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

Rapport intégral

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

Rapport intégral

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

Avril 2022

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

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
EJN :	European Judicial Network / Réseau judiciaire européen
FAI :	Fournisseur d'accès internet
GDPR :	General Data Protection Regulation / RGDP : Règlement général sur la protection des données
GRETA :	Groupe d'experts du Conseil de l'Europe sur la lutte contre la traite des êtres humains
HDD :	Hard Disk Drive / Unité de disque dur
IA :	Intelligence artificielle
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
PIB :	Produit intérieur brute
TEH :	Traite des êtres humains
TIC :	Technologies de l'information et de la communication
TOR :	The Onion Router
UE :	Union européenne
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 (TEH).

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 (CdE) 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 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 Groupe d'experts du Conseil de l'Europe sur la lutte contre la traite des êtres

humains (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 Secrétariat du 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 contextuelle

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 contextuelle

Les technologies de l'information et de la communication (TIC) peuvent avoir une incidence considérable sur le respect des **droits humains**, y compris les droits à la vie privée, la liberté d'expression et la protection contre la discrimination. Les programmes de lutte contre la traite qui s'appuient largement sur des outils technologiques doivent être conçus dans le respect des droits humains.

Des questions cruciales ont été posées qui concernent **la confidentialité des données à caractère personnel, l'éthique, la transparence, la responsabilisation et le consentement éclairé**. L'Organisation pour la sécurité et la coopération en Europe (OSCE, 2020) a retenu plusieurs questions d'ordre éthique, liées aux technologies développées pour lutter contre la traite, notamment : a) la protection de la confidentialité des données à caractère personnel ; b) les protocoles de consentement signés par des victimes ; c) la formation destinée aux personnes qui traitent des données sensibles, en particulier les données des victimes ; d) le stockage de données sécurisé ; 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 des technologies de façon à ne pas bafouer les droits fondamentaux des victimes et de la population générale. Le Groupe interinstitutions de coordination contre la traite des personnes (2019) et d'autres sources ont mis l'accent sur les risques inhérents au 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 situation de traite, mais elle constitue également **une forme de surveillance qui peut s'avérer très intrusive** pour la vie privée d'une personne.

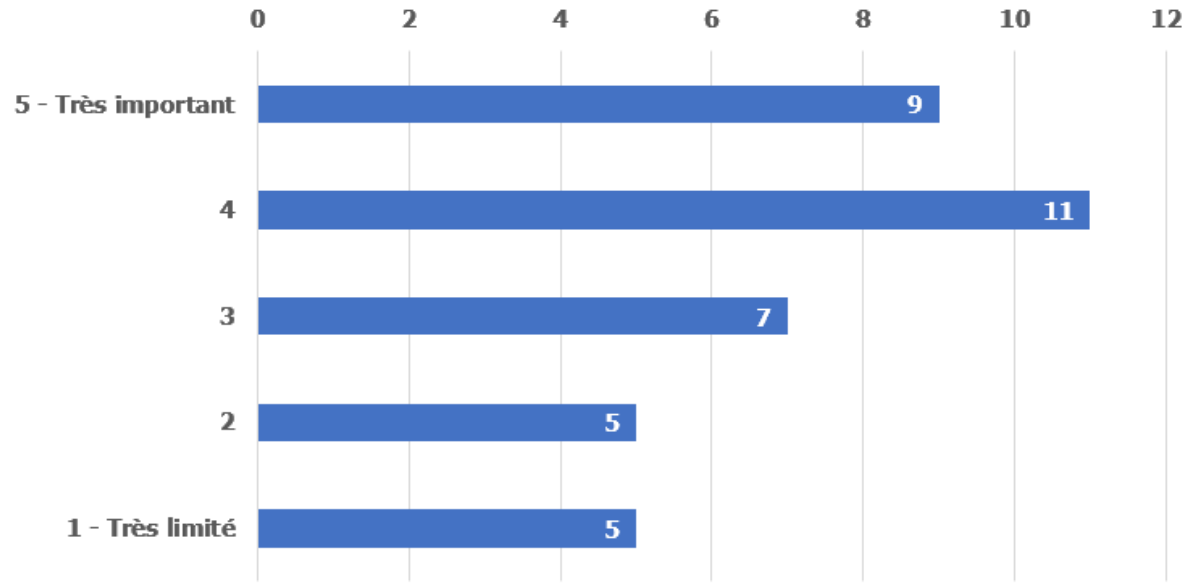
Enfin, quelques sources, notamment Milivojevic *et al.* (2020) et Gerry *et al.* (2016), ont souligné l'importance de **ne pas détourner les victimes de la technologie**, car l'accès à la technologie peut être leur seule façon de communiquer avec le monde extérieur, et représenter un moyen de défense crucial. La suppression de l'accès à la technologie risque d'accroître la dépendance des victimes ; il conviendrait plutôt de promouvoir un accès sécurisé à la technologie. D'une manière générale, l'**intérêt supérieur de la victime** devrait être placé au centre de l'action.

1. Impact de la technologie sur la traite des êtres humains

1.1. Informations communiquées par les États parties

Les informations communiquées par les États parties confirment l'importance croissante de la technologie dans le domaine de la traite, et particulièrement du recrutement et de l'exploitation. Les technologies et les activités en ligne occupent une place grandissante dans la vie des citoyens – et cette tendance se retrouve dans le domaine de la traite. La majorité des États parties qualifient l'impact de la technologie sur la traite de « très important » ou d'« important » (figure 1)[4].

Figure 1. Impact de la technologie sur la traite : États parties



Remarque : N = 37

Parmi les pays ayant évoqué un impact limité, certains ont dans le même temps mentionné un nombre de cas de traite très faible, voire nul (autrement dit, faible impact de la technologie, faible nombre de cas de traite). Pour les autres pays, c'est l'usage global de la technologie qui est (encore) plutôt limité (faible usage de la technologie, faible impact technologique). Dans ces derniers cas, la situation pourrait évoluer à mesure que l'usage de la technologie se généralisera. En effet, certains États parties ont souligné **l'importance croissante** des contenus, des annonces et des sites/applications en ligne dans la recherche d'un 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**.

[4] Trois pays n'ont pas répondu à cette question.

1.1.1. La traite aux fins d'exploitation sexuelle

S'agissant du **recrutement aux fins d'exploitation sexuelle**, plusieurs États parties ont observé l'existence d'offres d'emploi proposant des salaires étrangement élevés, souvent dans le secteur des services, qui étaient en fait des méthodes de recrutement à des fins d'exploitation. Ces offres d'emploi particulièrement trompeuses, voire mensongères, sont souvent publiées sur des sites web très fréquentés, et placées à côté d'offres sérieuses. En outre, des éléments probants ont mis en évidence le rôle des plateformes de médias sociaux dans la diffusion d'offres d'emploi émanant de personnes individuelles, par exemple dans les secteurs de l'hôtellerie (restauration) et de l'agriculture. Les trafiquants promettent généralement un emploi (inexistant) bien rémunéré à l'étranger, puis contraignent la personne à fournir des services sexuels dans le pays de destination.

D'après le Rapport de situation 2019 sur la traite dans la fédération (Bundeslagebild Menschenhandel) présenté par les autorités allemandes, 11 % des victimes recensées ont été contactées ou recrutées sur internet (N = 47). Sur ces 47 victimes, 31 ont été contactées ou recrutées sur une plateforme de réseaux sociaux très fréquentée et 13 par le biais de portails publicitaires. (Trois victimes ont été recrutées sur internet mais à l'aide d'une « autre » méthode.) La Commission nationale bulgare de lutte contre la traite des êtres humains a indiqué que les victimes potentielles contactées par le biais de plateformes de médias sociaux sont « principalement des jeunes filles et des femmes ». Les autorités néerlandaises ont fait savoir que, d'après le système d'information de la police, des plateformes de réseaux sociaux étaient utilisées pour recruter des victimes mineures. Selon les données fournies par l'Autriche, le recrutement se déroulerait généralement dans le pays d'origine des victimes.

Lorsqu'ils s'approchent des victimes potentielles sur internet, les trafiquants pourraient adopter des modes opératoires relativement sophistiqués, souvent fondés sur de faux profils affichant un niveau de vie élevé et une fortune considérable. Comme l'ont indiqué les autorités bulgares, « plusieurs enquêtes ont montré qu'avant d'aborder leurs victimes potentielles en vue d'amorcer le recrutement, les trafiquants examinaient soigneusement les photos de leurs cibles [pour] étudier leurs conditions de vie, leur statut social et leur environnement, leurs connaissances familiales et leur situation amoureuse (mariage, divorce ou fiançailles). […] C'est seulement après ces examens minutieux que les trafiquants contactaient leurs victimes, en usant de talents psychologiques remarquables pour motiver les victimes et les persuader d'adopter certains comportements ». Un large éventail de pays, à savoir l'Autriche, la Bosnie-Herzégovine, la Bulgarie, la Belgique, la Croatie, la Hongrie, la République de Moldova, les Pays-Bas, la Pologne, le Portugal, la Slovaquie, la Suède et l'Ukraine, ont attesté de ces modes opératoires par des données probantes. Ceux-ci s'intègrent souvent dans la technique du *loverboy*, qui consiste à simuler une relation romantique pour contraindre la victime à se livrer à la prostitution. Comme l'ont constaté les autorités roumaines, entre autres, « la technique du *loverboy* reste l'outil le plus courant ». Elle consiste à contacter une personne sur une plateforme en ligne, en apprenant peu à peu à connaître ses passe-temps, ses centres d'intérêt, et sa situation personnelle et familiale (ainsi que ses points faibles). Le « trafiquant aborde [ensuite] la victime avec empathie et la ferme volonté de l'aider, de la comprendre et de la soutenir financièrement. La victime est souvent manipulée par des promesses de relation sérieuse pouvant aller jusqu'à une demande en mariage, dans l'intention de gagner sa confiance et d'en prendre ainsi le contrôle psychologique » (renseignements communiqués

par la Roumanie). Selon certaines données fournies par la Belgique, les victimes recrutées sur des plateformes de médias sociaux se caractérisent souvent par des structures familiales instables, le décrochage scolaire, la faible estime de soi et, plus généralement, des vulnérabilités psychosociales.

Selon certaines informations fournies par les autorités françaises, des réseaux de traite de plusieurs nationalités, réunissant notamment des ressortissants sud-américains, d'Europe de l'Est et français impliqués dans les trafics dits de cité (« proxénétisme des cités ») utilisent les réseaux sociaux pour recruter des victimes. Il semble que les réseaux de traite organisés par des personnes d'origine africaine soient une exception à la règle. Plusieurs pays (notamment le Royaume-Uni, la Norvège, la Finlande, l'Autriche l'Ukraine et le Belarus) ont démontré que certaines applications de rencontre étaient utilisées pour recruter des victimes.

Plusieurs pays font état de nombreux cas de **chantage**. Cela se fait souvent en rassemblant au départ des données « compromettantes » sur la victime, par exemple en demandant des photographies ou des vidéos d'elle-même nue, puis en utilisant ces données pour la contraindre à se livrer à la prostitution. Le plus souvent, les trafiquants entrent en relation avec la victime, gagnent sa confiance, puis réclament des informations « compromettantes ». Ce type de comportements a pu être observé par plusieurs États parties, notamment la Bosnie-Herzégovine, la Bulgarie, la Croatie, les Pays-Bas, la Finlande, la Lituanie et la Suède.

Certains pays dont donné des exemples de victimes recrutées en ligne parmi les personnes proposant des services sexuels ; mais, une fois sur place, elles doivent supporter des horaires de travail qui relèvent de l'exploitation et de très mauvaises conditions de logement, ainsi que des rémunérations radicalement différentes de celles proposées dans les offres d'emploi (données fournies par la Hongrie et la Pologne). La Pologne a également indiqué que des femmes proposant des services sexuels étaient ciblées par les trafiquants, intimidées et contraintes de partager leurs bénéfices (mécanisme comparable à celui de l'extorsion).

Plusieurs pays font largement mention de sites web utilisés pour **proposer des services sexuels**. Parmi ces annonces figurent des publicités liées aux services fournis par des victimes de la traite. Comme l'ont observé les autorités britanniques, les sites web pour adultes « restent le principal **catalyseur de l'exploitation sexuelle** lié à la traite au Royaume-Uni ». Ils « séduisent les trafiquants, car ils requièrent peu de contrôle de l'utilisateur et offrent l'accès à une large base de clients potentiels » (document soumis par les autorités britanniques). Selon des renseignements fournis par la Finlande, « les plateformes informatiques, en particulier les sites d'annonces fondés sur des forums, sont le principal mode opératoire employé pour le marketing et la prise de contact avec les clients dans le domaine de la traite ». D'après les autorités françaises, 65 % des victimes d'exploitation sexuelle recensées ont utilisé internet en 2019, contre 49 % l'année précédente. Les autorités britanniques ainsi que d'autres pays jugent préoccupant que « les annonces des trafiquants acquièrent une certaine légitimité du fait qu'elles apparaissent à côté d'annonces créées par des travailleurs du sexe autonomes ». Selon les autorités finlandaises, « les victimes de la traite et les travailleurs du sexe qui ne sont pas soumis à la traite emploient les mêmes sites ». Il est souvent très difficile pour les autorités de séparer les annonces liées à la traite de celles publiées par des travailleurs du sexe indépendants (voir aussi chapitre 2).

La technologie peut être utilisée pour **coordonner des activités pendant la phase d'exploitation** et établir le contact avec des clients potentiels (négociation des prix, choix des lieux et conclusion des accords). Point essentiel, **la technologie permet de séparer** le lieu où l'activité sexuelle est pratiquée et celui où la coordination est assurée. Il en résulte une complexification de la tâche pour les services répressifs. Par exemple, les autorités de la Bosnie-Herzégovine ont démontré l'existence d'un réseau d'exploitation de femmes bosniennes fournissant des services sexuels en Allemagne et en Autriche ; ces services étaient coordonnés et supervisés par des trafiquants établis en Bosnie-Herzégovine, qui géraient les profils en ligne des victimes et planifiaient les rencontres avec les clients. Les autorités françaises ont signalé la présence de plateformes téléphoniques qui organisaient les rendez-vous à distance depuis Chypre (pour les réseaux russophones) et la Chine (pour les réseaux sinophones). En 2019, la police suédoise a enquêté sur plusieurs affaires où « des réseaux criminels étaient soupçonnés d'organiser des activités de prostitution depuis le pays d'origine des femmes ou par l'intermédiaire d'une agence installée dans un pays tiers ». Le rapport signalait également que les images de différentes femmes étaient associées à des adresses électroniques identiques ou similaires et/ou aux mêmes numéros de portables. Les autorités ont considéré que ces indices constituaient des indicateurs « drapeaux rouges ». La Suède a également fait état d'affaires où des femmes nigérianes et roumaines analphabètes avaient un profil sur des sites web pour adultes. Cela supposait que ces profils étaient écrits et gérés par de tierces personnes – autre drapeau rouge possible.

Certains pays ont démontré que les trafiquants employaient parfois des outils technologiques pour **surveiller et contrôler les victimes** pendant la phase d'exploitation. Dans une affaire citée par les autorités slovènes, les trafiquants demandaient aux victimes de rendre compte de chaque service fourni, mais aussi de les informer sur les autres victimes, afin d'avoir le contrôle total de leurs activités. Dans d'autres affaires, des applications spécifiques étaient utilisées pour suivre les déplacements d'une victime.

Enfin, outre les deux « principaux » domaines du recrutement et de l'exploitation, les informations disponibles montrent que la technologie facilite la logistique de la traite, c'est-à-dire l'achat de billets d'avion, voire, dans certains cas, l'obtention de faux documents de voyage et autres (données fournies par Chypre). Des applications et des sites web servent également à louer des propriétés dans lesquelles les services sexuels sont fournis (données émanant de la France, de l'Estonie, du Royaume-Uni et de l'Espagne). Bien qu'elles fassent partie du processus de la traite, ces activités sont secondaires par rapport au recrutement et à l'exploitation.

Parmi les **tendances émergentes** en matière d'exploitation sexuelle figure le développement de la **diffusion en direct** d'actes sexuels concernant des victimes de la traite. Ces vidéos diffusées en direct sont souvent liées à des abus sexuels sur enfants, mais une poignée de pays a mentionné également des victimes d'âge adulte. Les autorités chypriotes ont relevé l'essor des webcams en direct. D'après les autorités espagnoles, les trafiquants recourent « de plus en plus » à des pages web de vidéos en continu pour vendre les services fournis par les victimes de la traite. De la même façon, les autorités irlandaises ont observé l'expansion rapide des applications de chat vidéo « payantes à l'usage », telles qu'Escortfans et Onlyfans, qui remplacent les plateformes de sites web traditionnelles et permettent de rencontrer des escortes dans des salles de chat privées ou publiques. Les autorités irlandaises

ont soutenu qu'il « était quasiment impossible de déterminer si quelqu'un utilisait les plateformes de manière volontaire ou contrainte, en raison de la nature même de ces applications et de ces sites ». (Une tendance similaire est relevée en Finlande.) Ce segment de marché aurait « progressé de manière exponentielle » depuis l'épidémie de covid-19. D'après les autorités néerlandaises, le nombre de plateformes « devrait encore augmenter dans un proche avenir ». Cette tendance s'étend aux sites et applications de rencontre, aux sites web comportant des publicités à caractère sexuel et aux médias sociaux qui ne sont pas centrés sur les services sexuels mais peuvent être employés à cette fin.

Les autorités chypriotes ont également mentionné le recours croissant à des applications pour contrôler les victimes, qui peuvent envoyer, par exemple, des messages automatiques sur le téléphone portable d'un trafiquant chaque fois que la victime effectue une action spécifique (comme ouvrir la porte d'entrée). De leur côté, les autorités suisses ont fait savoir que des applications de localisation avaient été détectées sur le téléphone des victimes, peut-être téléchargées à leur insu. Une tendance semblable à utiliser la technologie pour contrôler les victimes a pu être observée en Autriche. En outre, les autorités grecques ont signalé qu'un nombre croissant d'enfants migrants étaient recrutés à des fins sexuelles à l'aide de technologies mobiles.

