dans les affaires de traite (en revanche, elles sont utilisées pour payer des services de diffusion en direct d'abus sexuels sur des enfants).

Les **ONG** dressent un tableau similaire à celui des États parties. Elles ont constaté qu'internet et les réseaux sociaux étaient employés à tous les stades de la traite des êtres humains et

particulièrement a) le recrutement ; b) l'exploitation ; c) l'exercice d'une emprise et d'une pression sur les victimes. En outre, les trafiquants peuvent utiliser les TIC, notamment des réseaux sociaux et des applications cryptées, pour garder le contact avec les victimes de traite lorsque celles-ci ne se trouvent plus en situation d'exploitation – souvent pour les empêcher de déposer plainte et de se tourner vers la justice.

Les nouvelles tendances qui se dégagent des éléments transmis par les ONG suggèrent une augmentation de l'exploitation des mineurs par la voie **des webcams et des réseaux sociaux**. Selon certaines sources, les trafiquants commenceraient à utiliser les **jeux vidéo** pour entrer en contact avec des victimes potentielles.

Enfin, les données disponibles suggèrent que l'utilisation de la technologie ne remplace pas les relations personnelles dans le monde réel, mais les complète. La technologie et les échanges traditionnels doivent être plutôt considérés comme intégrés l'un à l'autre.

Difficultés dans la détection, les enquêtes et les poursuites concernant la traite facilitée par les technologies

Défis de la détection

Il reste très difficile de détecter les cas de traite en ligne et facilitée par la technologie, et d'identifier les victimes. Les États parties mettent en avant un certain nombre de défis à relever :

- Le volume en constante augmentation des activités et échanges en ligne. Le maintien de la sécurité sur internet mobilise énormément de ressources et doit obéir à des contraintes juridiques (comme des lois sur la protection de la vie privée et des restrictions à l'utilisation des robots d'indexation dans certains pays) ;
- Le volume des annonces en ligne (ouvertes et classées) proposant des services sexuels et non sexuels est souvent trop important pour faire l'objet de recherches manuelles ;
- Les difficultés à identifier à la fois les trafiquants et les victimes, car ils peuvent utiliser des surnoms et des pseudonymes lorsqu'ils évoluent en ligne et se servir de logiciels d'anonymisation (par exemple, des réseaux privés virtuels ou VPN) ;
- Communications cryptées entre les trafiquants et les victimes. Leurs conversations se déroulent dans des groupes fermés ;
- Comportement fluctuant des usagers d'internet ;
- Difficultés à classer les annonces en ligne de façon à distinguer celles qui sont liées à la traite, à la fois à des fins d'exploitation sexuelle et non sexuelle. Les drapeaux rouges visant à signaler les annonces liées à l'exploitation sexuelle et à l'exploitation par le travail restent rares ou ne sont pas systématiquement employés ;
- Absence d'unités spécialisées au sein de la police et/ou manque d'enquêteurs spécialisés en matière de traite et dotés de compétences informatiques avancées. Manque de policiers formés pour mener des opérations d'infiltration sur le web. Les cyber-opérations peuvent être longues et fastidieuses ;
- Lenteur des procédures d'envoi de demandes aux sociétés de réseaux sociaux et absence de réponses de certaines d'entre elles ;
- Courtes périodes de conservation des données pour les adresses IP et difficultés à y accéder.

Difficultés dans les enquêtes

Le **cryptage des données** constitue l'un des plus grands défis pour les États parties (score de gravité de 80 sur 100). Il est suivi du volume important des données (71), de la rapidité de l'évolution technologique (66), du manque d'équipement technique (63), d'outils législatifs inadéquats (61), des connaissances techniques insuffisantes des services répressifs (53) et de l'aide insuffisante apportée par le secteur privé (46).

Les protocoles de cryptage des données inclus dans les applications et les services en ligne populaires sont souvent jugés problématiques. Le cryptage limite également la possibilité de surveiller les communications. Quelques pays ont évoqué l'existence d'outils permettant de décrypter certains types de dispositifs. Cependant, il s'agit d'un paysage en constante évolution qui nécessite des investissements (importants) à la fois en formation et en logiciels. Parmi les efforts déployés pour résoudre ce problème figure la mise en place d'unités/centres de lutte contre la cybercriminalité, chargés de travailler sur les technologies de décryptage. En outre, il est utile de regrouper les ressources à l'échelle supranationale pour développer des produits technologiques tels que les logiciels de décryptage et les robots d'indexation.

Les dispositifs de communications électroniques et de TIC engendrent un **volume important de données en croissance constante** qui, à son tour, fait peser une lourde charge sur les enquêteurs. Cette charge se répercute sur la capacité des enquêteurs à extraire les données et à les examiner soigneusement, qui nécessite elle-même des logiciels spécialisés ainsi qu'une formation spécifique sur la systématisation et l'exploration de tels volumes de preuves.

Il existe un large consensus sur l'impérieuse nécessité de renforcer la capacité à traiter des volumes importants de **preuves électroniques**. En outre, cette capacité doit être constamment actualisée. Certains pays ont fait observer que les difficultés ne provenaient pas seulement du volume croissant des données issues des plateformes en ligne et des réseaux sociaux, mais aussi des **comportements fluctuants** de leurs utilisateurs.

Plusieurs pays ont insisté sur le problème du manque d'**équipement technique**. Les logiciels et le matériel spécialisés sont de plus en plus onéreux et exigent des mises à jour constantes et des accords de licence coûteux pour suivre le rythme de l'évolution technologique. Cette **nécessité de suivre le rythme de l'évolution technologique** grève considérablement les budgets de la police. Plusieurs pays, quel que soit le niveau de leur PIB (produit intérieur brut), ont soulevé cette question.

Il est tout aussi important d'investir dans le capital humain que dans les logiciels et le matériel, si n'est plus, notamment car les services répressifs doivent **améliorer leurs connaissances techniques**. D'après les informations fournies, les connaissances doivent être améliorées dans plusieurs domaines a) l'émergence de nouvelles tendances et l'évolution de l'utilisation de la technologie ; b) l'arrivée de nouveaux services et de nouvelles applications sur un marché informatique qui se caractérise par des changements rapides et c) le développement de nouveaux protocoles de sécurité et de nouvelles méthodes de cryptage. Il est essentiel que les connaissances soient diffusées intelligemment au sein d'une organisation. En effet, l'absence d'agents spécialisés au niveau local peut entraîner un **engorgement (blocage) des services d'investigation**, s'il est continuellement fait appel à l'assistance d'une unité centralisée (débordée).

Plusieurs pays ont souligné la nécessité de fournir des formations **supplémentaires à tous policiers,** y compris des connaissances sur la technologie et son fonctionnement. Parallèlement, des formations adéquates doivent être dispensées à l'ensemble des policiers concernés sur l'obtention et le traitement de preuves électroniques, et ce thème devrait faire partie intégrante des programmes de formation des policiers. Les affaires les plus complexes peuvent nécessiter de monter des équipes dotées de connaissances pluridisciplinaires (en regroupant, par exemple, des enquêteurs, des spécialistes de la finance et des experts en cybercriminalité).

Des problèmes supplémentaires découlent de certaines **obligations de conservation des données** imposées aux fournisseurs d'accès à internet (FAI) qui ne sont pas adéquates, et de l'application de la législation relative au respect de la vie privée, en ce qui concerne, par exemple, les robots d'indexation.

Difficultés dans les poursuites

D'une manière générale, il semble que les poursuites soient moins difficiles à conduire que les enquêtes, puisque seule la question de l'« obtention de preuves auprès d'autres pays » a un score légèrement supérieur à 50 (sur 100). Elle est suivie du manque de formation des procureurs (40), des outils législatifs inadaptés (38) et de l'assistance du secteur privé (33). L'extradition des suspects (28) et l'attribution de la compétence juridictionnelle (16) semblent jouer un rôle mineur.

La **formation adéquate des procureurs** est considérée comme indispensable pour s'assurer que les dossiers de traite facilitée par les TIC sont solides, que les preuves électroniques sont recueillies et employées correctement, et que les dossiers sont présentés aux juges et aux jurés en bonne et due forme. Certains États parties ont mentionné des affaires dans lesquelles les procureurs ne maîtrisaient pas les procédures à suivre pour demander des données électroniques aux entreprises privées ou obtenir des preuves et la coopération d'autres pays (par exemple, par le biais d'une équipe commune d'enquête [ECE] et d'une décision d'enquête européenne).

Certains États parties ont soulevé la question du traitement des documents électroniques, en particulier dans le cadre des **obligations liées au Règlement général sur la protection des données (RGPD)**. Des préoccupations ont également été soulevées autour de la réglementation internationale relative à la protection des données, qui peut entraver la collecte, la conservation et le traitement d'informations obtenues par des moyens d'investigation technologiques (telles que les robots d'indexation).