Quelques pays ont souligné l'**accroissement des communications en ligne** dû à la pandémie de covid-19, ce qui ouvre pour les trafiquants de nouvelles possibilités d'entrer en contact avec des personnes vulnérables. Les autorités roumaines ont relevé une augmentation du nombre de victimes recrutées en ligne ces dernières années, et particulièrement depuis l'adoption des mesures de santé publique relatives à la covid-19. Elles ont toutefois ajouté qu'en Roumanie, la majorité des victimes continuaient d'être recrutées via un contact direct par des amis, des partenaires ou des proches. En France, les autorités ont indiqué que depuis la loi du 13 avril 2016 criminalisant l'achat de services sexuels, le racolage sur la voie publique était progressivement remplacé par un système « plus discret » fondé sur des publicités en ligne. Elles ont noté en outre une accélération de ce processus à la suite de la pandémie de covid-19. D'après le ministère public suédois, l'utilisation d'internet associée à la traite à des fins sexuelles a pris tellement d'ampleur qu'il n'existe aujourd'hui « quasiment aucune affaire de traite dans laquelle internet n'apparaît pas » dans les modes opératoires des trafiquants. Les autorités belges prévoient de faire face à une augmentation des affaires dans lesquelles des enfants ou de jeunes adultes vulnérables sont recrutés par le biais des TIC à des fins d'exploitation sexuelle ; en effet, les citoyens qui appartiennent à ces tranches d'âge communiquent de plus en plus en ligne et par les TIC (dans un paysage technologique en perpétuelle évolution qu'il est très difficile d'explorer pour les enquêteurs).

1.1.2. La traite aux fins d'exploitation par le travail

S'agissant de la traite aux fins d'exploitation par le travail, des données fournies par certains États parties montrent que les TIC sont surtout utilisées pour **recruter** des victimes. D'après les autorités allemandes, internet et les médias sociaux jouent un « rôle de plus en plus important dans l'établissement de contacts et le recrutement à des fins de traite et d'exploitation par le travail ». Les autorités espagnoles partagent cet avis et considèrent que le recrutement en ligne à des fins d'exploitation par le travail « est en pleine expansion ». La covid-19 a probablement accéléré le phénomène, au point que les cyberespaces en viennent

à remplacer les échanges et les rencontres en tête à tête. Selon les autorités irlandaises, « ce recours croissant aux médias sociaux pour recruter des travailleurs migrants pose des difficultés supplémentaires pour les autorités qui luttent contre le recrutement abusif et l'exploitation par le travail en ligne ». Les autorités françaises ont constaté que, bien que les formes de recrutement traditionnelles (offres d'emploi dans la presse, petites annonces, prospectus, bouche à oreille, etc.) semblent encore l'emporter, l'utilisation d'annonces en ligne se développe. Cela vient du fait que les demandeurs d'emploi se tournent de plus en plus vers les TIC.

De nombreux pays, à savoir l'Autriche, la Croatie, Chypre, l'Estonie, la Finlande, la France, la Grèce, la Lettonie, la Lituanie, la République de Moldova, la Norvège, la Pologne, le Portugal, la Roumanie, la Suède et la Suisse, ont fourni des éléments attestant de l'existence d'**offres d'emploi fausses ou trompeuses** dans le cadre du recrutement aux fins d'exploitation par le travail. Les autorités bulgares ont signalé que plusieurs sites web de recherche d'emploi diffusaient des annonces où l'« employeur » promettait des salaires mirobolants, le transport et le logement gratuits ainsi que des primes pour des emplois n'exigeant ni un niveau de qualification élevé ni la maîtrise de la langue locale. Ces annonces font souvent partie des modes opératoires des trafiquants qui recherchent des travailleurs en vue de les exploiter. Les données fournies par les autorités allemandes conduisent au même constat : « Certains trafiquants présentent des offres d'emploi sur différents portails internet. Ces emplois sont décrits comme bien rémunérés, avec des horaires de travail conformes aux réglementations ». Mais une fois arrivés en Allemagne, les travailleurs ne reçoivent aucun contrat de travail et leur rémunération ne correspond pas aux promesses. Souvent, ils ne perçoivent aucune rémunération du tout ou seulement une partie de la rémunération promise ». Des annonces similaires ont été relevées en Espagne, où « de nombreuses victimes de la traite à des fins d'exploitation par le travail sont recrutées par le biais de sites d'annonces en ligne », selon les autorités.

Le Royaume-Uni a signalé la présence de fausses annonces de recrutement sur des médias sociaux pour des offres d'emploi très bien rémunérées, à Londres, dans le secteur du bâtiment (et d'autres) ; en réalité, comme l'ont expliqué les autorités, « très souvent, ce sont de fausses annonces et le travail n'existe pas ». Quant au contenu des annonces, les autorités britanniques ont relevé que la majorité des annonces de recrutement signalées comme utilisées par les trafiquants se fondent sur de vagues promesses attractives en termes d'emploi, de rémunération et de conditions de travail, sans aucune précision sur la forme de travail ou la rémunération. Toutefois, dans une minorité de cas de traite enregistrés, les annonces d'offres d'emploi donnaient ce type de précisions. Dans le domaine de l'exploitation par le travail plus que celui de l'exploitation sexuelle, il est courant que le secteur d'activité soit décrit, mais des allégations trompeuses sont aussi régulièrement signalées. Certains trafiquants ne ménagent pas leurs efforts pour créer une apparence de légitimité derrière laquelle ils peuvent cacher leur vraie nature : « Les propriétaires d'entreprises qui pratiquent l'exploitation utilisent également des facilitateurs internet qui calquent les opérateurs légitimes présents sur le même marché, en utilisant des répertoires de services et des services de cartographie pour indiquer les plages horaires d'accueil et les services offerts » (éléments fournis par le Royaume-Uni). Plusieurs pays ont fourni des éléments probants montrant que les annonces sont généralement placées sur des « sites web connus » à la fois dans le pays d'origine de la victime (éléments fournis par la Lituanie) et dans le pays d'exploitation

(éléments fournis par la France et la Grèce). Un autre mode opératoire des trafiquants mis en lumière par les autorités britanniques consiste à utiliser des « plateformes internet pour établir les rôles ou les postes vacants dans lesquels placer les victimes, et créer des comptes bancaires pour recevoir les salaires » (modèle de « non-employeur »).

Les différentes juridictions peuvent considérer la traite comme une exploitation par le travail sous différentes formes, et les frontières entre la traite, les violations des droits du travail et le non-respect de la règlementation peuvent être floues et varier d'un pays à l'autre (sur le plan des principes, il est possible d'établir une échelle de gravité allant du non-respect de la règlementation aux situations où les passeports sont confisqués et la liberté de mouvement extrêmement restreinte). Ainsi, les autorités britanniques ont observé que certaines annonces mentionnaient explicitement des salaires en dessous du salaire minimum national ; toutefois, « ces [annonces] renvoient probablement davantage à des violations des droits du travail et au non-respect de la règlementation qu'à des cas de traite ». Les trafiquants peuvent « se garder de tout engagement lié aux salaires, ce qui leur permet également d'éviter tout risque d'attirer l'attention des services répressifs et des organismes de réglementation ». Cela démontre une fois de plus les difficultés que les autorités doivent surmonter pour repérer et retirer ce type d'annonces.

Ces annonces ne sont pas seulement publiées sur des sites spécifiquement consacrés à l'emploi, mais également diffusées et transmises par la voie des médias sociaux, par exemple dans des **groupes spécialisés dans la recherche d'emploi** et des **groupes d'entraide en ligne** (comme « Les Bulgares de l'étranger » ou « Nguoi tim viec », « Personnes à la recherche d'un emploi » en vietnamien). Plusieurs pays ont souligné que des pages web destinées à favoriser les échanges d'informations entre travailleurs migrants risquent fort de devenir un espace de recrutement ciblé par les trafiquants ; en effet, ces pages web sont souvent peu réglementées, car elles peuvent être gérées par des particuliers ou des associations aux ressources limitées. Dans certains cas, ces annonces peuvent circuler par le biais de groupes de recherche d'emploi créés dans des applications de messagerie, telles que Telegram.

Certaines annonces contiennent des informations extrêmement fallacieuses sur les conditions de travail et les rémunérations et souvent, l'« employeur » ou l'« agence » ne peut être contacté qu'à l'aide d'applications cryptées, telles que Viber ou WhatsApp. Ce type de messages peut atteindre un large public à moindre coût. Dans le cadre d'une expérience sociale, une organisation non gouvernementale (ONG) bulgare a publié une annonce sur une page Facebook proposant un emploi au Danemark de « collecte d'œufs de poisson volant verts » (jeu de mots en bulgare, l'expression « envoyer quelqu'un chercher des œufs de poisson volant verts » signifiant envoyer quelqu'un à la chasse au dahu), pour un salaire horaire exceptionnel. En moins d'une semaine, plus de 150 candidats ont présenté leur curriculum vitæ. Comme indiqué dans les documents soumis par plusieurs pays, les compétences techniques requises pour tirer parti des ressources en ligne et des médias sociaux à des fins de traite sont relativement modérées et équivalent aux compétences détenues par la plupart des internautes (accessoirement, très éloignées de celles des hackers et des cybercriminels avertis).

D'après les informations communiquées par la Bulgarie, les offres d'emploi sont souvent liées aux secteurs de l'agriculture (travailleurs saisonniers), du bâtiment, de l'industrie

manufacturière et de l'hôtellerie. D'autres secteurs considérés comme étant à risques sont le travail domestique et les services de soins. Les autorités allemandes ont repéré des publicités en ligne dans les secteurs suivants considérés comme à risques : les travaux agricoles saisonniers, les services de nettoyage, les restaurants ethniques, la construction, l'industrie agroalimentaire, le transport et la cosmétique (manucure et salons de massage). Les autorités portugaises ont fait état de plusieurs affaires liées à des offres d'emploi extrêmement fallacieuses, voire fausses, dans les secteurs de l'agriculture et de la construction. Les autorités suédoises ont insisté sur les services de nettoyage, la construction, la restauration et la manucure. De leur côté, les autorités chypriotes ont mis l'accent sur de fausses offres d'enseignement dans des universités et d'autres établissements d'enseignement supérieur.

Parmi les **tendances émergentes** en matière d'exploitation par le travail, les autorités bulgares ont signalé une hausse des recrutements par internet et par les réseaux sociaux. Cette tendance aurait été accélérée par l'épidémie de covid-19 et les mesures de santé publique associées. Selon les autorités chypriotes, allemandes et françaises, entre autres, les annonces diffusées dans les médias sociaux suivraient la même évolution. En France, les autorités ont commencé à observer le recours à des groupes communautaires d'entraide pour recruter et contrôler des victimes, et transférer des fonds. Enfin, la France et le Royaume-Uni ont souligné que l'économie à la tâche augmente les possibilités d'exploiter les victimes, car les documents d'identité ne sont pas régulièrement contrôlés et des individus peuvent travailler pour le compte de quelqu'un d'autre. Ainsi, une tierce partie peut recevoir tous les salaires sur un compte bancaire et n'en verser qu'une fraction à la personne qui travaille. D'après les autorités britanniques, « ce mode opératoire est apparu comme facilitant les violences liées au travail et le travail illégal, mais le niveau de contrôle qu'un titulaire de compte a sur les ressources financières du travailleur engendre un risque de traite ». Ce point de vue est partagé par les autorités françaises, selon lesquelles, bien qu'aucune affaire de traite n'ait été formellement recensée pour l'instant, certains travailleurs indépendants organiseraient des formes d'exploitation en sous-louant leur compte à des migrants en situation irrégulière et en les faisant travailler sans rémunération ou avec de très faibles rémunérations. Pour finir, les autorités belges ont relevé qu'il était possible d'acquérir des documents falsifiés sur des groupes qui vendent leurs services sur des applications de communication cryptées ; ces documents peuvent ensuite être utilisés pour faciliter l'exploitation par le travail (par exemple, de faux documents d'identité et permis de conduire, de faux contrats de travail et de faux permis de travail).

1.1.3. Le *dark web* et les cryptomonnaies

D'une manière générale, les États parties n'ont fourni que peu d'éléments démontrant que le *dark web* occupe une place importante dans la traite. Les seuls éléments présentés dans ce sens se rapportent à la diffusion de matériel d'abus sexuels d'enfants. La France a signalé des cas où des trafiquants achèteraient les numéros de cartes de crédit et d'autres informations sur le *dark web*, afin de réserver des chambres d'hôtel et des appartements ; néanmoins, cette activité semble plutôt limitée et accessoire. Les autorités françaises et norvégiennes ont indiqué que des abus sexuels pouvaient être diffusés en direct sur le *dark web*, mais les données fournies n'ont pas permis de déterminer si ces diffusions en direct impliquaient principalement des enfants ou pouvaient aussi concerner des victimes adultes. D'une manière

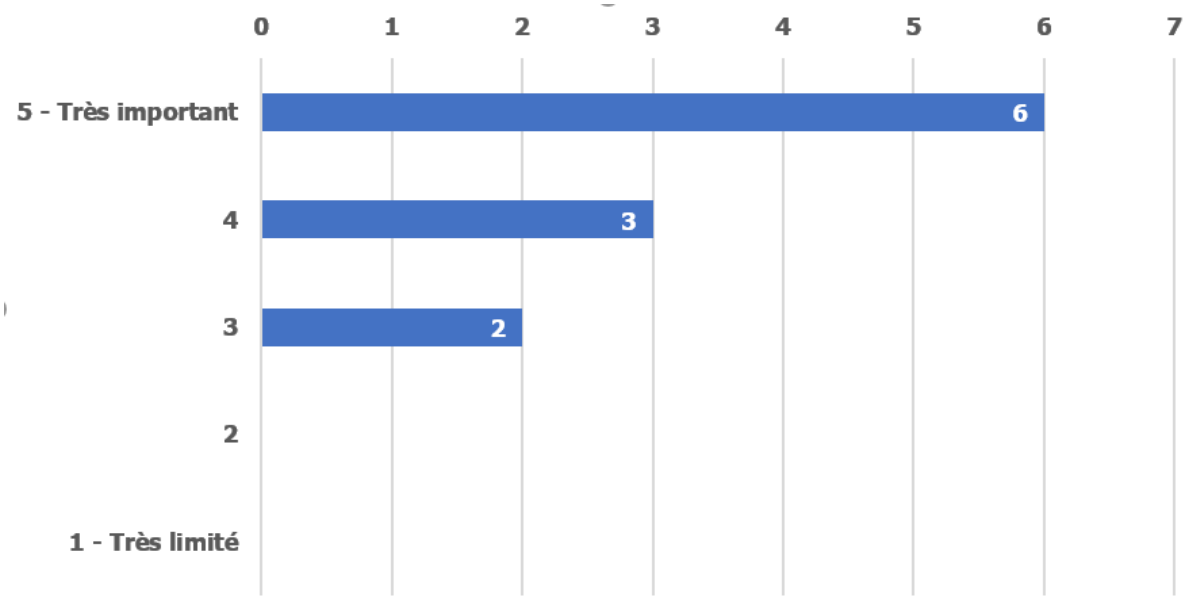
générale, il est peu probable que le *dark web* joue un rôle important pour l'instant, car les trafiquants chargés du recrutement et de l'exploitation tentent d'atteindre le plus large public possible, ce qui concorde peu avec le *dark web*, tel qu'il est actuellement configuré et utilisé. Pour le recrutement, les plateformes dotées d'un grand nombre d'utilisateurs sont privilégiées (l'un des principaux avantages de la technologie est la capacité de contacter un grand nombre de personnes pour un coût relativement faible). De la même façon, les annonces en ligne de services sexuels doivent toucher un grand nombre de personnes ; or, cela n'est pas possible sur le *dark web*, qui est un réseau secret.

Les cryptomonnaies semblent peu employées dans le domaine de la traite (en revanche, des données montrent qu'elles sont utilisées pour acheter des services de diffusion en direct d'abus sexuels d'enfants sur le *dark web*). Les transferts d'argent sont encore effectués avec des méthodes traditionnelles, par exemple par le biais d'entreprises comme la Western Union ou MoneyGram, ou parfois par l'entremise de personnes (dénommées les mules). Dans certains cas, des systèmes informels de transfert de fonds, tels que Hawala, peuvent être utilisés. Certains pays commencent à détecter des transferts d'argent par le biais d'applications de messagerie (WeChat, par exemple). Les produits fintech, par exemple les transferts fondés sur des applications, joueront probablement un rôle grandissant à l'avenir, à mesure qu'ils se généraliseront dans l'ensemble de la société (de même que les cryptomonnaies, une fois que – et si – elles atteignent une plus large circulation). Enfin, des éléments attestent de l'utilisation de cartes et de bons qui ne contiennent aucune information personnelle (comme les cartes PaySafe) pour payer des services en ligne, par exemple de l'espace publicitaire sur les sites web pour adultes.

1.2. Informations communiquées par des ONG

Trois ONG sur quatre interrogées pour la présente étude considèrent que la technologie a un impact « important » ou « très important » sur la traite, et aucune ONG ne qualifie l'impact de « limitée » ou « très limité » (figure 2)[5].

Figure 2. Impact de la technologie sur la traite : ONG



Note : N = 11

Dans l'ensemble, les données qualitatives fournies par les ONG qui apportent une assistance directe aux victimes de la traite dressent un tableau similaire aux États parties. Des ONG ont étudié l'utilisation d'internet et des médias sociaux à tous les stades de la traite, et en particulier concernant a) le recrutement ; b) l'exploitation ; et c) l'exercice d'une emprise et d'une pression sur les victimes. Les ONG partagent largement l'idée selon laquelle l'impact de la technologie sur la traite a augmenté pendant la pandémie de covid-19. Toutefois, la pandémie n'aurait peut-être accéléré qu'une tendance déjà existante. Comme l'a relevé KOK, un réseau allemand composé de 37 ONG gérant des services de conseil spécialisés pour les victimes de la traite, « depuis quelques années, les centres de conseil ont indiqué qu'internet et les médias sociaux jouaient un rôle de plus en plus important dans la traite ».

Les membres de La Strada International, plateforme réunissant 30 ONG européennes de lutte contre la traite dans 23 pays européens, ont signalé des affaires où des victimes de la traite avaient été recrutées sur différentes plateformes en ligne, notamment des médias sociaux et des sites de rencontre, à des fins d'exploitation sexuelle et d'exploitation par le travail. Ces affaires concernaient le recrutement d'adultes comme d'enfants. D'après les données fournies par CKM (ONG néerlandaise), les contacts en ligne jouent un rôle particulièrement important lorsque les victimes et les trafiquants ne se connaissent pas : dans presque 80 % de ces affaires, le premier contact se fait en ligne, par exemple par le biais de médias sociaux ou d'applications de rencontre (informations communiquées par La Strada International). Cela

[5] Une ONG n'a pas répondu à cette question.

est particulièrement vrai pour les victimes mineures. À la suite d'entretiens réalisés avec des victimes de la traite, l'ONG albanaise « Différents et égaux » a constaté que les médias sociaux « [étaient] devenus les principaux moyens » de recrutement des victimes pour les trafiquants. Le constat est particulièrement vrai pour les filles [recrutées] à des fins d'exploitation sexuelle ». En Suisse, FIZ a également observé une tendance émergente au recrutement des victimes de la traite par le biais de plateformes de médias sociaux et d'applications de rencontre. D'une manière générale, chacun s'accorde à reconnaître que la technologie est de plus en plus utilisée et prend une importance croissante dans les affaires de traite, et que ce phénomène à la hausse s'est accéléré ces dernières années.

1.2.1. La traite aux fins d'exploitation sexuelle

Les stratégies et les mécanismes qui régissent le recrutement par le biais de médias sociaux relevés par les ONG correspondent aux informations déjà évoquées dans la section 1.1.1 ci-dessus. Des éléments attestent de l'existence de la technique du *loverboy*, qui consiste à nouer une relation personnelle/romantique par la voie des médias sociaux en vue d'exploiter la victime ultérieurement. De faux profils de médias sociaux sont établis à cette fin. Les victimes sont généralement des mineurs ou de jeunes adultes. La Strada Moldova a constaté que les enfants qui vivent en zone rurale ou dans des familles socialement vulnérables ou ayant des difficultés financières sont particulièrement fragiles.

À propos du stade de l'exploitation, des ONG ont mis en évidence des mécanismes semblables à ceux décrits précédemment dans le présent rapport. Ceux-ci englobent le recours à des sites web pour proposer des services sexuels. D'après le réseau KOK (Allemagne), il est plus difficile pour la police et les services de conseil de prendre contact avec les prestataires de services sexuels en ligne que de prendre contact avec des individus qui proposent les mêmes services dans les établissements enregistrés, ce qui complique l'identification des cas de traite.

Par ailleurs, s'agissant de l'exploitation sexuelle, l'hébergement peut être réservé en ligne sur des sites spécialisés (éléments concernant la France fournis par La Strada International).

1.2.2. La traite aux fins d'exploitation par le travail

S'agissant du recrutement aux fins d'exploitation par le travail, des ONG ont fourni des informations supplémentaires sur les mécanismes décrits dans la section 1.2.2, en particulier l'utilisation d'offres d'emploi en ligne fausses et grossièrement trompeuses. Ainsi, en Albanie, l'ONG « Différents et égaux » a repéré des offres d'emploi en ligne liées à des pratiques d'exploitation ciblant des femmes comme des hommes. En Serbie, des membres de l'ONG Astra ont exprimé leur crainte que même des organismes officiellement inscrits au Registre des entreprises et munis d'un licence officielle ne proposent des emplois illégaux. Ils ont également relevé « un grand nombre » d'annonces « illicites », c'est-à-dire émises par de faux représentants d'organismes, et d'annonces liées à des pratiques d'exploitation. Selon eux, la plupart des annonces en ligne « ne sont soumises à aucune forme de contrôle ou de surveillance ». Des ONG allemandes et suisses ont également mis en lumière des processus de recrutement en ligne pour des emplois inexistants ou caractérisés par des conditions de

travail abusives. Dans le même temps, « les recrutements en ligne prolifèrent », comme l'a souligné le Centre pour les droits des migrants (Irlande).

Dans les documents soumis par les ONG, aucun élément n'atteste que la technologie joue un rôle clé dans le contexte de l'exploitation par le travail. Toutefois, il est apparu flagrant que les travailleurs relevant de l'économie à la tâche, en particulier les plateformes en ligne de livraison de produits alimentaires et autres, pouvaient être exposés à des mauvais traitements de la part des trafiquants. Comme l'a noté le Comité contre l'esclavage moderne (CCEM), ONG française membre de La Strada International, aucune affaire de traite n'a encore été recensée dans ce secteur, mais les procédures actuellement mises en œuvre par les plateformes de livraison en ligne peuvent permettre aux trafiquants d'employer des victimes sous l'identité d'une autre personne.

1.2.3. L'exercice d'une emprise et d'une pression sur les victimes

Des ONG ont indiqué que la technologie était employée pour exercer **une emprise sur les victimes**, en particulier dans le cadre de l'exploitation sexuelle. Des cas ont été relevés où les trafiquants utilisaient des outils de surveillance vidéo, des téléphones portables, des applications et des logiciels de localisation (données fournies par La Strada International). Les trafiquants recourent également aux TIC, par exemple les médias sociaux, pour menacer les proches de toute victime qui tenterait d'échapper à sa condition (données communiquées par KOK, Allemagne). Des informations similaires ont été recueillies par l'ONG Astrée en Suisse.

De plus, les victimes peuvent subir des **chantages** par la voie des médias sociaux et d'autres plateformes en ligne. Le chantage est souvent associé à la menace de divulguer des informations « compromettantes », y compris des photos et d'autres données à caractère personnel. (KOK signale le cas d'un trafiquant qui exerce un chantage sur sa victime en la menaçant de révéler sa séropositivité sur Facebook).

Élément essentiel, certaines ONG ont souligné que les trafiquants pouvaient utiliser les TIC, notamment les médias sociaux et les applications cryptées, pour **garder le contact** avec une victime de la traite, même lorsque celle-ci ne se trouve plus en situation d'exploitation – souvent pour l'empêcher de déposer plainte et de se tourner vers la justice. Selon CKM, aux Pays-Bas, environ un tiers des victimes interrogées seraient soumises à cette pression (informations fournies par La Strada International).

1.2.4. Tendances émergentes

KOK et La Strada Moldova ont observé une augmentation de l'exploitation des enfants par la voie des **webcams et des réseaux sociaux**. D'après La Strada Moldova, les trafiquants entrent en contact avec les enfants sur les réseaux sociaux ou des **jeux en ligne**, se lient d'amitié avec eux ou simulent une relation amoureuse. Certains trafiquants se feraient passer pour des représentants d'agences de mannequins. L'enfant est invité à partager des photos intimes qui sont ensuite utilisées pour le faire chanter. À ce stade, les trafiquants demandent à leurs victimes de produire et de partager toujours plus de matériels à contenu sexuellement explicite et de diffuser en direct des actes sexuels. Dans certains cas, les victimes subissent des pressions pour recruter d'autres enfants ou faire des rencontres hors ligne en vue de rapports sexuels. (KOK a observé des pratiques similaires.)

Plus généralement, La Strada International et KOK ont mis l'accent sur les vulnérabilités croissantes engendrées par la **publication d'un large volume d'informations personnelles** sur les médias sociaux et d'autres plateformes en ligne, et sur la facilité avec laquelle certaines personnes nouent des contacts intimes avec des étrangers sur les plateformes en ligne[6]. La tendance est particulièrement visible dans les jeunes générations. La technologie peut apporter des perspectives et des avantages considérables, y compris des échanges enrichissants, mais également aggraver les vulnérabilités. Par exemple, le fait de partager des images sexuellement explicites (*sexting*) ne va pas sans poser des risques liés à la traite et, plus généralement, des risques de chantage. Les données statistiques restent insuffisantes, mais une recherche commandée par La Strada Moldova en 2020 sur un échantillon représentatif d'enfants âgés de 9 à 17 ans fournit des indications contextuelles intéressantes. Selon ces travaux, 13 % des enfants moldaves considèrent qu'il est normal que des personnes qui s'aiment se partagent des photos intimes en ligne[7] ; 35 % ont déjà communiqué avec une personne inconnue en ligne et 20 % ont rencontré dans le monde réel des personnes dont ils avaient fait connaissance sur internet (2 % d'entre eux ont déclaré que la rencontre les avait bouleversés).

1.3. Autres informations issues de l'analyse contextuelle

La technologie peut avoir une incidence à tous les stades de la traite, mais son rôle est particulièrement préoccupant à deux stades du processus : le recrutement et l'exploitation (Latonero 2012 ; Di Nicola *et al.* 2017, entre autres).

La technologie peut intervenir pendant la phase du **recrutement** en facilitant l'identification et la localisation des victimes potentielles ainsi que la prise de contact. Les principaux changements dus à la technologie sont l'élargissement du champ d'action des trafiquants à la recherche de victimes, et l'abaissement des « frais de fonctionnement » liés à l'identification des victimes potentielles et à la prise de contact (Raets et Janssens 2018). Les trafiquants gardent cependant un champ d'action limité, car les interactions en personne continuent de jouer un rôle crucial. Selon la forme d'exploitation, différents mécanismes entrent en jeu, de sorte qu'il est indispensable de distinguer le recrutement aux fins d'exploitation sexuelle du recrutement aux fins d'exploitation par le travail[8].

S'agissant du recrutement des victimes aux fins d'**exploitation sexuelle**, la technologie peut favoriser le recrutement de deux façons :

a. Elle peut faciliter la création et la diffusion d'**offres d'emploi en ligne** qui promeuvent des possibilités d'emploi, le plus souvent à l'étranger, dans un certain nombre de secteurs allant de l'administration, du nettoyage ou de la garde des enfants (Europol 2014) au divertissement, au mannequinat, aux services d'escorte et à l'industrie du sexe (Conseil de l'Europe 2007 ; UN.GIFT 2008 ; Di Nicola *et al.* 2017).

[6] Il convient également de relever que les médias sociaux et les TIC peuvent aussi plus largement aider les ONG à identifier et à entrer en contact avec les victimes potentielles de la traite (pour en savoir plus, voir chapitre 3).
[7] Seules 1 % des personnes interrogées ont explicitement indiqué qu'elles partageaient des photos et des vidéos intimes (sexuellement explicites). Toutefois, ce chiffre doit être interprété avec prudence, car il a peut-être été influencé par un effet de désirabilité sociale.
[8] Rien ne prouve que la technologie soit utilisée pour le recrutement aux fins d'autres types d'exploitation, comme la mendicité forcée.

b. Elle peut faciliter l'identification et la prise de contact avec les victimes potentielles, souvent des personnes vulnérables, par la voie des médias sociaux et d'autres applications de gestion des contacts personnels (voir, par exemple, Di Nicola *et al.* 2017). Cela peut être considéré comme un type spécifique de **sollicitation en ligne d'enfants à des fins sexuelles**. La technique de recrutement du *loverboy* fondée sur la technologie s'appuie souvent sur ce mode d'approche. Les sites et applications spécifiques utilisés peuvent changer selon les comportements en ligne et les préférences propres à chaque pays. Certaines sources ont souligné une pratique émergente qui consiste à rassembler des « données compromettantes » pendant la phase de recrutement, puis à faire chanter les victimes pour prendre le contrôle sur elles (pratique semblable à la « sextorsion » ; Europol 2020).

S'agissant du recrutement aux fins d'**exploitation par le travail**, la technologie intervient principalement par la diffusion d'offres d'emploi en ligne. Des secteurs spécifiques ont été identifiés comment étant particulièrement exposés au risque de traite : les femmes sont plus susceptibles d'être embauchées dans les soins à la personne, les soins à domicile, la coiffure et la garde d'enfants, tandis que les hommes ont plus de chances d'être recrutés dans l'agriculture, la construction, le transport ainsi que la collecte et la distribution de sacs de dons (Europol 2014 ; Di Nicola *et al.* 2017 ; voir aussi Fine Tune Project 2011 et Conseil de l'Europe 2007). Parmi d'autres secteurs recensés figurent la restauration, l'industrie alimentaire et le conditionnement (Fine Tune Project 2011). Les annonces peuvent être publiées sur des sites web licites, largement consultés, publiées sur des sites ponctuels et/ou diffusées par la voie des médias sociaux.

Certaines sources semblent mettre en avant la séparation physique entre les trafiquants et les victimes grâce à la technologie (OSCE 2020), mais la réalité est plus complexe. De solides éléments laissent à penser que l'utilisation de la technologie complète plus qu'elle ne remplace les relations personnelles dans le monde réel. La technologie et les échanges traditionnels doivent plutôt être considérés comme intégrés. Il est fort probable que l'ampleur de l'impact de la technologie dépende de facteurs propres aux populations vulnérables dans des pays spécifiques, à savoir : a) l'utilisation d'internet et des médias sociaux, en général ; b) l'utilisation d'internet et des médias sociaux dans la recherche d'emploi ; et c) les connaissances technologiques de certains groupes vulnérables.

Des recherches ont montré que les victimes étaient généralement, mais pas toujours, recrutées dans leur pays d'origine, puis exploitées à l'étranger. Cette conclusion était déjà avancée par le Conseil de l'Europe (2007) et des données ultérieures, bien que limitées, la confirment. Il en résulte que, pour contrer le phénomène, il conviendra probablement d'adopter des mesures bilatérales et multilatérales.

S'agissant du **stade de l'exploitation**, la technologie peut jouer un rôle relatif à l'exploitation sexuelle. En revanche, la présente étude ne donne aucun élément attestant que la technologie jouerait un rôle important dans l'exploitation par le travail (Di Nicola *et al.* 2017 ; Raets et Janssens 2018, et d'autres).

Pour l'**exploitation sexuelle**, la technologie peut intervenir de deux façons différentes :

a. Elle permet aux trafiquants de **contrôler** les victimes sans être physiquement présents, en utilisant le système GPS ou d'autres applications mobiles. Les chantages et l'exploitation de données compromettantes contre les victimes sont également mentionnés

comme des stratégies possibles pour exercer le contrôle (Raets et Janssens 2018). Un élément de preuve inédit semble montrer une proportion relativement faible de cas où des chantages ont été exercés aux Pays-Bas (8,8 % de cas, non daté ; source : OSCE 2020).

b. Elle peut faciliter la **vente** de services sexuels fournis par des victimes de la traite sous la forme d'annonces en ligne ciblant des clients finals. Ces annonces sont souvent publiées sur des sites web spécialisés ou des pages web ponctuelles.

Globalement, l'impact de la technologie sur le **transport** est considéré comme limité, car les victimes voyagent souvent librement et n'expérimentent la contrainte qu'une fois arrivées dans le pays de destination (phase d'exploitation ; données probantes fournies par les services répressifs bulgares, roumains et italiens et présentées dans l'étude de Di Nicola *et al.* 2017). Les outils technologiques, tels que les téléphones portables et les applications ainsi qu'internet, sont utilisés pour coordonner les dates et lieux des rencontres, acheter les billets et organiser l'ensemble des déplacements. Les trafiquants peuvent recourir au dark web pour acheter des billets falsifiés ou des numéros de cartes de crédit qui serviront ensuite à acheter des documents de voyage (falsifiés), mais une étroite évaluation des multiples sources – travaux universitaires ou documents des services répressifs accessibles au public – semble indiquer que l'utilisation du dark web reste très restreinte.

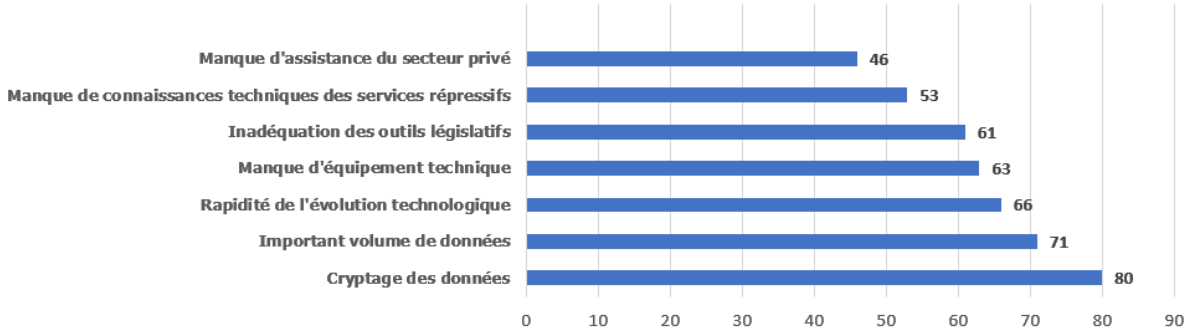
2. Difficultés dans la détection, les enquêtes et les poursuites concernant la traite facilitée par la technologie

Le présent chapitre examine les difficultés causées par l'utilisation de la technologie dans le contexte de la traite et non pas, plus largement, toutes les difficultés rencontrées par les États parties à propos de la traite. Il commence par décrire les difficultés relatives aux enquêtes, puis examine celles relatives aux poursuites et à la coopération internationale, à l'aide d'informations communiquées par les États parties. Celles-ci sont complétées par des données factuelles recueillies auprès d'ONG, et par l'analyse de la documentation existante.