Des défis ont été relevés à propos des adresses IP et des preuves électroniques. Dans la mesure du possible, les adresses IP doivent être liées à des pseudonymes et à des utilisateurs. Toutefois, les pseudonymes peuvent être modifiés à tout moment et sont souvent utilisés par les suspects de manière interchangeable.

Un autre problème porte sur la **présentation des preuves** devant des jurés (et des juges), car les preuves techniques peuvent être complexes dans les affaires facilitées par les TIC et doivent souvent être présentées par un expert. Il peut donc s'avérer particulièrement utile de

développer l'expertise interne des agents sur la manière de présenter des preuves électroniques de façon efficace et précise.

Difficultés dans la coopération internationale

Pour la majorité des États parties, l'un des principaux obstacles à la coopération internationale est le long délai de traitement des **demandes d'entraide judiciaire**. Les procédures d'entraide judiciaire sont considérées comme lentes, parfois imprévisibles, et elles devraient s'appuyer sur des modèles convenus à l'échelle internationale.

La **coopération en dehors du cadre juridique de l'Union européenne** est perçue comme un processus chronophage et laborieux, en raison du manque d'harmonisation entre les différents systèmes juridiques et d'éléments d'imprévisibilité et d'incohérence. Des procédures opérationnelles plus claires, des échanges réguliers renforcés entre les points de contact, des obligations d'entraide judiciaire bien définies et la tenue de discussions dès le début de la coopération contribueraient à optimiser le processus.

La technologie permet aux réseaux criminels d'organiser et de contrôler les activités d'exploitation à distance – par exemple depuis un autre pays, sachant souvent que les demandes de coopération judiciaire ne seront pas satisfaites en temps voulu, si tant est qu'elles le soient. Il est donc nécessaire d'améliorer les accords, voire d'en conclure, avec les pays d'origine des victimes s'ils sont situés en dehors de l'Union européenne.

Les difficultés de traitement des demandes d'entraide judiciaire peuvent également résulter du manque **de personnel suffisamment formé** pour compiler et traiter les demandes, et de l'utilisation de technologies obsolètes.

Les preuves électroniques ne permettent pas toujours de connaître le lieu exact et notamment le pays où sont stockées les données et, partant, la juridiction dont elles relèvent, si bien qu'il est difficile d'élaborer une demande d'entraide judiciaire.

Des appels ont été lancés en faveur d'un cadre juridique commun qui autoriserait l'**échange rapide de preuves numériques**. Plusieurs pays ont exprimé leurs préoccupations à propos de l'absence de réglementation homogène en matière de **conservation de données**, ce qui entrave l'échange de preuves électroniques. D'une manière générale, les États parties ont souligné la nécessité de mettre en place un cadre plus complet pour réglementer la conservation et le transfert des preuves électroniques, et un cadre juridique commun pour remplacer les accords de coopération bilatéraux ad hoc qui existent actuellement entre les États et les entreprises privées détentrices des données (voir également ci-dessous). Les États parties ont insisté sur la nécessité d'améliorer les échanges de données pendant les enquêtes.

Difficultés dans la coopération avec les entreprises privées

Plusieurs pays ont indiqué que les FAI, les hébergeurs de contenu et les entreprises de réseaux sociaux étaient généralement coopératifs s'agissant des questions liées à la traite et à l'exploitation sexuelle des enfants. Toutefois, un certain nombre de défis ont été identifiés. Ils concernent :

- **L'obtention d'une réponse rapide** de la part de certains FAI et hébergeurs de contenu. La prise de contact avec les hébergeurs, qui exige l'envoi de commissions rogatoires par l'intermédiaire des autorités concernées, peut engendrer de longues attentes, avec le risque que le contenu recherché ne soit détruit avant que la demande ne soit traitée ;
- **La clarification des conditions juridiques** qui régissent le fonctionnement des entreprises TIC et des FAI. Certains pays s'inquiètent du fait que les FAI imposent parfois des formalités indues aux services répressifs et ne motivent pas ou n'expliquent pas suffisamment leurs refus ;
- **L'absence de point de contact désigné** au sein des entreprises privées. Les grandes entreprises présentes dans de multiples pays manquent souvent d'employés possédant les compétences linguistiques et juridiques pertinentes pour chaque pays dans lequel elles interviennent ;
- **Le manque de connaissance** des hébergeurs de contenus et des entreprises de réseaux sociaux concernant les agences nationales responsables de telle ou telle décision, par exemple le retrait de contenus illégaux. Il a été proposé de créer des « signaleurs de confiance » c'est-à-dire des organismes spécifiques qui seraient chargés de faire le lien avec les fournisseurs internationaux pour le retrait des contenus. Le signaleur de confiance aurait un canal de communication ouvert avec les entreprises et instaurerait une confiance mutuelle.

Informations communiquées par les ONG

D'une manière générale, les informations fournies par les ONG reprennent les thèmes abordés ci-dessus. Plus précisément, les ONG ont souligné les questions suivantes :

- **Les capacités insuffisantes** des services répressifs en matière de formation, d'équipement et de logiciels, et l'utilisation limitée des techniques spéciales d'enquête. Est également constatée l'absence de spécialisation des forces de l'ordre et du système judiciaire dans la traite liée à la technologie ;
- **L'évolution rapide du paysage technologique et du mode opératoire des trafiquants**. Il peut être difficile pour les professionnels de se tenir informés de l'évolution de la traite facilitée par les technologies, ce qui entrave leur capacité de détecter rapidement les cas de traite. Les connaissances sur le paysage technologique et les modes opératoires sont souvent cloisonnées ;
- **L'utilisation de forums privés, de salles de chat ou d'applications de discussions cryptées entre les auteurs de traite et les victimes.** Il est par conséquent difficile a) de détecter ces discussions et b) de s'en servir comme des preuves recevables devant un tribunal. Des ONG suggèrent que les applications et les salles de chat affichent des renseignements/avertissements sur une utilisation sûre des moyens de communication privés ;
- **Les règles de protection des données et de la vie privée** peuvent empêcher l'identification des victimes et des trafiquants. Le RGPD limite l'utilisation des technologies pour détecter les traces numériques laissées par les victimes et les auteurs d'infractions ;
- **L'absence de collaboration technologique interdisciplinaire** entre les entreprises privées, les organismes publics et les ONG pour exploiter pleinement le volume croissant de données sur la traite ;
- **L'absence de stratégie concernant les technologies** dans les plans d'action nationaux sur la traite ;

- **L'insuffisance des capacités, des ressources et des outils technologiques** au sein des ONG pour détecter régulièrement l'exploitation en ligne facilitée par la technologie ;
- **Des objectifs contradictoires** ou des approches différentes entre les ONG et les services répressifs.

Informations communiquées par les entreprises de technologie

Comme indiqué ci-dessus, seules deux entreprises ont fourni des réponses au questionnaire. Facebook a noté que les contenus relatifs à la traite étaient « rarement signalés » par les utilisateurs. IBM a noté que plusieurs obstacles compromettent la coopération avec les services répressifs, à savoir des problèmes relatifs à la légalité de cette coopération, en particulier eu égard à la confidentialité des données et à la complexité juridique découlant de compétences juridictionnelles multiples. IBM a également demandé des clarifications sur les autorisations juridiques internationales permettant de rassembler des données et de les partager avec les services répressifs compétents.

Stratégies et bonnes pratiques

Détection des cas de traite facilitée par les TIC

Les pays ont indiqué qu'ils appliquaient diverses stratégies pour détecter les cas de traite en ligne et facilitée par les TIC. Une stratégie largement évoquée est la **surveillance d'Internet**, y compris des forums et, dans certaines affaires, des réseaux TOR (*dark web*). Elle se conjugue avec l'utilisation de **renseignements issus de sources ouvertes (Open Source Intelligence ou OSINT)**, c'est-à-dire la collecte de données tirées des réseaux sociaux et d'autres sources en ligne accessibles au public, qui permettent de connaître le réseau de contacts d'une personne, ses conditions de vie et sa situation financière.

Certains pays ont créé des **« cyber-patrouilles » avec des agents spécialisés** chargés de mener des enquêtes OSINT sur internet. Certaines juridictions autorisent des infiltrations en ligne (cyber-infiltration).

Certains services répressifs utilisent des **outils de collecte automatique de données en ligne** spécifiquement conçus pour extraire des informations de sites web, pour identifier notamment les risques et la vulnérabilité sur les sites web pour adultes.

Liées aux enquêtes OSINT, des **techniques d'analyse des réseaux sociaux** sont utilisées pour comprendre et reconstruire le réseau de contacts d'un trafiquant et/ou d'une victime. Les **informations relationnelles** sont essentielles : les informations recueillies auprès de différentes sources peuvent être systématisées et utilisées pour **recomposer des réseaux criminels**, c'est-à-dire les relations entre les lieux, les trafiquants et les victimes.

Toutefois, les États parties n'ont pas tous indiqué qu'ils employaient des stratégies « proactives ». Certains d'entre eux ont déclaré que leurs enquêtes sur la traite facilitée par les TIC restaient « réactives ».

Plusieurs pays mettent en œuvre des **systèmes permettant aux internautes de signaler les contenus et les sites web** qu'ils soupçonnent d'être liés à des activités illégales, y compris l'exploitation sexuelle et l'exploitation par le travail. Ainsi, dans certains pays comme la France, les fournisseurs d'accès à internet (FAI) et les hébergeurs de sites web sont tenus d'aider les services répressifs à lutter contre la diffusion de matériels relatifs à des infractions spécifiques, telles que la traite. Ils doivent établir un dispositif bien visible et facilement accessible à l'aide duquel tous les internautes peuvent signaler tout contenu suspect.

Certains pays ont signalé le recours à des **campagnes de sensibilisation** pour améliorer la détection des cas de traite facilitée par les TIC. Ces campagnes visaient à sensibiliser les clients des sites web qui hébergent des offres de services sexuels sur le risque de rencontrer des victimes de traite (Belgique et Royaume-Uni) et à informer les internautes sur la recherche d'emplois en toute sécurité (Pologne et Bulgarie). Les autorités se sont appuyées sur les réseaux sociaux pour diffuser des messages ciblés, parfois en créant des annonces ciblées sur Facebook reliées à une ligne téléphonique de signalement.

Enquête sur les cas de traite facilitée par les TIC

Dans certains pays, les services répressifs mènent des **cyber-infiltrations** dans des réseaux criminels à l'aide de techniques secrètes et d'enquêtes sous couverture. Plusieurs d'entre eux ont souligné la nécessité de développer ces **enquêtes sous couverture** et, partant, d'investir dans la formation d'agents spécialisés. Chacun s'accorde à reconnaître l'importance d'acquérir des **logiciels spécialisés** et d'y avoir accès, ainsi que sur l'importance des mégadonnées et d'améliorer les capacités de traitement des celles-ci. Il est également essentiel de développer des outils qui permettent de télécharger les données de téléphones portables en contournant le mot de passe et de décrypter des conversations sur les applications de communication.

Il est largement considéré comme tout aussi essentiel d'**investir dans le capital humain** que d'investir dans le matériel technologique. L'investissement dans le capital humain peut signifier fournir aux forces de l'ordre une formation continue et des activités de développement fondées sur de bonnes pratiques locales et globales. Dans le même esprit, plusieurs pays ont relevé l'importance d'intégrer des enquêteurs spécialisés dotés de « connaissances numériques » dans les enquêtes sur la traite. Un modèle serait d'intégrer dans chaque unité spécialisée dans la lutte contre la traite des agents spécifiquement formés à la conduite d'enquêtes sur internet et les réseaux sociaux. Cela permettrait de créer des **groupes d'appui technique** pour les enquêteurs. Ces groupes pourraient être constitués de policiers assermentés ou non assermentés. Cette idée s'éloigne du modèle traditionnel de la police reposant uniquement sur des policiers assermentés, et reprend le principe – déjà appliqué par certains services de police – d'adjoindre des agents non assermentés pour occuper des fonctions plus techniques (par exemple des analystes).

Par ailleurs, des États parties soulignent l'intérêt d'un **travail d'enquête interinstitutionnel**, avec la participation et la coopération d'un large éventail d'organismes spécialisés, et du partage de connaissances entre les institutions. De la même façon, les pays préconisent d'**améliorer la coopération transfrontalière** en échangeant mutuellement

des agents avec les pays d'origine des victimes, par exemple. Au niveau opérationnel, certains pays notent que les enquêtes pourraient être facilitées en simplifiant la **préservation et l'accessibilité des preuves sur le plan transnational.**

Lors des enquêtes, il a été suggéré que les pays ne devraient pas se fier, de manière excessive, à une liste prescriptive d'indicateurs, par exemple pour identifier les annonces en ligne à haut risque, mais d'exploiter aussi des ensembles d'informations de différentes natures, à savoir les renseignements, les informations de source ouverte et les casiers judiciaires. L'**importance de l'analyse des réseaux et des données relationnelles** a été soulignée.

Bien qu'elle demande beaucoup de temps, l'**analyse stratégique** qui fait ressortir les tendances émergentes et des informations actualisées sur le mode opératoire des trafiquants (y compris les technologies et les sites web utilisés) présente un grand intérêt.

Dans le cadre d'enquêtes ou de poursuites liées à la traite, les technologies permettent également de **faciliter la collecte de preuves auprès des victimes** et donc d'alléger la charge qui pèse sur elles.

Favoriser la coopération internationale

Les États parties ont recensé les principes suivants pour favoriser la coopération internationale :

- Tirer parti des ressources disponibles dans les organismes tels qu'Europol et Eurojust et créer des équipes communes d'enquête pour les pays qui entrent dans le cadre juridique de l'Union européenne ;
- Établir des contacts avec les autres parties intéressées dès les débuts d'une enquête ;
- Développer une très bonne compréhension du contexte juridique et des possibilités de coopération avec un pays ou un ensemble de pays donnés ;
- Organiser des réunions de coordination pour échanger des renseignements et des preuves aussi facilement et rapidement que possible, et élaborer *d'emblée* une stratégie commune ;
- Élaborer une compréhension commune d'approches harmonisées et assurer l'interopérabilité transnationale des services répressifs au moyen de sessions de formation transnationales.

La coopération entre les autorités non policières, souvent négligée, peut être aussi pertinente que la coopération policière, en particulier dans la lutte contre la traite aux fins d'exploitation par le travail (par exemple, entre les corps de l'inspection du travail).

Identification et assistance des victimes

La **reconnaissance faciale** semble largement utilisée dans le cas de l'exploitation sexuelle des enfants. Toutefois, son utilisation semble plus limitée dans les autres domaines d'exploitation. Quelques pays ont mentionné des outils technologiques qui leur permettent d'identifier des victimes de la traite en exploitant les mégadonnées (principalement des robots d'indexation, mais aussi des outils de reconnaissance faciale employés dans des conditions plus strictes).

Pour identifier les cas de traite, plusieurs pays s'appuient sur des indicateurs (« **drapeaux rouges** ») ; néanmoins, ce sont des indicateurs « généraux » de traite et non des indicateurs spécifiques à la traite facilitée par les TIC. Bien qu'il existe un besoin clair d'élaborer des indicateurs spécifiques à la traite facilitée par les TIC, les autorités ont également mis en garde contre le fait de recourir uniquement et de façon excessive aux « drapeaux rouges ». Même lorsque des indicateurs sont spécifiquement élaborés pour identifier des victimes sur les sites web pour adultes, comme au Royaume-Uni, ils montrent des limites évidentes et s'utilisent de préférence en combinaison avec l'**analyse des réseaux sociaux et l'évaluation humaine** des preuves.

Les outils technologiques peuvent être très utiles pour effectuer la compression des données et gérer des volumes importants d'information ; toutefois, ils doivent être employés par des opérateurs chevronnés qui maîtrisent le thème/la question traitée (par exemple la traite). Le recours à l'intelligence artificielle et aux outils technologiques pour identifier les victimes n'est pas exempt de problèmes, y compris des préoccupations éthiques et un risque de discrimination (en cas de profilage fondé sur des critères discriminatoires ; voir plus loin).

Pour ce qui concerne les initiatives technologiques destinées à aider les victimes et à renseigner les populations à risque, les pays ont identifié des exemples de 1) dispositifs d'auto-signalement en ligne et des lignes téléphoniques d'assistance, dont une assistance numérique au moyen d'une fonction de chat ; 2) campagnes de sensibilisation en ligne, qui ciblent souvent des groupes à risque spécifiques (par exemple les demandeurs d'emploi) ; 3) applications et outils en ligne conçus pour un usage précis ; et 4) documents officiels rendus accessibles en ligne et traduits en plusieurs langues. Une bonne pratique consiste à collaborer avec des entreprises privées pour diffuser des **publicités sur les réseaux sociaux** (élaborées et sponsorisées conjointement avec des réseaux sociaux). Toutefois, les campagnes en ligne ne devraient pas remplacer le contact direct et personnel avec les individus vulnérables.