2.1. Difficultés dans les enquêtes

On a présenté aux États parties une liste de sept difficultés pouvant entraver les enquêtes, qui a été établie après examen de la base de connaissances existante et de travaux précédents réalisés par le GRETA et le Conseil de l'Europe, notamment l'atelier de 2019 intitulé « Intensifier l'action du Conseil de l'Europe contre la traite des êtres humains à l'ère du numérique »[9]. La figure 3 présente le **score de gravité** pour chacune des sept difficultés[10].

Figure 3. Scores de gravité des difficultés constatées dans les enquêtes



Remarque : échelle de scores = [0, 100]

Le cryptage des données est retenu comme la plus grave difficulté (score de 80). À l'extrémité opposée du classement, l'absence d'assistance des entreprises du secteur privé est considérée comme la difficulté la moins grave. Mise à part cette absence d'assistance, toutes les difficultés ont un score supérieur à 50, ce qui signifie qu'elles ont un impact général plus important que celui d'un problème « mineur ».

Les difficultés sont évaluées chacune à leur tour dans les sections suivantes : le cryptage des données (2.1.1), le volume important de données à traiter (2.1.2), le manque d'équipement technique (2.1.3), les connaissances techniques insuffisantes des services répressifs (2.1.4) et la rapidité de l'évolution technologique (2.1.5). Les difficultés relatives à l'assistance du secteur privé sont examinées à la section 4 du présent chapitre, et celles qui concernent les outils législatifs sont traitées au chapitre 5. Il convient de relever que, bien que présentées

[9] https://www.coe.int/fr/web/anti-human-trafficking/-/round-table-on-action-against-trafficking-in-human-beings-in-the-digital-age

[10] Pour chaque difficulté, il a été demandé aux États parties d'évaluer le score de gravité en utilisant un barème de trois points (réponses « Normalement pas un problème », « Problème mineur » et « Problème majeur » respectivement transformées en 0, 1 et 2). Les scores ont ensuite été rééchelonnés de 0 à 100.

séparément, certaines difficultés sont étroitement liées. Par exemple, le cryptage (et décryptage) des données nécessite d'investir régulièrement dans les technologies, et de développer les compétences au sein des services répressifs. Les États parties ont également été invités à signaler toute autre difficulté rencontrée en sus des sept déjà recensées. Ces difficultés supplémentaires sont mentionnées dans la section 2.1.6 ci-dessous.

2.1.1. Cryptage des données

Le cryptage des données est considéré comme constituant la principale difficulté rencontrée par les autorités lorsqu'elles enquêtent sur les affaires de traite facilitée par les TIC. L'impact des réseaux TOR/Darkweb ou des réseaux de téléphones cryptés, tels que EncroChat, est jugé négligeable, mais les pays ont mis l'accent sur les difficultés posées par les protocoles de cryptage inclus dans des applications et des services en ligne largement utilisés (comme WhatsApp et Telegram). Le cryptage de données peut « rendre toute récupération de données impossible pour une enquête de police scientifique » (autorités albanaises). Les autorités de la Bosnie-Herzégovine ont affirmé que « de plus en plus d'enquêtes se [heurtaient] à des disques durs cryptés, des appareils téléphoniques verrouillés, des clés USB et des données cryptées ». D'après les autorités islandaises, la plupart des problèmes rencontrés par les services répressifs concernent des « comptes et applications de messagerie anonymes et chiffrés, tels que ProtonMail, ou la [difficulté d'accéder aux] renseignements sur les abonnés, par exemple ». Le suivi et la surveillance sont également limités, voire impossibles – même avec un mandat judiciaire et contrairement aux autres types de communication. Les autorités autrichiennes ont souligné l'impossibilité de placer les produits de téléphonie VoIP sous surveillance, et les autorités françaises ont mis en évidence « l'impossibilité de surveiller la messagerie instantanée (WhatsApp, Messenger, TikTok, WeChat, Snapchat) », ce qui « entrave considérablement les enquêtes (difficultés d'identifier les trafiquants et les victimes, d'établir des liens entre les personnes, de recueillir des données sur la contrainte et la subordination) »[11]. Les autorités belges ont en outre indiqué que les activités d'investigation menées dans des canaux cryptés fermés nécessitaient l'aide d'informateurs et d'agents infiltrés, ce qui peut poser problème dans certaines juridictions (notamment en Belgique). Les autorités irlandaises observent que « le cryptage se renforce » et plusieurs États parties font le même constat. Le grand public dispose d'un éventail de technologies cryptées de plus en plus large, avec un nombre croissant d'applications de messagerie instantanée conçues pour renforcer le cryptage et diminuer le volume de données utilisateur générées (Threema ou Signal, par exemple).

Comme le mentionne le document soumis par les autorités suisses, l'incidence du cryptage varie selon que les enquêteurs ont accès à l'appareil physique ou pas. Si l'appareil se trouve physiquement entre les mains des enquêteurs, le « cryptage des données est un problème mineur et les données peuvent être décryptées par les services de police spécialisés ». (Le Luxembourg fait une observation similaire.) Toutefois, les agents dotés de ces compétences techniques n'étant pas légion, ces services spécialisés risquent fort d'être rapidement débordés – ce qui peut retarder les enquêtes. Si les services répressifs n'ont pas accès à l'appareil physique, « les enquêtes sont plus difficiles » (document soumis par les autorités

[11] Cette observation se retrouve dans le document soumis par les autorités grecques.

suisses). Dans certains pays, par exemple le Royaume-Uni, les services répressifs ont le pouvoir d'exiger qu'une personne donne le mot de passe et le code PIN de son téléphone portable. Néanmoins, comme l'indique le document soumis par les autorités britanniques, certains problèmes persistent : « même une fois l'arrestation et la saisie de ces appareils réalisées, il peut être difficile d'accéder aux communications importantes », surtout lorsque l'appareil dispose de fonctions de sécurité de haut niveau. Les autorités belges sont parvenues à la même conclusion, en expliquant que le décryptage des algorithmes les plus complexes posait problème (et nécessitait d'investir davantage dans de nouveaux outils de décryptage).

Quelques pays ont mentionné l'existence d'outils permettant au moins de déchiffrer certains types d'algorithmes. Il apparaît cependant clairement que le paysage en constante évolution exige des investissements (massifs) dans la formation et les ressources logicielles. Les mesures prises pour résoudre ce problème englobent la création d'unités/centres de cybercriminalité spécialisés dans le décryptage, comme l'a fait la Norvège, par exemple. De son côté, la France travaille actuellement à l'élaboration d'un appareil de craquage de mots de passe « au niveau central ».

Les autorités slovènes ont soulevé la question des coûts liés au décryptage des données électroniques. Ces coûts ont engendré la nécessité d'embaucher des experts hautement qualifiés, et d'acheter des logiciels spécialisés capables de déjouer le cryptage. En outre, comme les protocoles de cryptage évoluent sans cesse, il est nécessaire de tenir constamment les logiciels à jour, ce qui engendre souvent des frais de licence élevés.

De plus, il pourrait être utile de partager les ressources au niveau supranational pour élaborer des produits technologiques, tels que des logiciels de décryptage et des robots d'exploration, comme l'ont suggéré, entre autres, les autorités suédoises. D'une manière générale, il ressort des informations fournies que les pays pourraient **favoriser davantage l'échange de connaissances et mutualiser l'élaboration de produits technologiques**. Une coopération plus étroite et bien financée s'est avérée très fructueuse, par exemple dans l'infiltration du réseau de messagerie cryptée Encrochat utilisé dans toute l'Europe par des groupes de criminalité organisée de haut niveau. (Il en est résulté de multiples enquêtes et procès très médiatisés en France, aux Pays-Bas, au Royaume-Uni et en Suède, entre autres pays.)

Dans certains cas, comme l'ont fait savoir les autorités françaises, le cryptage peut être surmonté en utilisant différentes techniques d'enquête, par exemple la « surveillance technique des lignes téléphoniques des victimes [qui] reste un moyen efficace, en attendant une technologie qui permettra de contourner le cryptage ».

2.1.2. Volume de données important

Les dispositifs de communications électroniques et de TIC engendrent un volume de données en croissance permanente qui, à son tour, fait peser une lourde charge sur les enquêteurs. Comme l'ont indiqué plusieurs pays, le gros volume de données générées se répercute sur la capacité d'extraire les données, car cela exige un équipement technique puissant. L'analyse et l'examen minutieux d'une quantité massive d'informations constituent également une véritable gageure. Les smartphones ont des capacités de stockage toujours plus grandes ; les données factuelles générées par les utilisateurs revêtent des formes multiples : de (longues)

conversations en ligne, mais aussi des images, des enregistrements vidéo et des messages vocaux qui peuvent prendre des « semaines » pour être analysés (informations émanant de la Suisse). La tâche est particulièrement complexe lorsqu'« il n'est pas possible de rechercher un mot-clé spécifique et que les [enquêteurs] doivent passer toutes les données au crible » (informations fournies par la Suisse). D'après les autorités suisses, « l'expérience et la pratique ont montré que le volume des données avait considérablement augmenté avec les médias sociaux modernes, nécessitant de très longues activités d'investigation […] susceptibles d'occuper l'enquêteur pendant des mois et de créer des goulets d'étranglement ».

Le volume de données important nécessite souvent des logiciels spécialisés, ainsi qu'une formation spécialisée sur la systématisation et l'exploration de ces masses de preuves. Selon les autorités britanniques, « les marchés internet et les réseaux sociaux engendrent une immense quantité de données [qui] peut être difficile à analyser, et il est coûteux d'acquérir des licences ou de développer des outils qui puissent efficacement analyser ces informations ». Les autorités françaises ont également insisté sur la nécessité d'élaborer des outils capables d'aider les enquêteurs à traiter de gros volumes de données, par exemple en utilisant des algorithmes d'intelligence artificielle. (Les autorités espagnoles ont émis une observation similaire.) D'après les autorités norvégiennes, le volume de données électroniques rend les « enquêtes plus complexes et nécessite [donc] des méthodes d'investigation davantage centrées sur la technologie »[12]. Ces méthodes « débouchent [pourtant souvent] sur un gros volume de données [dont] seule une infime partie […] est utile à l'enquête ».

Il existe un large consensus sur l'impérieuse nécessité de renforcer la capacité de traiter de gros volumes de preuves électroniques. Toutefois, ces capacités doivent être constamment actualisées pour rester en phase « avec des catalyseurs internet en constante mutation en raison de la rapidité de l'évolution technologique » (document soumis par les autorités britanniques). Les autorités néerlandaises partagent ce constat, en mettant en avant le volume croissant de données issues des plateformes en ligne et des médias sociaux, ainsi que les problèmes liés aux **comportements fluctuants** de leurs utilisateurs, ce qui rend « les recherches difficiles ». La disponibilité des outils numériques est considérée comme la première étape (nécessaire) ; parmi les étapes suivantes requises figure une adaptation constante à l'environnement numérique sur le plan technologique et comportemental.

En outre, il est souvent nécessaire de traiter et d'analyser des volumes de données importants dans un délai très court. Par exemple, lorsqu'un suspect est appréhendé, les agents sont tenus d'examiner une masse de preuves électroniques dans des délais très serrés, comme l'ont indiqué les autorités slovènes. Le laps de temps restreint dont disposent généralement les enquêteurs pour examiner le matériel exige les « **meilleures technologies pour chercher l'information et la classer »** (données issues du Royaume-Uni). En outre, plusieurs États parties ont souligné que les données électroniques recueillies dans le cadre d'enquêtes sur la traite sont souvent dans une langue que les enquêteurs ne maîtrisent pas, ce qui exige des traductions longues et coûteuses. (Cette question est particulièrement critique dans les pays de destination.)

[12] Les autorités portugaises ont émis des observations similaires.

2.1.3. Manque d'équipement technique

Plusieurs pays ont mentionné le manque d'équipement technique comme un défi majeur pour les enquêtes. Il englobe un nombre souvent insuffisant de machines capables d'accomplir des tâches spécialisées, comme le craquage du cryptage, et des difficultés à maintenir les ressources logicielles et matérielles à jour. Comme cela a déjà été mentionné ci-dessus, 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 technique. Cela grève considérablement les budgets de la police. Dans les pays où le pouvoir d'achat est le plus bas, il est difficile de maintenir l'équipement technique à jour. S'ils n'avaient pas été aidés par des partenaires internationaux et des donateurs du secteur privé, certains pays auraient déjà été exclus du marché international pour les outils techniques spécialisés. (Ce point émane explicitement des autorités albanaises, mais il ressort aussi de documents soumis par d'autres pays.) Néanmoins, le problème ne se limite en aucune façon aux pays moins pourvus. L'Allemagne, la Belgique, la Suède, la France et le Royaume-Uni, entre autres, ont exprimé leur vive préoccupation face au coût des logiciels et du matériel spécialisés.

La plupart des affaires de traite ont une ampleur internationale et impliquent souvent des victimes provenant de pays moins pourvus, qui sont exploitées dans des nations plus prospères. Il en résulte la nécessité pour les pays d'établir une coopération internationale sur des affaires spécifiques. Il en ressort également la nécessité souvent négligée de programmes renforcés d'assistance technologique pris en charge par les pays de destination au bénéfice des pays d'origine des victimes – outre les programmes multilatéraux existants, tels que ceux gérés par l'Union européenne, qui apportent déjà une aide financière pour la mise à niveau de l'équipement technique.

2.1.4. Manque de connaissances techniques des services répressifs

Pour que les services répressifs utilisent efficacement l'équipement technique, ils doivent bénéficier d'une formation efficace. Plus généralement, il est tout aussi important, voire plus, d'investir dans le capital humain, à savoir la formation et les connaissances techniques des policiers, que dans les logiciels et le matériel. Les États parties ont largement insisté sur la nécessité de fournir ces formations et des connaissances techniques supplémentaires aux policiers. Selon les autorités belges, il est « impératif » de diminuer la « **fracture numérique entre les trafiquants et les policiers** ». Les États parties ont souligné la nécessité de transmettre un large éventail de connaissances.

Premièrement, il est nécessaire d'améliorer les connaissances sur l'émergence des nouvelles tendances et l'évolution de l'utilisation de la technologie par les trafiquants et les victimes. Deuxièmement, les pays ont souligné l'importance d'améliorer les connaissances sur l'arrivée de nouveaux services et de nouvelles applications sur un marché informatique qui se caractérise par des changements rapides. Troisièmement, il est nécessaire de se tenir informé sur l'élaboration de nouveaux protocoles de sécurité et de nouvelles méthodes de cryptage. Les connaissances doivent être habilement diffusées au sein d'une organisation. En effet, l'absence d'agents spécialisés au niveau local peut entraîner un **engorgement des services d'investigation**, s'il est continuellement fait appel à l'assistance d'une unité centralisée (débordée). Il est indispensable que les pays se penchent sur ce problème, qui figure dans

les documents soumis par plusieurs États parties, comme l'Albanie, la Belgique, l'Islande, la France, le Portugal, la Slovaquie et la Slovénie (pour en savoir plus sur la formation, voir chapitre 4).

Plusieurs pays ont souligné la nécessité de **dispenser des connaissances techniques supplémentaires aux policiers généralistes**. Outre le fait d'apporter aux agents spécialisés des connaissances techniques approfondies, relatives à des logiciels ou à des techniques de décryptage spécifiques, il est nécessaire de transmettre un ensemble de compétences numériques de base et de connaissances techniques à tous les policiers. Il est indispensable que les policiers qui arrivent les premiers sur une scène de crime possèdent ces connaissances. Comme l'ont relevé les autorités albanaises, les erreurs faites par les premiers intervenants « peuvent compromettre la collecte de preuves électroniques valables pour les analyses futures ». Une formation adéquate sur l'obtention et la gestion de **preuves électroniques** doit être dispensée à l'ensemble des policiers. En outre, les policiers devraient suivre régulièrement des programmes de perfectionnement pour rester à niveau dans ce domaine.

Par ailleurs, ces connaissances techniques élémentaires seraient un atout réel pour tous les enquêteurs, mais certaines affaires plus complexes pourraient nécessiter de monter des équipes dotées d'un ensemble de compétences pluridisciplinaires (en regroupant, par exemple, des enquêteurs, des spécialistes de la finance et des experts en cybercriminalité). Le cas échéant, les pays pourraient envisager d'adopter – ou de renforcer – des mesures qui faciliteraient la création rapide de telles équipes, voire d'intégrer l'interdisciplinarité comme une fonction structurelle du travail policier moderne. Le dispositif pourrait s'étendre aux équipes communes d'enquête internationales, en joignant à ces équipes des experts en technologie et communication (suggestion émise par les autorités bulgares).

D'après les autorités suisses, « pour les services répressifs, la nécessité de rester à la pointe du progrès technologique constitue un défi considérable » et les enquêteurs d'aujourd'hui doivent posséder une certaine expertise en matière de traite et de TIC, notamment la maîtrise des médias sociaux et des compétences techniques. Les autorités françaises ont évoqué la nécessité de former les fonctionnaires aux nouvelles technologies et aux techniques d'enquêtes financières. Les autorités bulgares ont mentionné une affaire dans laquelle un ensemble de techniques d'enquête en ligne et hors ligne avait été employé en coopération avec les autorités françaises. Partant de la découverte d'images pornographiques d'enfants, les enquêteurs étaient parvenus à trouver une adresse IP, puis à la localiser dans un hôtel. Lors de leur descente à l'hôtel, ils avaient trouvé des femmes forcées de fournir des services sexuels et obtenu une série de surnoms Facebook d'autres victimes ; celles-ci avaient pu être identifiées lorsqu'elles avaient utilisé leur profil Facebook. Au final, 60 victimes de la traite aux fins d'exploitation sexuelle avaient été recensées, dont un enfant contraint de produire du matériel pornographique et 18 trafiquants. Cet exemple montre bien la nécessité pour les enquêteurs de disposer de solides connaissances sur les techniques d'investigation en ligne comme hors ligne, qui leur seront très probablement indispensables dans les enquêtes relatives à la traite. Cela nécessite naturellement une formation continue.