Informations communiquées par les ONG

Les ONG ont souligné l'importance de disposer **d'informations adéquates et actualisées** auxquelles peuvent aisément accéder en ligne les personnes soumises à la traite et celles vulnérables à l'exploitation et aux abus. Ces plateformes en ligne devraient également **permettre l'auto- identification** des victimes. Le tout devrait être accompagné de **campagnes de sensibilisation**.

Par ailleurs, les ONG ont insisté sur l'importance de développer les connaissances des organisations qui viennent en aide aux victimes, y compris les services de conseils, sur les risques liés aux TIC et, plus généralement, la traite facilitée par les nouvelles technologies. La **préservation des preuves électroniques** étant essentielle pour conduire une enquête solide, les conseillers et les ONG qui interviennent en premier lieu doivent impérativement connaître des méthodes de préservation des preuves électroniques (par exemple, en stockant les historiques des chats).

Les données fournies par les ONG montrent que les **« drapeaux rouges »** destinés à signaler les cas de traite facilitée par les TIC sont rarement employés. Les ONG indiquent

qu'elles utilisent des indicateurs standard, mais demandent une **révision de ces indicateurs** pour que les spécificités de la traite facilitée par les TIC soient prises en compte.

Les ONG ont présenté des exemples d'**initiatives technologiques** élaborées par leurs soins pour a) encourager les victimes à s'auto-signaler en ligne ; b) établir des contacts avec les populations à risque, par exemple pour rompre l'isolement des victimes et favoriser leur autonomie ; c) sensibiliser les groupes vulnérables et à risque, et rechercher de l'aide, au moyen d'applications et de sites web conçus à cet effet ; et d) organiser des campagnes de sensibilisation en ligne.

D'une manière générale, les ONG se tournent de plus en plus vers la technologie, mais leur niveau général reste « limité ». Chacun s'accorde à reconnaître que les ressources technologiques pourraient être davantage exploitées, en particulier pour diffuser des informations ; entrer en contact avec les victimes potentielles et établir le dialogue ; et recevoir des signalements et des déclarations.

Les ONG ont également soulevé des **questions cruciales** portant sur les initiatives et les outils technologiques, y compris l'importance des périodes d'essai pour les nouveaux outils et – avant toute chose – des preuves de leur efficacité (qui reste très limitée). Elles ont réclamé que les outils technologiques mis au point fassent l'objet d'une **évaluation et d'une analyse d'impact plus poussées**. En outre, la plupart du temps, aucune stratégie financière à long terme n'est mise sur pied pour promouvoir l'utilisation des outils produits, pas même des ressources qui permettraient de les actualiser. Les ONG ont également indiqué que, dans l'ensemble, il y a peu d'**outils technologiques disponibles que les professionnels *peuvent* utiliser** (pour répondre aux besoins des ONG, les outils doivent être « peu coûteux » et « faciles à utiliser »).

Autres informations issues de l'analyse du contexte

D'autres questions soulevées dans la base d'informations factuelles disponible englobent :

- La nécessité d'exploiter les informations obtenues par des moyens technologiques (dans une affaire examinée par Rende Taylor et Shih (2019), les signalements par des travailleurs sous la forme de commentaires sur des applications évoquant l'exploitation par le travail dans les chaînes d'approvisionnement n'ont guère été exploitées) ;
- Les technologies ne peuvent en aucun cas se substituer à des connaissances de terrain ;
- La détection participative des victimes ne va pas sans soulever des questions relatives à la vie privée et aux risques de faire justice soi-même. Les signalements faits par les clients sont jugés très fiables, mais les initiatives participatives doivent être examinées de près et mises en balance avec le risque de créer des groupes virtuels (et non virtuels) de personnes faisant justice elles-mêmes ;
- La nécessité d'améliorer la collecte et l'analyse de preuves électroniques pour alléger la charge qui pèse sur les victimes (lorsqu'elles doivent fournir des preuves à l'encontre des trafiquants ou nécessaires à leur défense).

Formations : ce qui est dispensé et ce qui est nécessaire

La grande majorité des pays ont indiqué qu'ils dispensaient des formations sur la traite. Néanmoins, les niveaux et les types de formations dispensées aux **services répressifs** varient d'un pays à l'autre. Certains exigent que tous les policiers susceptibles d'entrer en contact avec une victime présumée suivent une telle formation, tandis que d'autres réservent ces formations aux unités spécialisées.

Il existe un consensus sur le fait que les agents doivent recevoir une formation sur a) la détection des cas de traite et l'identification des victimes de la traite ; b) la collecte, la sauvegarde et le traitement des preuves électroniques, y compris les méthodes d'extraction d'informations contenues dans des ordinateurs et d'autres supports numériques, et c) l'utilisation de logiciels pertinents, y compris les ***Big Data Analytics*** (processus d'analyse de mégadonnées) et les robots d'indexation (lorsque la législation interne l'autorise). Plusieurs pays considèrent qu'une **formation OSINT** est indispensable. Les techniques d'enquête comprenant des **enquêtes en ligne** réalisées par un agent sous couverture sont également considérées comme jouant un rôle de plus en plus important.

La plupart des pays ont indiqué qu'ils fournissaient des éléments de formation semblables à ceux décrits ci-dessus, tout en mentionnant certaines questions, notamment a) la nécessité d'actualiser les formations et, dans certains cas, d'améliorer considérablement les dispositions actuelles ; et b) d'augmenter la part de personnel qui reçoit une formation. Certains pays constatent avec préoccupation que les formations dispensées dans le domaine des TIC sont généralement limitées, et encore plus sur la traite facilitée par les TIC.

Dans cette perspective, le **risque de saturation du système** est particulièrement aigu. Sachant que les infractions facilitées par les TIC, y compris la traite, sont en voie d'augmenter régulièrement, il conviendra de ne pas recourir de manière excessive à des centres de cybercriminalité centralisés. Afin d'éviter les engorgements, il est essentiel d'intégrer des **cyber-connaissances générales/de base dans la formation habituelle** des enquêteurs plutôt que de les considérer comme un « domaine de spécialisation ».

Six grands domaines apparaissent comme indispensables au renforcement des capacités : la collecte et l'analyse de renseignements issus de sources ouvertes (OSINT) ; le profilage à partir des réseaux sociaux et des applications de communication, ainsi que du *dark web*/réseau TOR ; l'étude des données présentes sur les dispositifs de communication et de stockage d'informations, y compris les informations supprimées par les utilisateurs et les connaissances sur le cryptage ; la capacité de corroborer les données acquises par l'intermédiaire des TIC avec des compléments d'information obtenus au cours de l'enquête pénale ; l'identification de victimes (présumées) dans l'environnement en ligne ; une formation sur la criminalité économique et financière avec une partie dédiée aux transactions en ligne et aux cryptomonnaies virtuelles.

La **formation des procureurs et des juges** sur la traite facilitée par les TIC est relativement inégale d'un État partie à un autre. Plusieurs pays ont indiqué que, pour l'heure, les magistrats ne recevaient aucune formation sur ce thème. D'autres pays organisent une formation générale sur la traite sans aucun élément spécifiquement centré sur les questions liées aux TIC.

Les organisations non gouvernementales ont souligné la nécessité de recevoir une formation de la part des services répressifs nationaux et des organisations internationales sur les dernières évolutions en matière de technologie et de traite, y compris l'évolution des stratégies de recrutement. Elles ont également mis l'accent sur la nécessité d'organiser des formations sur les bonnes pratiques internationales et sur le partage d'expériences entre les pays.

Instruments juridiques

Lacunes dans le cadre international actuel

Globalement, les États parties ont exprimé une opinion positive sur les instruments juridiques existants qui facilitent la coopération entre les pays dans la lutte contre la traite. Les conventions du Conseil de l'Europe sur l'entraide judiciaire en matière pénale et la cybercriminalité sont considérées comme des instruments figurant parmi les « plus couramment utilisés » et sont jugées, dans l'ensemble, « adéquates ». Les États parties ont toutefois identifié quelques lacunes potentielles, ainsi que des domaines dans lesquels la législation actuelle pourrait être améliorée. Les principales lacunes identifiées concernent :

- L'absence de cadre juridique commun (harmonisé) sur lequel reposeraient les échanges entre les FAI et les autorités dans le contexte d'enquêtes spécifiques ;
- Dispositions permettant aux entreprises privées de répondre plus rapidement aux demandes de données ;
- Des dispositions contraignant les entreprises privées à divulguer des informations à la demande/sur ordre d'un autre État partie ;
- Des dispositions sur l'application de règles communes pour la conservation des données ;
- Des dispositions visant à faciliter la collecte de témoignages de victimes et leur utilisation dans un autre pays ;
- Les questions relatives à des mesures transnationales contre les sites web qui hébergent des éléments pouvant faciliter l'exploitation des victimes ;
- Des dispositions introduisant un « devoir de vigilance » des entreprises sur l'ensemble de leur chaîne d'approvisionnement ;
- L'emploi d'une terminologie qui ne permet pas toujours à la législation de se développer au rythme des changements de mode opératoire des trafiquants ;
- Des différences dans la transposition de l'infraction de traite (conformément au Protocole de Palerme des Nations Unies) dans les législations nationales.

La Convention sur la cybercriminalité (Budapest) et la lutte contre la traite facilitée par les TIC

La Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) est citée par les États parties comme l'instrument le plus utile dans la lutte contre la criminalité facilitée par les TIC.

Les États parties considèrent que les dispositions relatives au **droit procédural** (chapitre II, section 2 de la Convention) sont les plus utiles dans le cadre de la traite facilitée par les technologies. En outre, ils ont souligné l'**importance de mesures procédurales non limitatives contre les infractions expressément énumérées** (par exemple, au chapitre II, section 1 ;). La Convention ne produit clairement ses pleins effets que lorsqu'elle ne se limite pas aux infractions expressément répertoriées au chapitre II, section 1. Ce constat est particulièrement vrai dans le contexte de la traite facilitée par les TIC.

Plusieurs pays ont insisté sur l'utilité des dispositions énoncées au chapitre III de la Convention sur la coopération internationale, qui servent de base légale permettant aux pays de **rassembler et de partager des preuves électroniques**. La Convention évoque l'établissement d'un réseau de points de contact. Ce réseau constitue un outil important mais, il est probable qu'à l'avenir, compte tenu du rôle de plus en plus central joués par les TIC et les preuves électroniques, ces points de contact subiront une pression croissante et seront rapidement débordés si leurs effectifs sont insuffisants. Cela renvoie au risque de blocage d'un système ; l'emplacement du point de contact dans le système de justice pénale est crucial et peut entraîner des conséquences majeures.

À l'avenir, les mesures suivantes permettraient **une utilisation plus poussée de la Convention sur la cybercriminalité** dans la lutte contre la traite :

- Application du Deuxième Protocole additionnel à la Convention, qui a été adopté en novembre 2021 et qui sera ouvert à la signature le 12 mai 2022 ;
- Compléter l'harmonisation des législations nationales avec la Convention sur la cybercriminalité pour qu'elle produise ses pleins effets ;
- Formation élargie et améliorée sur les possibilités offertes par la Convention sur la cybercriminalité car, à l'heure actuelle, tous les États parties ne tirent pas le meilleur parti des outils disponibles ;
- Plus de sensibilisation sur le champ d'application des dispositions procédurales incluses dans la Convention, car certaines données mettent en évidence un certain désaccord entre les États parties sur l'application des dispositions en vigueur aux cas de traite ;
- Mise en œuvre d'une procédure qui accélère la fourniture de l'entraide judiciaire en autorisant l'envoi direct d'une demande à une entité située dans un Etat étranger à la condition que l'autorité judiciaire de ce pays en soit informée ;
- Construire des synergies entre le GRETA et le groupe d'experts chargé du suivi de l'application de la Convention sur la cybercriminalité (TC-Y) pour évaluer en permanence l'application de la Convention sur la cybercriminalité dans la lutte contre la traite.

Difficultés mentionnées par les ONG

Les ONG ont mentionné des « restrictions claires » relatives au **RGPD et aux règles de confidentialité des données personnelles**. En outre, elles réclament une législation qui permettrait de se tourner vers la **criminalistique informatique** pour obtenir des preuves recevables dans tous les Etats. D'autres difficultés concernent l'actualisation de la réglementation pour prendre en compte la cybercriminalité et internet, ainsi que l'élaboration d'une législation et de règles de fonctionnement concernant les enquêtes numériques.

Cadres juridiques nationaux relatifs à la suppression des contenus liés à la traite

La grande majorité des pays ont pris des mesures juridiques pour réglementer l'identification, le filtrage et la suppression des contenus internet liés à la traite. En règle générale, ces mesures ne font pas spécifiquement référence à la traite mais plus généralement aux « contenus illégaux » (l'exception étant le matériel lié à l'exploitation sexuelle d'enfants). Dans quelques pays, les procédures permettant de supprimer les contenus relatifs à la traite requièrent une décision de justice. Certains de ces pays estiment que ces procédures sont « trop rigides » ou inefficaces, et plaident en faveur de moyens plus performants. Enfin, certains pays ont souligné que les entreprises implantées à l'étranger pouvaient aisément contourner les législations nationales sur la responsabilité juridique des fournisseurs d'hébergement.

Droits humains, éthique et protection des données

Informations communiquées par les États parties

Tous les États parties ont indiqué avoir adopté une législation interne qui réglemente **le traitement** et la **protection des données**. S'agissant de la **protection personnelle des victimes**, plusieurs pays ont fait savoir que des mesures avaient été introduites pour empêcher les auteurs d'infractions d'entrer en contact avec les victimes ; pour l'audition des témoins par visioconférence pour empêcher tout contact avec les défendeurs ; et, dans certains cas, la possibilité pour les victimes de fournir des preuves de manière anonyme pour protéger leur identité.

Des États parties ont indiqué avoir mis en place des **protocoles tenant compte de l'âge**, sous la forme de différents types de procédures et de mesures de protection qui sont normalement appliquées selon que la victime soit majeure ou mineure (âgée de moins de 18 ans). Quant aux **protocoles tenant compte de la dimension du genre**, tous les pays pour lesquels cette information est disponible ont fait savoir qu'ils n'avaient pas de tels protocoles. La seule exception est l'Autriche, qui a mentionné un système d'assistance différent selon le genre de la victime.

Informations communiquées par les ONG

Dans le cadre d'une procédure standard, les ONG demandent le consentement de la victime avant de partager des informations avec les services répressifs. Des problèmes se posent lorsque les victimes ne souhaitent pas porter plainte, pour diverses raisons telles que le risque de représailles, d'exclusion sociale ou d'expulsion. Les ONG constatent que c'est le cas pour de « nombreuses victimes de la traite ». Les questions de protection des données et de

partage des données peuvent poser des **dilemmes moraux**. Bien que le partage des données avec les services répressifs et le dépôt de plaintes facilitent *effectivement* les enquêtes, ce qui peut en retour préserver et protéger les victimes sur le long terme, cela a un certain coût pour les victimes prises individuellement, qui peuvent être exposées à des risques et à des menaces.

Les ONG ont attiré l'attention sur les **risques et les dommages potentiels engendrés par la collecte de données à grande échelle et les outils technologiques**. Elles ont également appelé à approfondir la réflexion et à prendre des mesures de contrôle supplémentaires concernant l'utilisation des données et leur stockage sécurisé – et pour veiller au respect des règles de protection des données.

Enfin, très peu d'éléments attestent de l'existence de **protocoles sensibles au genre** élaborés par des ONG. **Des protocoles adaptés à l'âge** sont normalement appliqués selon que la victime est mineure ou adulte

Autres informations issues de l'analyse du contexte

Les TIC peuvent avoir une incidence considérable sur les **droits humains** des individus, y compris les droits à la vie privée, la liberté d'expression et la non-discrimination. Les politiques qui emploient de nombreuses ressources technologiques pour lutter contre la traite doivent être conçues dans le respect des droits de l'homme.

Plusieurs sources ont relevé des questions clés relatives à la **confidentialité des données personnelles, l'éthique, la transparence, la responsabilisation et le consentement éclairé**. L'Organisation pour la sécurité et la coopération en Europe (OSCE, 2020) a identifié plusieurs questions éthiques liées au développement de la technologie pour lutter contre la traite, notamment : a) la protection de la confidentialité des données personnelles ; b) les protocoles de consentement signés par des victimes ; c) la formation des personnes manipulant les données sensibles, en particulier les données des victimes ; d) le stockage sécurisé de données ; e) la prévention de l'utilisation de la technologie pour obtenir des données sensibles sur les personnes vulnérables (par exemple, la collecte générale de données auprès de populations vulnérables ou marginalisées, qui engendre des risques de pratiques discriminatoires) ; et f) l'utilisation de la technologie d'une manière qui ne porte pas atteinte aux droits fondamentaux des victimes et de la population générale. Le Groupe de coordination inter-agences contre la traite des personnes (ICAT, 2019) et d'autres sources ont mis l'accent sur le caractère sensible du partage des données. Lorsque des pays et/ou des organismes compétents se partagent des données, ils doivent respecter les principes de la confidentialité et du droit à la vie privée.