2.1.5. Rapidité de l'évolution technologique

Le rythme rapide de l'évolution technologique est un problème transversal qui se répercute sur tous les enjeux susmentionnés : le décryptage, la formation des policiers, l'équipement technologique et la collecte de preuves électroniques. Pour en savoir plus, consulter les observations ci-dessus.

2.1.6. Autres difficultés dans les enquêtes

Plusieurs pays ont mis en lumière un problème relatif à certaines **obligations de conservation des données** imposées aux fournisseurs de services internet (FSI) qui ne sont pas adéquates, et son impact sur les enquêtes. En Bulgarie, par exemple, la législation en vigueur impose aux FSI de stocker ces données pendant six mois – une durée qui est jugée trop courte pour réaliser des enquêtes solides. Les autorités néerlandaises et maltaises ont ainsi allongé la durée de rétention des données. Les autorités norvégiennes ont relevé qu'en vertu de la législation nationale, les FSI ne sont pas autorisés à stocker des informations sur des adresses IP pendant plus de 21 jours, ni tenus de sauvegarder des données sur le lien entre les abonnés et les adresses IP. Les autorités bulgares et roumaines ont recommandé une harmonisation des réglementations nationales afférentes au stockage de données sur le trafic internet, ainsi que des méthodes d'investigation relatives aux infractions facilitées par les TIC.

L'interdiction des chevaux de Troie (des logiciels espions) est également considérée comme un frein pour les enquêtes fondées sur les TIC ; en effet, les services répressifs n'étant pas autorisés à pénétrer dans les domiciles et d'autres locaux, ils ne peuvent pas installer de logiciels espions sur les appareils utilisés par les personnes visées par une enquête. Les autorités soutiennent que ces outils permettraient aux services répressifs d'atténuer les difficultés liées au décryptage et à l'écoute des conversations VoIP. Les autorités belges ont préconisé une modification du cadre juridique pour faciliter le travail d'enquête en utilisant de nouvelles technologies. Elles ont insisté sur la nécessité de simplifier les procédures et les instruments juridiques en tenant compte du mode opératoire des trafiquants.

Les autorités bulgares ont soulevé un problème relatif aux preuves électroniques, qui nécessiterait d'instaurer sur le plan international l'obligation pour les FSI de mettre en œuvre des protocoles de sécurité visant à prévenir toute **falsification des données** pendant leur stockage et leur transmission aux services répressifs.

Les autorités néerlandaises ont évoqué le risque de **non-respect de la vie privée**, lors du recours à des robots d'exploration, par exemple.

Les autorités espagnoles ont réclamé davantage de personnel spécialisé dans la lutte contre la traite et doté de compétences avancées en informatique. Les autorités belges ont fait une observation similaire.

Les autorités moldaves ont fait part de leurs difficultés de garder les experts qualifiés (car les policiers expérimentés quittent souvent les unités spécialisées pour rejoindre d'autres sections de l'autorité judiciaire ou du secteur privé) et mis en avant l'importance d'évaluer régulièrement les motivations pour attirer les talents et les retenir.

Les autorités autrichiennes ont mis l'accent sur un problème lié aux peines prévues par le Code pénal national pour l'infraction de traite, qui vont de six mois à dix ans

d'emprisonnement. Cette peine est suffisante pour qu'un tribunal puisse ordonner une surveillance des messages, mais elle ne permet pas aux forces de police de recourir à une surveillance visuelle et acoustique (comme la surveillance audio de conversations privées et de locaux privés).

Les autorités britanniques ont relevé un problème à propos des adresses IP et des preuves électroniques. Les adresses IP peuvent constituer le point de départ d'une enquête et, une fois qu'elles sont connues, les services répressifs doivent les associer à plusieurs pseudonymes et utilisateurs. Toutefois, les pseudonymes peuvent être modifiés à tout moment et sont souvent utilisés par les suspects de manière interchangeable. Les services répressifs doivent alors impérativement vérifier le maintien du lien entre les adresses IP et les pseudonymes. En outre, dans les salles de chat virtuelles, certains utilisateurs peuvent être vus à l'écran et leur identité prouvée, mais d'autres n'activent pas leur webcam. Certains suspects peuvent partager leurs appareils avec d'autres personnes, par exemple s'ils vivent en colocation, ce qui de fait rend leur identification plus complexe.

Les autorités britanniques ont également posé la question du traitement des appareils électroniques inutilisés, en particulier dans le cadre des obligations liées au Règlement général sur la protection des données (RGPD). Parallèlement, les autorités néerlandaises considèrent que la réglementation internationale sur la protection des données « entrave la collecte, le stockage et le traitement d'informations obtenues à l'aide de pratiques d'investigation technologique (telle que l'exploration du web) », ce qui « compromet l'utilisation optimale de [ces] techniques » d'investigation.

ZOOM | Difficultés dans la détection des cas de traite facilitée par les TIC

Les enquêtes et les poursuites dépendent avant tout de la détection des cas. Les difficultés recensées par les pays pour la *détection* des cas de traite facilitée par les TIC sont les suivantes :

- Internet représente un immense espace à surveiller et le volume d'activités/échanges en ligne augmente constamment. Les ressources couvrent un vaste spectre diversifié allant de sites d'annonces en ligne et de sites web pour adultes aux plateformes de réseaux sociaux, aux salles de chat et potentiellement au dark web. La surveillance de cet espace 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'exploration dans certains pays).

- La recherche manuelle des sites en ligne constitue un véritable défi, tout comme les masses importantes de données non structurées rendent l'exploration du web très difficile (si tant est que celle-ci soit autorisée par les législations nationales). 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 d'identifier à la fois les trafiquants et les victimes, car ils peuvent utiliser des surnoms et des pseudonymes lorsqu'ils évoluent en ligne. L'utilisation de logiciels d'anonymisation (comme les réseaux privés virtuels ou VPN) et de communications cryptées entre les trafiquants et les victimes contribue aussi à entraver l'identification. Les conversations entre les trafiquants et les victimes se déroulent en cercles fermés (Facebook, WhatsApp ou Telegram, par exemple).

- Comportement fluctuant des internautes (de nouvelles technologies émergent, de nouveaux sites web/applications deviennent très vite populaires). En outre, sous l'effet de la concurrence effrénée du secteur technologique, de nouveaux outils apparaissent rapidement et peuvent fournir aux trafiquants de nouveaux moyens de contacter les victimes et de les exploiter.

- Difficultés à classer les annonces en ligne de façon à distinguer celles qui sont liées à la traite, à des fins d'exploitation sexuelle ou non sexuelle. Les annonces diffusées pour proposer des services sexuels fournis par des victimes de la traite utilisent souvent les mêmes sites, la même terminologie et les mêmes libellés que les annonces publiées par des travailleurs du sexe indépendants. Les « drapeaux rouges » visant à signaler les annonces liées à l'exploitation par le travail restent rares ou ne sont pas systématiquement utilisés.

- Absence d'unités qualifiées au sein de la police et/ou manque d'enquêteurs spécialisés dans la lutte contre la traite et dotés de compétences informatiques avancées. Manque de policiers formés pour mener des opérations d'infiltration sur le web (en créant et en entretenant un faux profil, par exemple).

- Formation insuffisante des policiers sur les particularités de la traite facilitée par les TIC (mode opératoire des trafiquants, plateformes sur lesquelles ils sévissent, comment aborder clandestinement les trafiquants et créer des profils en ligne crédibles).

- Possibilité pour les trafiquants de supprimer/modifier les conversations (preuves électroniques).

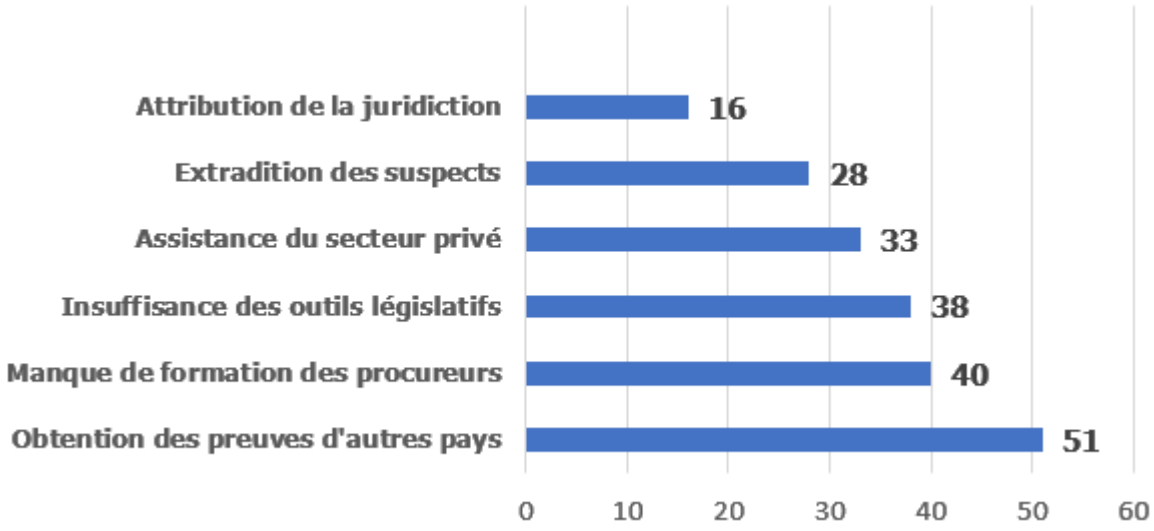
- Lenteur des procédures d'envoi de demandes aux sociétés de réseaux sociaux (souvent basées à l'étranger) et absence de réponses de certaines d'entre elles.

- Durée de rétention des données courte pour les adresses IP et difficultés d'y accéder.

2.2. Difficultés dans les poursuites

Les États parties se sont vu proposer une liste de six difficultés pouvant entraver les poursuites, établie après examen de la base de connaissances existante ainsi que des travaux précédents effectués par le Conseil de l'Europe, notamment la table ronde de 2019 intitulée « Intensifier l'action du Conseil de l'Europe contre la traite des êtres humains à l'ère du numérique »[13]. La figure 4 présente le **score de gravité** de chacune des six difficultés[14].

Figure 4. Scores de gravité des difficultés dans les poursuites



Remarque : échelle des scores = [0, 100]

D'une manière générale, les difficultés rencontrées dans les poursuites ont des scores inférieurs à ceux relevés à propos des enquêtes, puisque seule la difficulté d'« obtention de preuves d'autres pays » enregistre un score de gravité légèrement supérieur à 50 (ce score indique qu'une difficulté est largement perçue comme plus grave qu'un « problème mineur »). Cela vient probablement du fait que lorsqu'une affaire en est au stade des poursuites, la plupart des obstacles ont déjà été écartés avec succès au stade de l'enquête.

Ci-dessous sont présentés des éléments qualitatifs supplémentaires concernant trois difficultés : l'attribution de la compétence, l'extradition des suspects et la formation des procureurs. La section 2.4 décrit les difficultés liées à l'assistance du secteur privé et les difficultés liées aux outils législatifs sont traitées au chapitre 5. Les difficultés relatives à l'obtention de preuves auprès d'autres pays sont évoquées à la section 2.3, qui porte sur les obstacles à la coopération internationale.

Attribution de la compétence : en général, l'attribution de la compétence est considérée comme une difficulté mineure entre les États parties, mais il arrive que des problèmes

[13] https://www.coe.int/fr/web/anti-human-trafficking/-/round-table-on-action-against-trafficking-in-human-beings-in-the-digital-age

[14] Pour chaque difficulté, il a été demandé aux États parties d'évaluer le score de gravité en utilisant un barème de trois points (réponses « Normalement pas un problème », « Problème mineur » et « Problème majeur » respectivement transformées en 0, 1 et 2). Les scores ont ensuite été rééchelonnés de 0 à 100.

ponctuels surgissent dans les affaires facilitées par les TIC en cas de compétences concurrentes. Dans certains cas, des difficultés surviennent dans l'identification des suspects et, point essentiel, dans leur localisation, qui consiste à relier une adresse IP à une personne, puis cette personne à un lieu soumis à une compétence spécifique.

Extradition des suspects : dans l'ensemble, cet élément apparaît comme une difficulté relativement mineure. Le mandat d'arrêt européen (MAE) et la décision d'enquête européenne sont considérés comme deux outils importants qui ont « permis de relever efficacement (et rapidement) les défis posés par le caractère transnational de l'infraction » (autorités portugaises). Les travaux d'Eurojust ont été mentionnés comme un exemple de bonne pratique. Les autorités suisses ont mis l'accent sur les obstacles issus du fait qu'elles ne peuvent pas émettre de MAE et de décision d'enquête européenne. De la même façon, les autorités britanniques ont indiqué que « la sortie du Royaume-Uni de l'Union européenne peut avoir une incidence sur les extraditions », car la « non-extradition des ressortissants nationaux de certains pays [ou *nationality bar*] signifie que [le Royaume-Uni] ne peut plus extrader certains ressortissants de l'Union européenne et requiert des discussions sur la question de savoir quel pays mène les poursuites ». Les différences législatives liées à la traite entre les pays peuvent compromettre l'extradition des suspects.

Formation des procureurs : quelques pays ont souligné l'importance d'une formation efficace des procureurs sur la traite facilitée par les TIC, indiquant que ce type de formation faisait défaut ou n'était pas adéquate. La formation des procureurs est considérée comme essentielle pour que les dossiers de traite facilitée par les TIC soient étayés, les preuves électroniques recueillies et employées correctement, et les dossiers (et les preuves y afférentes) présentés aux juges et aux jurés en bonne et due forme. Certains pays, comme la Norvège, prévoient d'intensifier ces formations en demandant à un procureur expérimenté dans les affaires de traite de donner des conférences à ses collègues. En outre, tous les parquets du pays ne disposent pas nécessairement de ce type de compétences. Les autorités néerlandaises (entre autres) ont mis ce problème en avant et, pour y répondre, le ministère public et la police nationale évaluent actuellement le niveau d'expertise des services. Cette procédure de suivi intra-étatique peut être considérée comme un exemple de bonne pratique pour garantir la cohérence et le niveau d'expertise dans une juridiction. En outre, 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 ; dans d'autres affaires, les procureurs ne connaissaient pas les procédures à suivre pour obtenir des preuves d'autres pays et faciliter la coopération (par exemple, par la création d'une équipe commune d'enquête [ECE] et l'émission d'une décision d'enquête européenne). Une meilleure formation des procureurs devrait faciliter la collaboration avec d'autres pays et des entreprises privées. Finalement, les États parties estiment qu'une formation interdisciplinaire comprenant des éléments d'enseignement sur la traite et sur les TIC devrait être dispensée également aux juges.

Par ailleurs, il a été demandé aux États parties de faire état de **tout autre obstacle** rencontré en matière de poursuites dans les affaires de traite facilitée par les TIC. Ces difficultés sont énumérées ci-après :

- Les autorités britanniques ont signalé la difficulté de prouver la participation et l'intention coupable (*mens rea*) des trafiquants individuels dans les affaires facilitées par les TIC qui

portent sur une activité de groupe ; par exemple, dans une salle de chat, un écran peut afficher un abus commis sur une victime de la traite, alors que d'autres écrans peuvent montrer d'autres utilisateurs qui se livrent à une activité entre adultes consentants. Il peut être très difficile de prouver la participation de plusieurs personnes en raison des différents rôles en jeu.

- Un autre problème mis en avant par les autorités britanniques concerne la **présentation des preuves** devant des jurés (et des juges). Dans les affaires facilitées par les TIC, la présentation des preuves techniques est souvent réalisée par un expert technologique (qui explique, par exemple, comment fonctionne la diffusion en direct de vidéos issues de salles de chat, ses fonctions et les enregistrements qui ont pu être saisis, y compris la description de ce qu'un enregistrement affiche). Il peut donc s'avérer particulièrement utile de développer l'expertise interne des agents sur la manière de présenter des preuves électroniques de façon précise et efficace. Une difficulté associée porte sur la présentation de gros volumes de matériel électronique à un jury. Pour y parvenir, le Royaume-Uni envisage d'utiliser des tablettes.

2.3. Difficultés dans la coopération internationale

Dans le cadre de cette étude, les États parties ont été invités à faire état des difficultés rencontrées en matière d'enquêtes transnationales et de coopération judiciaire relatives à la traite facilitée par les TIC. La plupart de ces difficultés ne portent pas spécifiquement sur la traite facilitée par les TIC, mais plus généralement sur les enquêtes transfrontalières et la coopération judiciaire, en l'occurrence les barrières linguistiques, les bases juridiques différentes, la coordination d'enquêtes parallèles et l'échange rapide d'informations. Toutefois, les spécificités de la traite facilitée par les TIC aggravent souvent ces difficultés, surtout s'agissant des preuves électroniques. De plus, dans le contexte de la traite facilitée par les TIC, il est souvent essentiel de recevoir l'entraide judiciaire et d'obtenir des preuves dans les plus brefs délais.

2.3.1. Demandes d'entraide judiciaire

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 internationaux. Comme l'ont indiqué les autorités espagnoles, « trop de sources d'information ne sont accessibles que sur autorisation judiciaire ». Ces demandes doivent être traitées par la voie de demandes d'entraide judiciaire qui, elles-mêmes, compliquent et prolongent les enquêtes. Le système actuel a été décrit comme « inadéquat » par plusieurs pays. Les demandes d'entraide judiciaire entre les États parties du Conseil de l'Europe peuvent suivre deux scénarios différents : a) dans le cadre de l'Union européenne relatif à la coopération judiciaire (avec l'aide d'Europol et d'Eurojust) et b) en dehors du cadre de l'Union européenne. Étant donné que les difficultés et les procédures peuvent être radicalement différentes selon le scénario, il convient de les traiter séparément.

Coopération dans le cadre juridique de l'Union européenne. Pour les États parties du Conseil de l'Europe également membres de l'Union européenne, le cadre coordonné européen de la coopération policière et judiciaire est avantageux et permet d'optimiser le processus. Il englobe le travail d'organismes de l'Union européenne, tels qu'Eurojust et Europol. Toutefois, des difficultés persistent. D'après les autorités françaises, « bien qu'intéressants, les outils de coopération internationale sont lents : une décision d'enquête européenne prend plusieurs mois et une équipe commune d'enquête (ECE) est difficile à mettre en place ». L'un des principaux obstacles à la mise en place d'ECE est la nécessité d'organiser une enquête miroir dans l'autre ou les autres pays. Les autorités norvégiennes partagent cette opinion.

Coopération à l'extérieur du cadre juridique de l'Union européenne. Le processus est considéré comme plus chronophage et laborieux que dans le scénario précédent en raison du manque d'harmonisation entre les différents systèmes juridiques (comme l'ont souligné, entre autres, les autorités chypriotes et espagnoles). Les autorités suisses ont indiqué que la réponse aux « demandes d'entraide judiciaire internationale dépend souvent de la bonne volonté ou de l'intérêt des procureurs étrangers ». Cela introduit un élément d'imprévisibilité et d'incohérence dans le processus. Ces « négociations entre parquets sont souvent interminables ». **Des procédures opérationnelles plus claires, des échanges réguliers 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. Les autorités de la Macédoine du Nord ont fait remarquer que toutes les demandes d'entraide judiciaire devaient passer par une unité centralisée au sein du ministère de la Justice, ce qui crée un goulet d'étranglement et ralentit souvent les procédures. Elles ont suggéré d'établir d'autres mécanismes qui permettraient à des institutions clés spécifiques d'entrer directement en contact avec leurs homologues internationaux (le ministère public, l'Inspection du travail ou le ministère de l'Intérieur, par exemple).

Les autorités norvégiennes ont souligné la nécessité d'améliorer l'accord existant et d'élaborer de nouveaux accords avec les pays d'origine des victimes s'ils sont situés en dehors de l'Union européenne. Le problème a également été mentionné par les autorités françaises, qui ont fait ressortir que « de nombreuses organisations criminelles qui utilisent les TIC viennent de pays avec lesquels la coopération internationale est soit insuffisante, soit inexistante. C'est le cas des réseaux chinois et des réseaux issus de la Russie et de l'Ukraine ». Grâce aux TIC, ces réseaux criminels peuvent organiser leurs opérations de telle façon que les principaux membres peuvent contrôler les activités de prostitution depuis leur pays d'origine – sachant souvent que les demandes de coopération judiciaire ne seront pas satisfaites en temps voulu, si tant est qu'elles le soient. La lenteur ou l'absence de coopération se répercute sur l'identification des trafiquants, la collecte de preuves et la fermeture de sites web.

ZOOM | Quels enseignements peut-on tirer du cadre judiciaire de l'Union européenne ?

Il est évident que le cadre judiciaire de l'UE offre un espace juridique plus intégré et propice à la coopération judiciaire comparé aux difficultés rencontrées par les États parties pour toute coopération extérieure (en dépit de ses limites et obstacles). Quels éléments de ce cadre pourraient être étendus au-delà de la coopération entre les pays de l'UE ? La question est difficile et nécessiterait une analyse juridique complète, mais nous pouvons avancer ici des suggestions préliminaires. La présentation des autorités suisses (pays qui n'entre pas dans le cadre judiciaire de l'UE) résume bien les avantages clés du cadre de l'UE, en particulier la décision d'enquête européenne :

- il se fonde sur un ensemble de règles communes avec un vaste champ d'application ;
- il établit des délais précis pour la collecte de preuves ;
- les motifs de refus sont restreints ;
- il allège les charges administratives par l'introduction d'un formulaire type standardisé ;
- il garantit la protection des droits essentiels de la défense.

Il est clair que certaines mesures ne peuvent être étendues que si elles s'inscrivent dans un ensemble complet de règles juridiques communes. Toutefois, il est possible que certains États parties souhaitent examiner quels aspects spécifiques de la décision d'enquête européenne peuvent fonctionner en dehors du cadre de l'Union européenne. Cela pourrait concerner la coopération entre les États parties à la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains et à la Convention européenne des droits de l'homme. Des mesures visant à établir des délais de collecte des preuves et à réduire la charge administrative par l'instauration de procédures normalisées pourraient être envisagées sans changements radicaux des systèmes juridiques internes. Un ensemble de règles communes, dont certaines seraient renforcées, pourrait aussi être envisagé, à condition que les dispositions énoncées dans la Convention européenne des droits de l'homme soient respectées.

Difficultés supplémentaires liées aux demandes d'entraide judiciaire. Des données fournies par des États parties mettent aussi en lumière des difficultés dans le traitement des demandes d'entraide judiciaire qui sont imputables à l'absence de personnel convenablement formé pour compiler et traiter ces demandes, et à l'utilisation de technologies obsolètes. Ainsi, certains pays ont indiqué qu'ils ne sécurisaient pas toujours les courriels et autres formes de correspondance lors des échanges de documents avec des partenaires étrangers. Pour mieux coopérer à l'échelle internationale, les pays devraient développer l'utilisation de formes de communication électronique sécurisées, assorties de règles et de garanties, et promouvoir leur adoption auprès de tous les États parties. En outre, la diffusion d'informations pratiques sur les points de contact/unités dédiées d'un pays qui servent d'« interlocuteur privilégié » dans les affaires de traite, y compris la traite facilitée par les TIC, pourrait simplifier les formalités.

2.3.2. Les preuves électroniques

Les difficultés relatives à l'obtention de preuves électroniques se rapportent souvent aux demandes d'entraide judiciaire, mais la nature et la pertinence desdites preuves posent des difficultés supplémentaires qu'il serait intéressant d'examiner séparément.

Comme l'ont indiqué les autorités autrichiennes et britanniques, dans le cas de preuves électroniques, les données ne peuvent pas toujours être localisées précisément. Faute de connaître le pays et, partant, la juridiction dont elles relèvent, il est difficile de faire une demande d'entraide judiciaire. Les autorités portugaises considèrent que les formalités permettant d'obtenir des preuves électroniques d'autres pays ne sont pas adaptées, et il a été suggéré de les améliorer en s'inspirant du Deuxième Protocole additionnel à la Convention de Budapest sur la cybercriminalité[15]. De la même façon, les autorités grecques préconisent l'adoption d'un cadre juridique commun pour un échange rapide des preuves numériques (sachant qu'il existe un cadre juridique commun pour la préservation des preuves).

Une difficulté a été mentionnée à propos du moment où il est légalement possible de faire une demande de preuves électroniques. D'après les autorités britanniques, « les services répressifs ont parfois besoin d'accéder au contenu des communications pour démontrer une cause probable, mais une condition préalable pour obtenir cette aide doit être satisfaite avant que le contenu ne soit partagé ». Cela se répercute particulièrement sur les premières phases d'une enquête. De leur côté, les autorités autrichiennes soulignent la difficulté associée au « seuil élevé imposé pour obtenir des données relatives au contenu auprès de certaines juridictions ». Les mêmes autorités souhaiteraient en savoir plus sur le type d'information qu'il est possible de demander dans le cadre d'une enquête, et sur le fondement juridique de la demande (avec ou sans décision de justice, etc.). Elles plaident en faveur d'un « accès standardisé aux informations des services de police judiciaire dans le cadre des enquêtes pour traite » (par exemple, pour demander aux opérateurs de téléphonie mobile des données sur leurs abonnés). Elles relèvent que « dans certains pays, [cela n'est] possible que lorsqu'un tribunal compétent a envoyé une décision d'enquête européenne, alors qu'en Autriche, c'est possible sans décision judiciaire au cours des enquêtes des services de police judiciaire ».

Comme indiqué plus haut dans le présent rapport (section 2.1.6), les règles sur la durée de conservation des données sont mises en avant comme particulièrement problématiques. Plusieurs pays ont exprimé leurs préoccupations par rapport à l'absence de réglementation homogène en matière de conservation de données, ce qui entrave l'échange de preuves électroniques. Il est possible que certains pays n'aient aucune législation sur la conservation des données.

Enfin, plusieurs pays ont fait part de leurs inquiétudes pour ce qui est d'accéder aux preuves électroniques stockées dans des serveurs situés en dehors de leur juridiction. Les expériences sur ce point varient d'un pays à l'autre et selon l'entreprise détentrice des données. Toutefois, des difficultés apparaissent clairement s'agissant d'identifier une entreprise, de la localiser, d'obtenir sa coopération et d'organiser le transfert de preuves. Les États parties ont souligné la nécessité de mettre en place un cadre plus complet pour réglementer la préservation et le transfert des preuves électroniques, ainsi qu'un cadre juridique commun pour remplacer les

[15] Deuxième Protocole additionnel à la Convention sur la cybercriminalité adopté par le Comité des Ministres du Conseil de l'Europe - News (coe.int)

accords de travail bilatéraux ad hoc qui existent actuellement entre les États et les entreprises privées détentrices des données.

2.4. Difficultés dans la coopération avec les entreprises privées

L'étude a étudié les difficultés rencontrées par les États parties lorsqu'ils travaillent avec des entreprises des TIC et les FSI, y compris des hébergeurs de contenu et des réseaux sociaux, pour lutter contre la traite. Certaines de ces difficultés ont déjà été évoquées plus haut, mais il serait bon d'examiner plus avant les questions soulevées par les États parties. Elles sont résumées ci-après :

- La réponse en temps utile des FSI et des 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, au risque que le contenu recherché ne soit détruit avant que la demande n'aboutisse. Les autorités françaises ont souligné le long temps de réponse aux demandes de métadonnées sur les comptes liés aux trafiquants ; pour les données relatives au contenu, il est souvent nécessaire d'émettre une demande d'entraide judiciaire qui peut prendre plusieurs mois pour être satisfaite, car les entreprises sont souvent situées à l'extérieur du territoire relevant de la compétence du pays demandeur (et de l'Union européenne).

- La clarification des exigences légales qui régissent le fonctionnement des entreprises des TIC et des FSI. Les autorités autrichiennes s'inquiètent du fait que « des fournisseurs internationaux imposent souvent des formalités indues aux services répressifs comme conditions préalables à la communication d'informations et à la mise à disposition de données relatives aux usagers et aux contenus. Il est parfois très compliqué de se plier aux injonctions de poursuite ». Selon les autorités belges, les refus ne sont souvent pas motivés ou expliqués convenablement. Les autorités de Bosnie-Herzégovine ont signalé des difficultés pour obtenir des données non personnelles au cours des enquêtes (tant qu'aucun tribunal n'a émis d'injonction). L'identification du FSI lui-même peut s'avérer difficile, comme l'indiquent les autorités finlandaises.

- Les autorités françaises ont mis l'accent sur des questions liées à la non-reconnaissance du parquet en tant qu'autorité judiciaire indépendante lors de l'émission d'une demande formelle de réquisition de données ; un autre problème se pose lorsque le service juridique d'une entreprise n'accepte de se prononcer sur la transmission de données qu'après avoir reçu de nombreux éléments afférents à l'enquête en cours.

- Les autorités belges ont relevé le manque de retour d'information sur les opérations réalisées en interne par les entreprises (les opérations associées à la suppression de contenu, par exemple). Elles ont également constaté des difficultés dans la communication avec les entreprises – souvent aggravées par les changements fréquents d'interlocuteur.

- Comme mentionné précédemment, les pays désignent l'absence de législation harmonisée sur la conservation des données et des dispositions juridiques inadéquates comme posant des problèmes cruciaux. En Norvège par exemple, les FSI ne sont pas autorisés à stocker des informations sur les adresses IP plus de 21 jours, et ils ne sont pas tenus de conserver des informations sur le lien entre l'abonné et l'adresse IP. D'après les autorités

norvégiennes, cela rend « difficile pour la police d'identifier des personnes soupçonnées de traite facilitée par les TIC ». Ce problème est encore plus aigu avec les entreprises spécialisées dans les services anonymes et cryptés.

- Les autorités moldaves ont noté l'absence de point de contact désigné au sein d'entreprises privées qui s'occupent de médias sociaux ou d'autres applications de réseautage. Il a été suggéré qu'un point de contact soit mis en place pour chaque pays/zone (selon le nombre d'utilisateurs). (Des points de contact pourraient également être désignés selon la langue pratiquée.) Les autorités moldaves ont proposé que les FSI, les hébergeurs de contenu et les médias sociaux soient soumis à l'obligation d'établir des points de contact. La question des compétences linguistiques au sein des entreprises a été mise en avant par les autorités slovaques, qui ont indiqué que les multinationales manquaient souvent d'employés possédant les compétences linguistiques et juridiques pertinentes pour chaque pays dans lequel elles exercent.

- Les FSI ne connaissent pas toujours clairement les agences nationales responsables de telle ou telle décision (le retrait de contenus illégaux, par exemple). Les autorités slovaques ont proposé de faire appel à 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 et d'agir sur d'autres dispositions juridiques. Le signaleur de confiance aurait une voie de communication ouverte avec les entreprises et instaurerait une confiance mutuelle.

Plusieurs pays, dont Chypre, l'Irlande, la Lettonie, le Luxembourg, Malte, les Pays-Bas et le Royaume-Uni, ont indiqué que les FSI, les hébergeurs de contenu et les entreprises de réseaux sociaux étaient généralement coopératifs pour les questions liées à la traite et à l'exploitation sexuelle des enfants. Toutefois, les autorités britanniques ont souligné la nécessité d'aller plus loin et de travailler avec des entreprises en ligne pour « **restreindre les possibilités** de traite sur leurs sites web et travailler en coopération avec les services répressifs à des fins de prévention des activités de traite ».

Les autorités chypriotes ont mentionné comme bonne pratique l'utilisation de Sirius, une plateforme gérée par Europol pour faciliter l'accès transfrontalier aux preuves électroniques. Cette plateforme donne aux services répressifs la capacité de communiquer directement avec des entreprises privées pour la conservation et la divulgation des données. Ce point a aussi été souligné par les autorités françaises (projet E-evidence).

2.5. Informations communiquées par des ONG

En complément des informations communiquées par les États parties dans le cadre de cette étude, les ONG qui portent assistance aux victimes ont été invitées à faire part des problèmes relevés dans le contexte de la traite facilitée par la technologie.

2.5.1. Problèmes en matière d'identification et d'enquête

D'une manière générale, les informations fournies par les ONG correspondent aux problèmes signalés par les États parties et évoqués précédemment dans le présent chapitre. Plus

précisément, les ONG ont mis l'accent sur l'ensemble de facteurs suivants qui entravent la détection des cas de traite facilitée par la technologie et les enquêtes qui en découlent :

- Les capacités insuffisantes des forces répressives en matière de formation, d'équipement et de logiciels, et l'utilisation limitée des techniques spéciales d'enquête. Certaines ONG ont relevé l'absence de spécialisation des services répressifs et judiciaires dans la traite liée à la technologie et l'insuffisance des capacités dans le domaine des mégadonnées. Les outils de collecte automatique de données en ligne expérimentés par Hope Now (Danemark) en 2016-2018 ont toutefois atteint de modestes résultats.

- L'évolution rapide du paysage technologique et des modes opératoires des trafiquants. Il peut être difficile pour les professionnels de se tenir informés de l'évolution de la traite facilitée par la technologie, ce qui entrave leur capacité de détecter rapidement les cas de traite et d'ouvrir des enquêtes. Les connaissances sur le paysage technologique et les modes opératoires sont souvent cloisonnées (services répressifs, entreprises privées, ONG, milieux universitaires, etc.).

- Les forums privés, les salles de chat ou les applications de discussions cryptées entre les auteurs 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 de fournir des renseignements/avertissements sur une utilisation sûre des moyens de communication privés.

- Les difficultés à démasquer les trafiquants anonymes lors de la diffusion en direct d'actes d'exploitation en ligne, et les difficultés à collecter les preuves de ces sévices, sauf si les enregistrements vidéo ont fait l'objet de captures d'écran.

- À partir des seules informations à la disposition du public (dans les annonces de services sexuels en ligne, par exemple), les professionnels ont des difficultés à déterminer si une personne qui se cache derrière un profil/une annonce en ligne fournit volontairement les services mentionnés. En effet, les délinquants peuvent créer et gérer des profils en ligne pour le compte des victimes. En outre, lorsqu'un profil est bloqué, ils peuvent facilement créer de nouveaux profils.

- Les règles de protection des données et de la vie privée peuvent empêcher l'identification des victimes et des trafiquants. Le RGPD restreint l'utilisation des technologies pour détecter les traces numériques laissées par les victimes et les auteurs d'infractions (traces laissées sur les réseaux sociaux et sur internet mais aussi liées aux comptes financiers). Les enquêtes pâtissent d'un manque d'analyse complète des traces numériques centrées sur la victime concernant notamment les biens immobiliers, les comptes bancaires, les transactions par guichet automatique, les transactions par cartes de crédit et les dossiers médicaux.

- 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. La Sustainable Rescue Foundation a cité les facteurs suivants qui entravent les collaborations intersectorielles autour des données :
    - les plateformes indépendantes n'attirent pas l'attention des services répressifs et des instances gouvernementales ;
    - l'absence de stratégie technologique dans les plans d'action nationaux sur la traite ;

- les unités informatiques des services répressifs n'ont ni la capacité ni le budget pour concevoir, tester, lancer, améliorer, mettre à jour et entretenir des applications relatives à la détection des cas de traite en temps opportun ;
- des difficultés dans le partage des données des victimes ;
- les intérêts commerciaux.