Gerry *et al.* (2016) ont mis en garde contre le risque de généralisation des **outils de suivi** pour lutter contre la traite. En effet, la technologie offre de nouvelles possibilités d'intervention en cas de traite, mais elle constitue également une **forme de surveillance qui peut s'avérer très intrusive** dans la vie privée d'une personne.

Enfin, quelques sources, notamment Milivojevic *et al.* (2020) et Gerry *et al.* (2016), ont souligné l'importance de **ne pas détourner les victimes de la technologie**, car l'accès à

la technologie peut être leur seule façon de communiquer avec le monde extérieur, et représenter un moyen de défense crucial. La suppression de l'accès à la technologie risque d'accroître la dépendance des victimes ; il convient plutôt de promouvoir un accès sécurisé à la technologie. D'une manière générale, l'**intérêt supérieur de la victime** doit être placé au centre de toute action.

Recommandations

Actions visant à améliorer la détection des cas de TEH facilités par la technologie

1. Les services répressifs devraient investir dans le renforcement des capacités dans les domaines de la **surveillance d'Internet, des cyber-patrouilles, des enquêtes en ligne sous couverture (cyber-infiltration), de l'utilisation de l'OSINT des agents spécialisés, de l'analyse des réseaux sociaux** et de l'utilisation **d'outils de recherche automatique** pour analyser les preuves. Le développement et l'utilisation de ces outils doivent respecter les principes de l'Etat de droit. Les pays devraient envisager d'adapter la législation existante pour permettre les cyber-patrouilles et les enquêtes en ligne par des agents sous couverture (cyber-infiltration) - en tenant compte des considérations éthiques. Les autorités devraient également envisager d'investir dans des outils aidant les enquêteurs à gérer et à traiter des volumes importants de données (capacités en matière de big data). Des ressources pourraient être mises en commun au niveau supranational pour le développement de produits technologiques, tels que les robots d'indexation du web, ainsi que pour le partage de l'expertise sur leur utilisation.

2. Les services répressifs et les inspections du travail devraient mettre en œuvre des **réglementations plus strictes et des contrôles plus fréquents sur les sites web d'offres d'emploi**. Cela pourrait se faire à l'aide d'outils technologiques développés en coopération avec des entreprises privées (par exemple, des outils de validation des offres d'emploi en ligne, des outils pour scruter les sites d'offres d'emploi et apposer des marqueurs

TEH). Les inspections du travail devraient **développer une expertise numérique et accroître leur présence en ligne**.

3. Les États/prestataires privés/ONG doivent améliorer les **mécanismes de signalement confidentiel en ligne**, en permettant le signalement anonyme des cas de TEH ainsi que l'autoidentification des victimes. Les fonctions de chat, y compris les chatbots, et de messagerie instantanée pourraient être des outils en ligne utiles. Les pays devraient collaborer avec les entreprises privées offrant des services en ligne afin d'**éliminer les opportunités pour les trafiquants**, de développer des **analyses de contenu** pour détecter les cas de TEH et de mettre en place des mécanismes facilement accessibles pour que les clients puissent **signaler** les activités/publicités suspectes. Lorsque la législation nationale le permet, cette mesure devrait être étendue aux entreprises offrant des services en ligne pour adultes. Le contenu et les informations en ligne (par exemple, les adresses IP) liés aux activités/publicités signalées devrait être stockés en toute sécurité par les entreprises.

Actions visant à améliorer l'enquête sur la TEH facilitée par la technologie

4. Les services répressifs devraient envisager de former des agents spécialisés à la fois dans les TIC et la TEH. Les pays devraient également envisager de créer des **groupes d'appui technique** composés de policiers assermentés ou non, spécialisés dans les TIC et intégrés aux unités de lutte contre la TEH. En outre, les pays devraient revoir la **répartition interne des capacités d'enquête numérique**, afin d'anticiper et d'éviter les **engorgements des services d'enquête**. Étant donné que la criminalité facilitée par les TIC, y compris TEH, est susceptible d'augmenter constamment, le manque d'agents spécialisés au niveau local et la dépendance excessive à l'égard de l'assistance des unités centralisées de lutte contre la cybercriminalité (très occupées) risquent de créer des engorgements.

5. Les autorités répressives devraient s'assurer que tous **les agents** aient un niveau d'expertise adéquat en matière de collecte et de traitement de preuves électroniques. La formation sur les **preuves électroniques** devrait faire partie intégrante des programmes de formation et être constamment mise à jour en raison de l'évolution rapide du contexte technologique et comportemental. La préservation des preuves électroniques étant essentielle pour monter des enquêtes solides, les **conseillers et les premiers intervenants** des ONG doivent également être familiarisés avec les stratégies de préservation de preuves numériques (par exemple, en stockant les historiques de chat).

6. Les États/organisations internationales devraient régulièrement procéder à une **analyse stratégique** permettant de connaître les tendances émergentes en matière de *modus operandi* des délinquants et de se tenir au courant de l'évolution rapide des comportements des utilisateurs de technologies et du contexte technologique. Sur la base de ces éléments stratégiques, les États peuvent ensuite lancer des opérations de police ciblées, mettre en place des accords de coopération, ainsi que concevoir des campagnes de sensibilisation ciblées. Les connaissances devraient être régulièrement diffusées aux niveaux national et supranational.

7. Les États devraient accroître la coopération transfrontalière en **rationalisant les procédures**, en **partageant les meilleures pratiques et meilleures technologies** (par exemple, des logiciels spécialisés) et en améliorant la **diffusion d'informations pratiques** sur les points de contact/unités dédiées qui servent de « contact privilégié » dans les cas de

TEH, y compris la TEH facilitée par les TIC. La coopération et le soutien entre les pays de destination et d'origine doivent être encouragés (par exemple, des équipements technologiques coûteux pourraient n'être abordables que pour les pays de destination plus riches).

Actions visant à améliorer la poursuite en matière de la TEH facilitée par la technologie

8. Les procureurs devraient recevoir une **formation** spécifique sur la TEH facilitée par la technologie, sur le traitement des preuves électroniques et sur leur présentation devant un juge/un jury. Les États devraient prendre des mesures pour s'assurer que les **procureurs connaissent bien les procédures** de demande de preuves électroniques auprès des entreprises privées, ainsi que les procédures d'obtention de preuves et de coopération auprès d'autres États, tant dans le cadre juridique de l'UE (via les équipes communes d'enquête et les décisions d'enquête européenne) qu'en dehors.

Actions visant à renforcer la coopération avec les entreprises privées

9. Les pays devraient élaborer des **procédures de partage des données** avec les entreprises détenant des données pertinentes et envisager de mettre en place des **protocoles de coopération** avec les entreprises privées, y compris les entreprises des réseaux sociaux et d' « économie à la tâche » ainsi que les plateformes de location, afin de favoriser la fourniture d'informations en temps utile. Ces protocoles/procédures devraient clarifier les exigences légales en vertu desquelles les entreprises de TIC, les FAI et les hébergeurs de contenus opèrent ; désigner un point de contact au sein des entreprises ; et préciser les agences nationales responsables d'actions spécifiques, par exemple la demande de preuves ou le retrait de contenus liés à la TEH. Le refus de partager des preuves ou de retirer du contenu lié à la TEH devrait être rendu en temps utile, explicite et motivé.

Actions visant à renforcer la coopération internationale

10. Il convient de mettre en place un **processus plus fluide pour les demandes d'entraide judiciaire (MLA)**, notamment des procédures plus claires, un recours accru aux réseaux améliorés de points de contact, y compris les points de contact du réseau judiciaire européen, et des exigences en matière d'entraide judiciaire clairement définies et discutées dès le départ. Les Etats doivent s'assurer que leur personnel est correctement formé pour traiter les demandes d'entraide judiciaire, les décisions d'enquête européenne et autres outils internationaux. Les pays et les organisations internationales devraient élaborer des **modèles convenus et acceptés** par tous concernant les processus de coopération, afin de faciliter la communication, réduire les charges administratives et minimiser les erreurs dans les demandes. Les pays devraient également développer l'utilisation de **moyens sécurisés de communication électronique** et promouvoir leur adoption pour faciliter la coopération internationale.

Actions visant à améliorer la formation

11. Des **activités de formation conjointes (JTA)** devraient être envisagées pour les pays qui sont systématiquement engagés dans des affaires conjointes de TEH. L'échange transnational de connaissances peut être encouragé par la participation à des formations internationales/régionales axées sur des aspects spécifiques des enquêtes sur la TEH facilitée par les TIC. Ces formations devraient inclure des études de cas et des scénarios sur la TEH facilitée par les TIC. Une formation sur la TEH facilitée par les TIC et les instruments juridiques associés devrait également être dispensée aux procureurs et aux juges.