- Les limitations des enquêtes sur la traite par les institutions financières. Les données recueillies dans le cadre des obligations de connaissance client ne sont pas exploitées pour faciliter l'identification, en raison du manque de formation et de sensibilisation au phénomène de la traite, et des complexités du système de signalement (qualité des alertes, nombre très important de faux positifs, long temps de réponse, etc.).
- Le manque d'investissement dans l'intelligence artificielle (IA) et dans l'apprentissage automatique pour les opérations, la prédiction et la prévention. La Sustainable Rescue Foundation a cité en exemple l'apprentissage automatique dans le secteur médical qui permet « le partage d'informations entre les cliniques, les hôpitaux, les médecins et les universitaires sans enfreindre la législation sur la protection de la vie privée. Pour cela, le système utilise des données conformes aux principes FAIR (Faciles à trouver, accessibles, interopérables et réutilisables) pour les concordances de métadonnées, et l'apprentissage collaboratif pour l'analyse profonde fondée sur des sources multiples ». La Sustainable Rescue Foundation a également relevé qu'« aucun investissement et aucune stratégie en ce sens n'étaient en cours dans les organisations de lutte contre la traite ».
- L'absence de partage de données entre les différentes entités aux niveaux local, régional, national ou international, due à l'insuffisance des capacités opérationnelles au sein des services répressifs et aux limitations imposées par les législations nationales. En outre, les données sont souvent recueillies sous une forme non structurée, ce qui complexifie le partage des preuves et leur analyse plus approfondie.
- Les ONG qui apportent une aide directe aux victimes de la traite par la voie de plateformes en ligne, de téléconsultations et de permanences téléphoniques n'ont pas la capacité, les ressources ou les outils techniques pour détecter régulièrement l'exploitation en ligne facilitée par la technologie.
- La méconnaissance des risques et des éventuelles conséquences liées à l'utilisation des technologies par les personnes vulnérables à la traite. Le problème concerne particulièrement les enfants et les jeunes adultes. Plus généralement, la traite facilitée par la technologie est mal connue du grand public, ce qui entraîne un faible taux de signalement.

2.5.2. Difficultés dans la coopération avec les services répressifs

Toutes les ONG déclarent qu'elles coopèrent avec les services répressifs, en signalant les cas de traite ou en portant assistance aux victimes lorsque les autorités le demandent. S'agissant de leur coopération avec les services répressifs, les ONG ont mis en relief les difficultés suivantes :

- des objectifs contradictoires ou des approches différentes entre les ONG et les services répressifs, y compris pour les décisions relatives à la nécessité d'ouvrir une enquête ;
- des questions liées à la protection des données et au respect de la vie privée ;
- l'absence de retour d'information sur les affaires que les ONG signalent aux autorités ;
- le manque de ressources qui favoriseraient la coopération entre les services répressifs et les ONG (cette insuffisance a également été relevée pour les conseils des « laboratoires de terrain » innovants établis aux Pays-Bas, auxquels siège la Sustainable Rescue Foundation) ;
- s'agissant des enfants, les services répressifs ne sont pas suffisamment formés pour aborder les victimes mineures et les convaincre de coopérer à une enquête. La Strada Moldova a souligné que les enquêtes impliquant des enfants présentaient une difficulté supplémentaire dans le traitement des preuves, car « les enfants se sentent généralement responsables, coupables ou honteux de ce qui leur est arrivé, ne sont pas coopératifs, ne veulent pas que les parents découvrent ce qu'ils ont subi ou que d'autres personnes voient leurs vidéos sexuellement explicites. Un grand nombre d'entre eux refusent de déposer plainte », empêchant ainsi les services répressifs de progresser dans leurs enquêtes.

2.6. Entreprises de technologie

Facebook a fait observer que les contenus relatifs à la traite étaient « rarement signalés » par les utilisateurs. La société a également indiqué que ce faible taux de signalement pourrait être dû à plusieurs facteurs : a) les victimes de la traite n'ont peut-être pas la liberté d'informer ou n'ont peut-être pas conscience de leur situation d'exploitation ; b) les acheteurs de services fournis par une personne soumise à la traite n'ont peut-être pas conscience de cette situation ou ne souhaitent faire aucun signalement, « car ils veulent bénéficier des services illicites ou très peu coûteux résultant de l'exploitation ». Dans d'autres cas, il est noté que « pour certaines formes de traite comme la servitude domestique, qui est entrée dans les mœurs dans certaines régions, les personnes qui voient ces contenus ne réalisent pas qu'elles peuvent ou devraient les signaler ».

S'agissant des difficultés de coopération avec les services répressifs, IBM a mis l'accent sur « plusieurs obstacles » ; avant toute chose, ses représentants ont souligné des « problèmes relatifs à la légalité de cette coopération, en particulier eu égard à la confidentialité des données, et à la complexité juridique de juridictions multiples ». Ils demandent des « éclaircissements sur les autorisations juridiques internationales en vigueur pour rassembler et partager des données (avec les services répressifs compétents) ». Facebook a indiqué que le caractère transfrontalier de l'exploitation d'êtres humains « posait des difficultés ». La société a notamment souligné que les trafiquants pouvaient se trouver dans un pays autre que celui où les actes de traite et les abus étaient commis : « de multiples juridictions peuvent ainsi participer aux enquêtes menées sur le réseau criminel. La nécessité de coordonner les services répressifs au sein de l'Union européenne et au-delà ajoute de la complexité aux efforts de lutte contre la traite ».

2.7. Autres informations issues de l'analyse contextuelle

Dans le cadre de cette étude, outre les informations fournies par les États parties, les ONG et les entreprises de technologie, des recherches documentaires ont été menées à partir de données factuelles disponibles sur les problèmes rencontrés dans la détection des infractions de traite commises en ligne et facilitées par la technologie, dans les enquêtes sur ces infractions et dans la poursuite de leurs auteurs.

Les informations portant sur les problèmes rencontrés dans l'**identification des offres d'emploi relatifs à la traite** sont particulièrement intéressantes. Il a été suggéré que la technologie produirait de meilleurs résultats si l'accent était mis sur l'identification des offres d'emploi plutôt que sur l'identification des victimes : l'idée remonte à des travaux très novateurs réalisés par le Conseil de l'Europe (2007) et dans le cadre du projet Fine Tune (2011). Ce projet a permis de dresser une liste préliminaire de **drapeaux rouges relatifs à l'exploitation par le travail**. Ceux-ci comprennent : a) un salaire excessivement élevé pour un emploi non qualifié ; b) une description de l'emploi très vague, sans précision concernant les fonctions, la localisation, le lieu de travail et les horaires journaliers ; c) l'absence d'adresse de la société ou de l'organisme employeur ; et d) l'absence de coordonnées autres qu'un numéro de téléphone ou une adresse électronique générique. Toutefois, selon les indications disponibles, il reste très difficile d'identifier les « vrais positifs » (c'est-à-dire les annonces liées à la traite). Plusieurs auteurs ont mentionné les **difficultés de distinguer** les vraies annonces de celles liées à la traite, malgré les efforts déployés pour élaborer des **indicateurs de risque potentiel** (et pour réinterpréter les indicateurs généraux de l'Office des Nations Unies contre la drogue et le crime [ONUDC] et de l'Organisation internationale du travail [OIT] pour les adapter au contexte en ligne : Di Nicola *et al.* 2017 ; Raets et Janssens 2018 ; Volodko *et al.* 2019) :

a. Sur un ensemble de 430 offres d'emploi en ligne en Lituanie analysé par Volodko *et al.* (2019), 98,4 % contenaient au moins un indicateur de la traite, ce qui laisse supposer que ces indicateurs sont souvent des caractéristiques courantes sur les marchés d'emplois peu qualifiés. Les résultats ont toutefois montré que seules 15 % des annonces présentaient plus de cinq indicateurs, ce qui permet d'espérer qu'avec des perfectionnements et des techniques d'analyse appropriées, des stratégies de réduction des dommages pourraient être mises en œuvre efficacement.

b. Outre le perfectionnement de l'ensemble de drapeaux rouges (et sa mise à jour constante, qui pose des difficultés supplémentaires), les méthodes informatiques fondées sur la collecte automatique de données en ligne, le traitement du langage naturel, la reconnaissance d'entités et les « tags » ainsi que, plus généralement, les techniques d'apprentissage automatique ont été proposés comme des moyens possibles de progresser (Volodko *et al.* 2019, entre autres ; et la plateforme Delta 8.7 de l'ONU). Ces solutions potentiellement prometteuses s'accompagnent aussi de nouveaux défis, en l'occurrence : 1) établir une « vérité de terrain » pour les modèles, ce qui exige une étroite collaboration entre les services répressifs et le secteur privé ; 2) exploiter les connaissances du secteur privé, puisque les services répressifs ont rarement les compétences requises en interne ; 3) examiner soigneusement les questions éthiques liées aux techniques d'apprentissage automatique à grande échelle ; et 4) évaluer les risques de pratiques discriminatoires et les problèmes de protection des données et de partage de l'information entre différentes entités.

Il peut arriver que les offres d'emploi dans le mannequinat et les loisirs - et, dans certains pays, dans les services sexuels à l'étranger - soient utilisées pour recruter des personnes qui sont ensuite soumises à l'exploitation sexuelle. Plusieurs drapeaux rouges ont été proposés pour séparer les annonces liées à la traite de celles qui sont légitimes ; ainsi, il convient de se méfier des annonces qui : a) sont mal rédigées et peu claires ; b) font des promesses exagérées ; c) sont trop générales ; d) ne précisent pas le pays de destination (mais renvoient à une destination « exotique ») ; et e) ne contiennent pas le nom complet d'une personne de contact, d'une agence de recrutement et/ou de l'entreprise qui emploierait les candidats retenus (Di Nicola *et al.* 2017). Malgré cela, les premières tentatives faites pour cribler les données disponibles sur la base de ces critères ont une nouvelle fois mis en évidence la difficulté de séparer les offres d'emploi liées à la traite des faux positifs.

Il reste très difficile de détecter les cas d'exploitation sexuelle parmi les **offres de services sexuels en ligne**, c'est-à-dire de distinguer les services sexuels fournis par des personnes soumises à la traite des services fournis librement, en se fondant uniquement sur les éléments textuels et visuels de l'annonce. Certains indicateurs d'exploitation ont été proposés, notamment des discordances entre les descriptifs, les images et les emplacements des profils ; la vérification croisée des sites web peut également faire ressortir ces discordances (Di Nicola *et al.* 2017). Les recherches ont montré que les numéros de téléphone jouaient un rôle essentiel, en particulier la présence du même numéro de téléphone dans des annonces, des sites web et des publications attribués à des personnes différentes (un drapeau rouge potentiel). Il a été suggéré d'employer la technique de reconnaissance faciale pour repérer les incohérences et les drapeaux rouges, ce qui s'apparente à l'approche adoptée dans la détection de matériels à caractère sexuel représentant des mineurs (Raets et Janssens 2018).

Toutefois, les premières tentatives pour transposer à plus grande échelle la stratégie de détection décrite ci-dessus se sont heurtées à des difficultés manifestes. Pour identifier des victimes de la traite aux fins d'exploitation sexuelle aux États-Unis, à l'aide d'annonces d'escortes en ligne, Ibanez et Ganzan (2014, 2016a et 2016b) ont utilisé des numéros de téléphone et des indicateurs de mouvement, mais les résultats n'ont pas été probants. En outre, certains indicateurs répertoriés dans Ibanez et Gazan 2014 sont assez surprenants ; ils pourraient ne pas témoigner de situations de traite et même, dans certains cas, représenter une situation inverse.

3. Stratégies et bonnes pratiques

Une fois présentées les difficultés rencontrées, l'étude examine les stratégies élaborées par les États parties pour détecter les cas de traite en ligne et facilitée par la technologie, et mener des enquêtes, favoriser la coopération internationale ainsi qu'identifier les victimes et leur venir en aide. S'ensuit l'analyse des informations fournies par les ONG et les entreprises de technologie sur les mêmes questions.

3.1. Détection des cas de traite facilitée par les TIC

3.1.1. Stratégies générales

Les pays ont indiqué qu'ils appliquaient diverses stratégies pour détecter les cas de traite en ligne et facilitée par les TIC. L'une de ces stratégies largement évoquée est la **surveillance d'internet**, y compris des forums, et, dans certaines affaires, des réseaux TOR (dark web). Elle est souvent associée à l'utilisation de **renseignements issus de sources ouvertes** (Open Source Intelligence ou OSINT), une stratégie d'enquête courante qui consiste à extraire les données de réseaux sociaux et d'autres sources en ligne accessibles au public concernant le réseau de contacts d'une personne, ses conditions de vie et sa situation financière. La méthode OSINT peut être utilisée de manière « proactive », par exemple pour détecter les cas de traite potentiels, identifier les trafiquants et les victimes potentiels ou obtenir de nouvelles informations. Certains pays ont créé des « **cyberpatrouilles » avec des agents spécialisés** qui mènent des enquêtes OSINT sur internet. Certaines juridictions autorisent des enquêtes furtives en ligne (cyber-infiltration). Aux Pays-Bas, dans les enquêtes sur les affaires de traite, il peut être fait appel à des « **spécialistes du numérique** » pour recueillir des preuves de traite en ligne. Les autorités finlandaises ont mentionné la création récente d'une entité spécialisée dans la lutte contre la traite en ligne au sein de l'équipe d'enquête nationale. (Elles ont également signalé l'existence d'un bureau du renseignement en ligne qui explore le web, y compris le dark web.)

En lien avec les enquêtes OSINT, certains pays ont indiqué qu'ils employaient des **techniques d'analyse des réseaux sociaux** pour saisir et reconstituer le réseau de contacts d'un trafiquant et/ou d'une victime. À titre d'exemple, si la victime A est liée au recruteur B, il est possible d'examiner tous les contacts du recruteur B pour identifier des victimes potentielles. Les **informations relationnelles** sont essentielles et les forces de police en tirent de plus en plus parti par le biais de l'« analyse de liens » ou de techniques plus sophistiquées d'« analyse des réseaux sociaux ».

D'autres **stratégies proactives** intègrent l'utilisation d'outils technologiques pour rechercher des preuves en ligne (par exemple, les robots d'exploration, également mentionnés ci-après) et des enquêtes stratégiques sur les modes opératoires TIC des trafiquants. Le développement et l'actualisation de ces connaissances stratégiques sur le phénomène (et au-delà) peuvent éclairer à la fois une approche globale et des enquêtes précises, plus ciblées. Malgré cela, les États parties n'ont pas tous indiqué qu'ils employaient des stratégies « proactives ». Certains

d'entre eux ont expressément déclaré que leurs enquêtes sur la traite facilitée par les TIC restaient « réactives ».

Certaines autorités ont fait savoir qu'elles étaient en liaison directe avec des fournisseurs de services en ligne pour identifier les cas de traite facilitée par les TIC. Dans les pays où les publicités pour les services sexuels en ligne sont légales, l'administration peut « effectuer un filtrage/ciblage des numéros de téléphone et [analyser] les données des utilisateurs associées à des trafiquants [présumés] » (document soumis par la Hongrie). En Suisse, une force de police cantonale effectue des « contrôles ciblés » sur les annonces en ligne proposant des services sexuels, en vue de détecter les victimes potentielles de la traite. Au Royaume-Uni, certains services répressifs emploient des **outils de collecte automatique de données en ligne** spécialement conçus pour extraire les informations de sites web, afin d'identifier les risques et vulnérabilités sur les sites web pour adultes. Les forces de police britanniques mènent des opérations de dragage (*trawling*) des sites web pour adultes en vue d'obtenir des données qui permettront d'analyser leurs activités et pourront donner matière à des poursuites.

Plusieurs pays ont mentionné l'existence d'un **mécanisme 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 (voir quelques exemples ci-dessous).

3.1.2. Stratégies par pays

Les pays ont élaboré des stratégies diverses visant à prévenir et réprimer l'utilisation malveillante du web, notamment par le biais d'offres d'emploi en ligne, dans le contexte de la traite facilitée par les TIC. Pour en savoir davantage, la présente section donne un bref aperçu des initiatives et mécanismes nationaux. Ces stratégies devraient être considérées en combinaison avec les bonnes pratiques décrites dans la section suivante, et avec les cadres juridiques nationaux relatifs à l'identification et à la suppression des contenus liés à la traite en ligne, qui sont présentés dans l'annexe web.

En Albanie, il existe un **mécanisme de permis** associé aux offres d'emploi en ligne et ces permis sont délivrés/contrôlés par les institutions (non précisées dans le document soumis par les autorités).

Depuis le début de la pandémie de covid-19, les autorités autrichiennes ont intensifié les recherches préventives sur différentes plateformes en ligne pour identifier les victimes de la traite et les trafiquants en recourant à des **technologies logicielles spéciales** (des robots d'exploration, par exemple), à des **spécialistes de l'OSINT** ainsi qu'à des **agents infiltrés** (enquêtes sous pseudonyme en ligne). Les activités sont menées conjointement par des enquêteurs spécialisés dans la traite et par des agents informaticiens. Cette approche pourrait éventuellement servir de cadre pour les enquêtes futures.

Les autorités belges ont indiqué qu'en vertu du « modèle abolitionniste » actuel adopté pour la prostitution, il est juridiquement impossible de conclure des accords avec les sites web qui publient des annonces proposant des services sexuels. Cela est considéré comme une « limitation » de la législation en vigueur. L'ONG Child focus prépare actuellement une

campagne destinée à sensibiliser les clients des sites web qui hébergent des offres de services sexuels au risque de rencontrer une personne mineure. Cette campagne est menée en partenariat avec les sites web concernés.

Les autorités croates ont indiqué qu'elles effectuaient des **contrôles sur les profils des réseaux sociaux** des personnes liées à des enquêtes judiciaires spécifiques, par exemple concernant des abus sexuels et l'exploitation sexuelle d'enfants, pour identifier des victimes et recruteurs potentiels. Ces contrôles sont assurés par des experts en cybercriminalité.

À Chypre, le département de lutte contre la cybercriminalité organise des campagnes de mobilisation des élèves et de leurs parents dans le cadre de la Stratégie nationale en faveur d'un meilleur internet pour les enfants. Depuis 2014, ce département gère également une plateforme de signalement de la cybercriminalité (*www.cyberalert.cy*).

En Estonie, les citoyens peuvent contacter des « gendarmes du web » pour signaler les contenus de médias sociaux pouvant être liés à des activités illégales telles que la traite.

La législation française autorise les enquêteurs à **cyber-infiltrer les réseaux criminels**. Les services répressifs emploient des enquêteurs qui patrouillent sur le web pour **repérer les annonces** et **identifier les réseaux criminels**. Des opérations de surveillance ciblée sont également déployées sur des forums internet spécifiques, à l'aide de techniques d'enquêtes discrètes, si nécessaire. Les enquêteurs utilisent également les annonces sur le web pour soumettre les données géographiques émanant d'autres sources à des vérifications croisées, en vue d'identifier les lieux de traite. Les informations issues de différentes sources sont systématisées et utilisées pour **reconstituer les réseaux criminels, c'est-à-dire les liens entre les lieux, les trafiquants et les victimes.** En outre, les services répressifs français s'emploient à établir des **protocoles de coopération** avec les entreprises de réseaux sociaux et les plateformes de location privée en ligne, afin d'encourager la fourniture d'informations. Les hébergeurs de contenu en ligne sont parfois submergés de demandes de transmission d'informations et de preuves ; les autorités ont donc suggéré d'**élaborer des procédures plus directes – et simplifiées – pour faciliter la coopération** entre les hébergeurs de contenu et les services répressifs. Ainsi, le site français Wannonce, parfois utilisé pour des annonces liées à la prostitution de mineurs, envoie un lien aux services répressifs qui leur permet de faire des recherches directes dans sa base de données sous réserve de fournir une adresse électronique. Enfin, en vertu de l'article 6(I)(7) de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), les fournisseurs d'accès à internet et les hébergeurs de sites web sont tenus de contribuer à la lutte contre la diffusion de matériels relatifs à des infractions spécifiques telles que la traite. Ils doivent mettre en place un dispositif bien visible et facilement accessible à l'aide duquel tous les internautes peuvent **signaler les matériels suspects**. Les entreprises sont également tenues d'informer sans délai les pouvoirs publics de toute activité illicite dont elles auraient pris connaissance et qu'exerceraient les destinataires de leurs services. Les citoyens peuvent signaler les contenus en ligne illégaux à la police et à la gendarmerie sur un site web (https://www.internet-signalement.gouv.fr). L'unité de police spécialisée PHAROS (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) examine ensuite les contenus signalés.

En Finlande, la ligne téléphonique d'urgence consacrée à la protection des enfants (*Nettivihje*) permet de signaler du matériel d'abus sexuels sur des enfants et des cas de traite d'enfants en ligne. *Nettivihje* travaille étroitement avec le Bureau national d'enquête et son équipe spécialisée dans les crimes sexuels. La police finlandaise a également un service de signalement en ligne de toute activité suspecte sur internet, y compris la diffusion de matériels pouvant être liés à des infractions sexuelles contre des enfants. Cette stratégie pourrait être étendue au-delà de l'exploitation sexuelle d'enfants.

En Allemagne (en mai 2020), la police a commencé à utiliser un **outil de recherche automatique** pour analyser un gros volume de données publiées sur des sites web d'annonces pour adultes. Cet outil de recherche structure les données de façon à extraire les informations pertinentes au moyen d'indicateurs spécifiques. Les autorités considèrent que cet outil automatisé est « très utile ».

Les autorités grecques assurent la **surveillance des sites web et des forums d'offres d'emplois** ou de services pour détecter les cas de traite en ligne grâce à une étroite coopération entre les unités anti-traite de la police hellénique et la division de la cybercriminalité. En outre, cette division a mis en place des activités de sensibilisation et d'éducation axées sur une utilisation responsable des nouvelles technologies et sur les risques en ligne (les journées de conférence « Surfer en toute sécurité », par exemple), ainsi que le site web et l'application Cyberkid, qui informent les élèves, les parents et les enseignants des formes de violence sur internet et des risques qu'ils pourraient courir sur les sites web des réseaux sociaux. L'ONG Smile of the Child organise régulièrement des événements à l'occasion de la Journée internationale pour un internet plus sûr (9 février).

En Islande, la Police métropolitaine de Reykjavik organise des « **semaines consacrées à internet** », pendant lesquelles elle passe au crible des sites web très fréquentés qui proposent des services sexuels, afin de rechercher les cas de traite. En cas d'activités suspectes, la police demande une ordonnance judiciaire pour placer sur écoute les lignes téléphoniques répertoriées dans les annonces et lancer des enquêtes.

En Irlande, l'Unité de lutte contre la traite des êtres humains et l'Unité d'enquête et de coordination en matière de traite de An Garda Síochána (la police irlandaise) collaborent avec plusieurs sociétés de réseaux sociaux et cabinets de recrutement pour les sensibiliser davantage aux risques potentiels d'offres d'emploi liées à la traite. En général, les entreprises des TIC établies en Irlande et d'autres entreprises internationales coopèrent, lorsque An Garda Síochána leur demande de supprimer des contenus en ligne qui sont jugés illégaux.

En Lettonie, l'Agence nationale pour l'emploi gère un site web officiel qui publie des offres d'emploi. Ce site vise à prévenir les cas d'exploitation par le travail en **offrant un espace sûr pour les annonces**.

En République de Moldova, il n'existe actuellement aucun mécanisme automatisé spécifique permettant d'identifier les annonces et les contenus en ligne susceptibles d'être liés à la traite. Les autorités travaillent avec les Pays-Bas pour acquérir le robot d'exploration élaboré par les services répressifs néerlandais.

Aux Pays-Bas, la **police peut créer de faux profils en ligne** (*lokprofiel*) pour repérer les cas de traite et les trafiquants, puis lancer des enquêtes. En outre, le ministère de la Justice et de la Sécurité étudie actuellement le rôle de la technologie dans chaque phase de la traite

dans le cadre de réunions d'experts et de recherches menées en coopération avec le Centre contre l'exploitation des enfants et la traite (CKM).

En Norvège, le Centre de lutte contre la cybercriminalité développe actuellement une **base de données sur les annonces sexuelles en ligne** publiées sur un site web local. L'objectif est de réaliser ensuite une analyse approfondie.

En Slovénie, un centre pour un internet plus sûr a été créé en 2005 pour sensibiliser le public et faciliter la détection des contenus illégaux en ligne. Il comprend trois grands services : a) un **centre de sensibilisation à l'utilisation responsable d'internet et des nouvelles technologies (Safe.si), qui organise pour les enfants**, les adolescents, les parents, les enseignants et les travailleurs sociaux des activités, des enseignements, des ateliers, des contenus et des campagnes de sensibilisation en ligne et hors ligne ; b) un service d'assistance téléphonique pour les enfants, les jeunes et les parents (également connu sous le nom de « Tom Telephone »), où des conseillers professionnels dispensent également des conseils sur la sécurité sur internet par le biais d'une **salle de chat** ; c) un service de signalement anonyme sur le web des contenus illégaux en ligne.

En Espagne, les autorités pratiquent le **traçage des réseaux sociaux** à l'aide de cyberpatrouilles centrées sur le repérage des victimes de la traite. Ces cyberpatrouilles font partie de l'Unité d'enquête centrale de la Guardia Civil spécialisée dans la lutte contre la traite et elles ont été renforcées pendant la pandémie de covid-19. La Policía Nacional a aussi créé récemment un groupe d'investigation spécialisé dans les cas de traite sur internet (Groupe d'opérations VI pour la lutte contre la cybertraite avec la Brigade centrale de lutte contre la traite de la Policía Nacional).

En Suède, la police assure un **suivi régulier des sites web** proposant des activités de prostitution, afin d'identifier le lieu, l'heure et la date desdites activités. (En vertu du droit suédois, tous les achats de services sexuels sont illégaux.)

En Suisse, certaines forces de police cantonales mènent des **enquêtes discrètes pour contrôler les annonces** des sites web pour adultes ainsi que les personnes impliquées, et repérer les cas de traite.

Au Royaume-Uni, l'autorité de contrôle des contremaîtres et des abus liés aux conditions de travail (GLAA) ainsi que CrimeStoppers ont utilisé Facebook pour informer les demandeurs d'emploi des fausses annonces de recrutement sur les médias sociaux. L'équipe **a créé des annonces de recrutement Facebook** contenant un hyperlien vers une page web de CrimeStoppers, dans laquelle les personnes à la recherche d'un emploi dans le secteur du bâtiment peuvent avoir des informations sur les indicateurs de risque. La campagne ciblait les hommes roumains âgés de 18 à 34 ans, et a atteint plus de 900 000 personnes. Les signalements de cas de traite ont augmenté de 13 % et parmi ces signalements, ceux relatifs à des victimes roumaines ont grimpé de 400 %. Dans le cadre d'une approche interinstitutionnelle (projet AIDANT) regroupant l'Agence nationale de lutte contre la criminalité (NCA), le service de contrôle aux frontières, le service de l'exécution des décisions en matière d'immigration, l'administration fiscale et douanière, la GLAA et les services répressifs, les autorités **élaborent et expérimentent de nouvelles méthodologies pour les signalements dans le secteur de l'industrie.** L'unité de la NCA spécialement conçue pour lutter contre l'esclavage moderne/la traite (MSHTU) s'emploie à relever les normes sur

les sites web pour adultes, en aidant les entreprises à identifier les cas de traite et d'exploitation sur leurs plateformes, et à les signaler aux services répressifs. Ceux-ci utilisent également des procédures automatisées de recherche de renseignements issus de sources ouvertes pour recueillir des informations tirées d'annonces publiées sur des sites web pour adultes. De l'avis des autorités britanniques, il ne serait pas judicieux de fermer les sites web pour adultes, car cela ne mènerait pas à l'élimination de la demande mais au déplacement des annonces vers d'autres plateformes, au détriment des victimes de la traite et des travailleurs du sexe. Par ailleurs, l'application Farm Work Welfare a été conçue pour les travailleurs saisonniers et les employeurs dans les secteurs de l'agriculture et de l'agroalimentaire, et un espace de parole a été créé pour les travailleurs (SAFERjobs, www.safer-jobs.com), afin de favoriser la transparence des chaînes d'approvisionnement et de collecter des renseignements concernant les abus sur le marché de l'emploi. Les organisations jugées non conformes sont à la fois visées par des mesures de répression et des messages destinés à leurs recruteurs finaux pour les sensibiliser, ce qui peut se traduire par une perte d'activité (stratégie de « désignation et stigmatisation »).

En Ukraine, les autorités ont commencé à bloquer les chaînes en ligne sur Telegram qui diffusent des informations sur l'exploitation sexuelle.

3.2. Enquête sur les cas de traite facilitée par les TIC

La présente section explore les stratégies et les bonnes pratiques conçues par les États parties pour accroître l'efficacité des enquêtes dans les affaires de traite facilitée par les TIC. (Ces stratégies et bonnes pratiques devraient être examinées en combinaison avec les mesures liées à l'identification de cas décrites ci-dessus, car l'identification et l'enquête peuvent être étroitement liées).

Plusieurs pays ont souligné l'importance d'offrir une **formation continue** aux membres des forces de l'ordre et de leur proposer des **activités de développement fondées sur de bonnes pratiques locales et mondiales**. La création d'unités spécialisées dans la lutte contre la traite facilitée par les TIC et la formation de leurs agents ont été mentionnées comme une stratégie importante. Plus généralement, de nombreux États parties estiment qu'il est tout aussi important d'**investir dans le capital humain** que dans l'équipement technologique. Parmi les profils spécialisés que les pays jugent indispensables pour enquêter efficacement sur les cas de traite facilitée par les TIC, figurent les agents spécialisés dans les nouvelles technologies, l'analyse criminelle opérationnelle, les enquêtes sous pseudonyme et les renseignements issus de sources ouvertes – OSINT (comme indiqué dans le document soumis par les autorités françaises, les autres pays ayant mentionné des profils similaires). D'après les autorités grecques, des formations devraient être dispensées non seulement sur la maîtrise des outils technologiques, mais aussi sur leur « utilisation éthique du point de vue des droits humains et de la protection des données » (pour en savoir plus sur la formation, voir chapitre suivant).

L'organisation de la formation varie d'un pays à l'autre. Lorsqu'il existe des centres nationaux de lutte contre la cybercriminalité, ils peuvent avoir pour mission d'élaborer des outils et des techniques, ainsi qu'un socle de connaissances, puis de *diffuser* ces connaissances auprès des unités de police et/ou de proposer leur aide en intégrant une autre unité spécialisée, par

exemple les unités de lutte contre la traite. Il est clair que les connaissances relatives aux « méthodes d'enquête et d'analyse informatiques avancées, notamment la sécurité relative aux éléments de preuve tirés des appareils numériques, des systèmes TIC, des fournisseurs d'accès à internet » sont indispensables (document soumis par les autorités norvégiennes). Plusieurs pays (mais pas tous) ont indiqué qu'ils possédaient une unité spécialisée dans la lutte contre la criminalité à forte composante technologique, par exemple des centres/unités de lutte contre la cybercriminalité ou des unités de lutte contre la criminalité faisant appel à des technologies avancées. Ces unités peuvent venir en aide à d'autres unités policières, comme celles spécialisées dans la lutte contre la traite.

Plusieurs pays ont insisté sur l'importance d'intégrer des « **spécialistes du numérique** » dans les enquêtes sur les affaires de traite. Il peut être fait appel à ces enquêteurs pour rechercher des indices en ligne sur la traite. Les autorités françaises recommandent un modèle opérationnel qui prévoirait 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. Point important, ces policiers pourraient être assermentés ou non assermentés ; des groupes d'appui technique des enquêteurs « traditionnels » seraient ainsi créés. Cette idée **s'écarte du modèle policier traditionnel** uniquement centré sur les 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 (des analystes, par exemple).

Outre la formation des agents, les autorités bulgares ont souligné l'importance d'engager des experts informatiques dans les enquêtes sur les affaires de traite et de renforcer la coopération avec le secteur privé. Les autorités chypriotes partagent ce point de vue et citent, comme bonne pratique potentielle, la création d'équipes d'enquêteurs et d'analystes spécialisés dans la traite *et* la cybercriminalité. L'intérêt du **travail d'investigation interinstitutions**, avec la participation et la coopération d'un large éventail d'agents spécialisés, est également mis en avant dans le document soumis par la Suisse, où des équipes communes ont ainsi été créées, et ce modèle pourrait s'étendre à la traite facilitée par les TIC.

Les autorités allemandes ont insisté sur l'importance d'améliorer le **partage des connaissances** entre les institutions et de renforcer les **compétences des policiers en matière de TIC**. D'après les autorités espagnoles, il est à la fois essentiel de « faire connaître davantage la criminalité en ligne » et de « faire participer des spécialistes en criminalité technologique dès le début » des enquêtes en matière de traite. Quelques pays ont également indiqué qu'il était indispensable de former les procureurs à la supervision et à la coordination des enquêtes relatives à la traite à forte composante technologique et/ou de renforcer leurs compétences en la matière, car les preuves électroniques prennent une place croissante dans les affaires de traite.

Pour améliorer les enquêtes sur la traite facilitée par les TIC, l'**importance d'acquérir et d'avoir accès à des logiciels spécialisés** est largement reconnue. Aux Pays-Bas, les autorités ont créé un outil d'exploration du web pour collecter et systématiser de gros volumes de données. Les services répressifs néerlandais testent actuellement l'outil sur des cas concrets de traite pour établir un cadre judiciaire. D'après les autorités néerlandaises, le robot d'exploration « vise principalement les annonces présentant un risque d'exploitation sexuelle et il est actuellement en phase d'essai » ; l'objectif consiste également à déterminer si « l'outil

offre un fondement juridique et une facilité d'utilisation adaptés pour être employé dans les enquêtes formelles ».

De la même façon, l'**importance d'améliorer les capacités de traitement de mégadonnées** a été relevée par plusieurs autres pays, tels que l'Estonie, la République de Moldova et la Grèce. L'élaboration ou l'acquisition d'outils capables de télécharger automatiquement des pages web et d'autres types d'informations électroniques sont considérées comme essentielles à la bonne conduite d'une enquête. Pour cette raison, en 2020, le Bureau de la police criminelle lituanienne a acquis la licence d'un logiciel de collecte d'informations tirées de sources en ligne et la licence d'un logiciel spécialisé dans l'analyse de ces informations. Toutefois, il ne s'agit pas seulement de collecter les données ; il est tout aussi crucial que ces outils aient la capacité de **stocker ces informations de façon sécurisée**, afin qu'elles puissent être utilisées *en toute confiance* « comme preuves devant un tribunal ou comme éléments d'information dans un dossier » (document soumis par la Suède).

Deux autres types d'outils sont considérés comme essentiels pour mener des enquêtes efficaces portant sur la traite facilitée par les TIC : premièrement, des outils qui permettent de télécharger les données de téléphones portables dont le mot de passe n'est pas disponible (document soumis par la Suède) ; deuxièmement, il convient d'élaborer et de mettre en place des outils capables de décrypter les conversations sur les applications de communication personnelle. Les autorités suédoises ont fait observer que ces outils devraient aussi pouvoir décrypter les conversations en temps réel. En Autriche, l'Office de police criminelle élabore un logiciel spécifique dédié à l'examen de téléphones portables en vue d'identifier des victimes de la traite.

Les autorités suisses ont souligné la nécessité d'intensifier les