12. Les ONG devraient recevoir une formation sur les dernières évolutions à la fois du contexte technologique et de la TEH, y compris les changements dans les stratégies de recrutement. Les ONG devraient être en mesure d'échanger leurs expériences sur les meilleures pratiques internationales.

Actions visant à améliorer les instruments juridiques

13. Les autorités devraient élaborer des **procédures communes pour l'échange rapide de preuves numériques avec les FAI** et **réévaluer la durée des obligations de conservation des données** imposées aux FAI (les périodes actuelles sont trop courtes, compte tenu de la durée des enquêtes policières). Des efforts devraient être faits pour adopter un **cadre commun** concernant les obligations de conservation des données et le partage des preuves électroniques.

14. Pour exploiter tout le potentiel offert par la **Convention sur la cybercriminalité**, les États devraient (a) achever l'harmonisation des législations nationales avec la Convention ; (b) élargir et améliorer la formation sur les possibilités offertes par la Convention, car tous les Etats parties ne tirent pas pleinement parti actuellement les outils disponibles ; (c) sensibiliser aux vastes étendues des moyens procéduraux et des outils de coopération internationale de la Convention, en particulier en ce qui concerne les affaires de TEH; et (d) mettre rapidement en œuvre les mesures incluses dans le Deuxième Protocole additionnel.

15. Les pays devraient évaluer soigneusement la question de savoir où se trouve leur **point de contact** (conformément à la Convention sur la cybercriminalité) au sein du système de justice pénale afin d'éviter les **engorgements**. Avec le rôle de plus en plus central joué par les TIC et les preuves électroniques, ces points de contact seront soumis à une pression croissante et seront rapidement débordés s'ils ne sont pas dotés en personnel de manière adéquate. Les pays pourraient envisager de doter ces points de contact de personnel ayant une expertise dans différents types de crimes, y compris la TEH facilitée par les TIC.

16. Les pays non européens devraient être encouragés à **adopter les principaux outils juridiques internationaux**, tels que la Convention du CdE sur la cybercriminalité et la Convention du CdE sur l'entraide judiciaire en matière pénale, afin de faciliter et de renforcer la coopération internationale.

17. La **coopération et les synergies** devraient être accrues entre le mécanisme de suivi de la Convention contre la TEH (GRETA et Comité des Parties) et la T-CY, par exemple, sous la forme d'un échange de positions ainsi que du développement d'activités de renforcement des capacités axées sur les deux conventions.

Actions visant à prévenir la victimisation et la re-victimisation

18. Les entreprises privées, en collaboration avec les autorités et les ONG, devraient augmenter la **publicité sur les réseaux sociaux**) en ligne pour prévenir la victimisation et améliorer la détection de la TEH facilitée par la technologie. Les pays devraient redoubler d'efforts pour informer les individus de leurs droits en matière d'emploi dans une langue qu'ils comprennent, en coopération avec les ONG et les hébergeurs d'offres d'emploi. L'impact des campagnes devrait être régulièrement évalué.

19. Les pays, les ONG et les entreprises privées qui fournissent des services en ligne et des services TIC devraient mener des initiatives de **sensibilisation aux risques liés à la technologie, y compris la manière dont les trafiquants peuvent exploiter la technologie** et comment des situations d'exploitation potentielle peuvent commencer. Le personnel éducatif devrait être associés à cet effort, car les enfants et les jeunes adultes sont exposés à des risques accrus. Les pays et les ONG devraient travailler avec les entreprises privées qui offrent des services de communication et de messagerie pour intégrer dans le système des informations et des avertissements sur **l'utilisation en toute sécurité de voies de communication privée**.

20. Les ONG devraient proposer des formations sur les techniques de protection des données et d'utilisation en toute sécurité des technologies, dans le cadre **des programmes de protection et de réintégration des victimes**. Les victimes ne devraient pas être exclues de la technologie en les privant des moyens de s'émanciper.

Action transversale

21. Les pays devraient inclure une stratégie technologique dans leurs **plans d'action nationaux** de lutte contre la traite des êtres humains.

Annexe 1 | Établir une base de données probantes sur la TEH en ligne et facilitée par la technologie : liste de sources

La base factuelle a été construite sur la base d'une vaste recherche de fond couvrant une variété de sources, notamment : (a) les organisations internationales ; (b) le monde universitaire ; (c) les rapporteurs nationaux sélectionnés ; (d) les ONG et les organisations caritatives ; (e) le secteur privé. Au total, 61 résultats ont été identifiés comme pertinents pour les besoins de ce travail. Bien que les résultats considérés couvrent la période 2003 - 2020, la grande majorité a été publiée à partir de 2015, et 21 ont été publiés au cours des trois dernières années. Tous les résultats considérés sont rédigés en anglais (à une exception près : la version française d'un rapport produit par Myria, le « fédéral Migration » belge).

Organisations internationales et nationales

1. Conseil de l'Europe (2021). *Protecting Women and Girls from Violence in the Digital Age.*
2. Conseil de l'Europe (2019). *Intensifier l'action du Conseil de l'Europe contre la traite des êtres humains à l'ère numérique.* Rapport de synthèse.
3. Conseil de l'Europe (2019). *9ème Rapport général sur les activités du GRETA.*
4. Conseil de l'Europe (2016). *Sauvegarde des droits de l'homme sur le net.*
5. Conseil de l'Europe (2016). *Étude sur les mesures de réduction pour lutter contre la traite des êtres humains à des fins d'exploitation du travail par l'engagement du secteur privé.*
6. Conseil de l'Europe (2016). *Bonnes pratiques émergentes des autorités étatiques, du monde des affaires et de la société civile dans le domaine de la réduction de la demande de traite des êtres humains à des fins d'exploitation du travail.*
7. Conseil de l'Europe (2015). *Étude comparative du blocage, du filtrage et du retrait des contenus illicites sur Internet.*
8. Conseil de l'Europe (2007). *La traite des êtres humains : Le recrutement sur Internet*.
9. Conseil de l'Europe (2003). *Impact de l'utilisation des nouvelles technologies de l'information sur la traite des êtres humains à des fins d'exploitation sexuelle*.
10. ICAT (2019). *Traite des êtres humains et technologie : Tendances, défis et opportunités. Groupe de coordination interinstitutions contre la traite des personnes.* Issue Brief 7.
11. OCSE (2020). *Tirer parti de l'innovation pour lutter contre la traite des êtres humains : Une analyse complète des outils technologiques*. OCSE et Tech Against Trafficking.
12. DON.ONU (2008). *Technologie et traite des êtres humains*. Le Forum de Vienne sur la lutte contre la traite des êtres humains : Background Paper.

13. UNODC (2019). Module 14 : Liens entre la cybercriminalité, la traite des personnes et le trafic de migrants. Modules d'enseignement E4J.

14. Myria (2017). *En ligne_ : Traite et trafic des êtres humains*, Rapport annuel 2017.

15. Europol (2020). *Les défis de la lutte contre la traite des êtres humains à l'ère numérique.*

16. Europol (2014). *La traite des êtres humains et l'internet.* Avis de renseignement.

Universités

17. Ibanez M. et Gazan R. (2016). « Détection des circuits de trafic sexuel aux États-Unis par l'analyse des annonces d'escortes en ligne ». Conférence internationale IEEE/ACM sur les progrès de l'analyse et de l'exploration des réseaux sociaux (ASONAM), 892 - 895.

18. Ibanez M. et Gazan R. (2016). « Indicateurs virtuels du trafic sexuel pour identifier les victimes potentielles dans les annonces en ligne », 818 - 824.

19. Ibanez M. et Suthers D. D. (2014). « Détection des indicateurs de trafic humain domestique et des tendances de mouvement en utilisant le contenu disponible sur les sources Internet ouvertes ». 47e conférence internationale de Hawaii sur la science des systèmes, 1556 - 1565.

20. Volodko A., Cockbain E. et Kleinberg B. (2019). "'Spotting the signs' of trafficking recruitment online : exploring the characteristics of advertisements targeted at migrant job-seekers". Trends in Organized Crime, 27 : 7-35.

21. Di Nicola A., Baratto G. et Martini E. (2017). *Surf and Sound. Le rôle d'Internet dans le trafic de personnes et la traite des êtres humains*. Rapport de recherche eCrime 3.

22. Sykiotou A. P. (2017). Cybertraite : recruter des victimes de la traite des êtres humains par le biais du net. Dans « Essais en l'honneur de Nestor Courakis ». A. N. Sakkoulas Publications.

23. Foot K.A., Toft A. et Cesare N. (2015). « Développements des efforts de lutte contre la traite des êtres humains : 2008 – 2011 ». Journal of Human Trafficking, 1:2, 136-155.

24. Gerry F., Muraszkiewicz J. et Vavoula N. (2016). « Le rôle de la technologie dans la lutte contre la traite des êtres humains : Réflexions sur les préoccupations relatives à la vie privée et à la protection des données ». *Computer Law & Security Review*, 32:2, 205-217.

25. Latonero M., Browyn W. et Dank M. (2015). *Technologie et trafic de main-d'œuvre dans une société en réseau : General Overview, Emerging Innovations, and Philippines Case Study*. Californie : Université de Californie du Sud, Annenberg Center on Communication Leadership & Policy.

26. Latonero M. (2011). *Le rôle des sites de réseautage social et des petites annonces en ligne*. California : Université de Californie du Sud, Annenberg Center on Communication Leadership & Policy Research Series.

27. Latonero, Mark (2012). *L'essor du mobile et la diffusion de la traite facilitée par les technologies*. Université de Californie du Sud, Annenberg Center on Communication Leadership & Policy.

28. Elliott J. et McCartan K., (2013). « La réalité de l'accès des victimes de la traite à la technologie ». *The Journal of Criminal Law*, 77:3, pp.255-273.

29. Hughes D. M. (2014). « La traite des êtres humains dans l'Union européenne : Genre, exploitation sexuelle et technologies de communication numérique. » Sage Open 4 : 4.

30. Kunz R., Baughman M., Yarnell R. et Williamson C. (2018*). Médias sociaux et processus de trafic sexuel : De la connexion et du recrutement, à la vente*. Ohio : Université de Toledo.

31. Farley, M., Franzblau, K., et Kennedy, M. A. (2013). Online prostitution and trafficking. *Albany Law Review*, 77:3, 101-157.

32. Barney, D. (2018). Trafficking Technology : Un regard sur différentes approches pour mettre fin à la traite des êtres humains facilitée par la technologie. *Pepperdine Law Review*, 45, 747-784.

33. Milivojevic, S., Moore, H., et Segrave, M. (2020). Freeing the Modern Slaves, One Click at a Time : Theorising human trafficking, modern slavery, and technology. *Anti-trafficking review,* (14), 16-32

34. Raets S. et Janssens J. (2019). Trafficking and Technology : Exploration du rôle des technologies de communication numérique dans l'activité belge de traite des êtres humains. *Revue européenne de politique et de recherche criminelles*, 1-24.

35. John G. (2018). Analyse de l'influence des technologies de l'information et de la communication sur le fléau de la traite des êtres humains au Rwanda. Revue académique des sciences sociales, 3:1, 1095-1102.

36. Maras, Marie-Helen (2017). « Les sites d'annonces classées en ligne : proxénètes et facilitateurs de la prostitution et du trafic sexuel ? », *Journal of Internet Law*, vol. 21, 17-21.

37. Stalans L. J. et Finn M A. (2016). Comprendre comment l'Internet facilite la criminalité et la déviance, Victimes et délinquants, 11, 501-508.

38. Van Reisen, M., Gerrima, Z., Ghilazghy, E., Kidane, S., Rijken, C., et Van Stam, G. (2017). Tracing the emergence of ICT-enabled human trafficking for ransom. Dans Piotrowicz R., Rijken C., Baerbel, Uhl B. H. (eda), *The Routledge Handbook on Human Trafficking*. Routledge : Londres

39. Raets, Sigrid et Jelle Janssens (2018). *Trafficking & Technology : Le rôle des technologies de communication numérique dans l'activité de traite des êtres humains*.

40. Dixon H. (2013). La traite des êtres humains et Internet (et d'autres technologies, aussi). Judges' Journal, 52:1, 36-39.

41. Thakor M. et Boyd D. (2013). Networked trafficking : Réflexions sur la technologie et le mouvement anti-trafic. *Dialectical Anthropology*, vol. 37, pp. 277-290.

42. Michell K. J. et Boyd D. (2014). Comprendre le rôle de la technologie dans l'exploitation sexuelle commerciale des enfants : le point de vue des forces de l'ordre. Université du New Hampshire : Centre de recherche sur le crime contre les enfants.

43. Heil, E., et Nichols, A. (2014). Hot spot trafficking : Une discussion théorique des problèmes potentiels associés à la police ciblée et à l'éradication de la traite sexuelle aux États-Unis. *Revue contemporaine de justice*, 17(4), 421-433.

44. Andrews S., Brewster B., Day T. (2016) Organised Crime and Social Media : Détecter et corroborer les signaux faibles de la traite des êtres humains en ligne. In : Haemmerlé O., Stapleton G., Faron Zucker C. (eds) Graph-Based Representation and Reasoning. ICCS 2016. Lecture Notes in Computer Science, vol 9717. Springer, Cham.

45. Mendel J. et Sharapov K. (2016). La traite des êtres humains et les réseaux en ligne : Politique, analyse et ignorance. *Antipode, 48*(3), 665-684.

46. TRACE (2017). Rapport sur le rôle des technologies actuelles et émergentes dans la traite des êtres humains. Livrable 4.1, FP7/Security Research, financé par la Commission européenne.

47. Landman T., Trodd Z., Darnton H., Durgana D., Moote K., Jones P., Setter C., Bliss N., Powell S. et Cockayne J. (eds). *Code 8.7 : Rapport de conférence 2019/02/19-20 New York*. New York : Université des Nations Unies, 2019.

48. Kiss L., Fotheringhame D., Mak J., McAlpine A. et Zimmerman, C. (2020). L'utilisation de réseaux bayésiens pour l'évaluation réaliste d'interventions complexes : preuves pour la prévention de la traite des êtres humains. *Journal of Computational Social Science*, 1-24.

49. Jackson B. et Lucas B. (2020). Une réponse du COVID-19 à l'esclavage moderne en utilisant la recherche en IA. 26 juin, www.delta87.org.

50. Rende Taylor L. et Shih E. (2019). "Worker feedback technologies and combating modern slavery in global supply chains: examining the effectiveness of remediation-oriented and due-diligence-oriented technologies in identifying and addressing forced labour and human trafficking", *Journal of the British Academy*, 7(s1), 131-165.

51. Musto J., Thakor M., et Gerasimov B. (2020), "Editorial : Between Hope and Hype : Critical evaluations of technology's role in anti-trafficking", *Anti-Trafficking Review*, 1-14, en ligne à l'adresse : https://doi.org/10.14197/atr.201220141.

52. Kougkoulos, I., Cakir, M. S., Kunz, N., Boyd, D. S., Trautrims, A., Hatzinikolaou, K., & Gold, S. (2021). Une approche multi-méthodes pour prioriser les lieux d'exploitation du travail pour les interventions au sol. Production and Operations Management, première version en ligne.

ONG/Associations caritatives/Secteur privé

53. Fine Tune Project (2011). *Le rôle d'Internet dans la traite à des fins d'exploitation du travail*. Rapport final pour la Commission européenne.

54. Thorn (2015). Un rapport sur l'utilisation de la technologie pour recruter, préparer et vendre des victimes de la traite sexuelle de mineurs domestiques.

55. Thorn (2018). Aperçus de survivants. Le rôle de la technologie dans la traite sexuelle des mineurs domestiques.

56. Chawki M. et Wahab M. (2005). La technologie est une arme à double tranchant : la traite illégale des êtres humains à l'ère de l'information. *Computer Crime Research Center*.

57. Caliber (2008). *Law Enforcement Response to Human Trafficking and the Implications for Victims: Current Practices and Lessons Learned*. Rapport final préparé pour le ministère de la Justice des États-Unis : National Institute of Justice.

58. Stop the Traffik (2019). Évaluation indépendante du travail et du modèle de Stop the Traffik.

Sites Web

59. Traffik Analysis Hub: https://traffikanalysis.org/ (IBM, Stop the Traffik and Clifford Chance)

60. The Counter Trafficking Data Collaborative: https://www.ctdatacollaborative.org/ (IOM, Polaris and Liberty Shared)

61. Alan Turing Institute, Data Science for Tackling Modern Slavery (Science des données pour lutter contre l'esclavage moderne) : https://www.turing.ac.uk/research/research-projects/data-science-tackling-modern-slavery

62. UN Delta 8.7. The Alliance 8.7 Knowledge Problem: https://delta87.org/ (Plateforme mondiale de connaissances explorant ce qui fonctionne pour éradiquer le travail forcé, l'esclavage moderne, la traite des êtres humains et le travail des enfants, cible 8.7 des ODD de l'ONU)

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en oeuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE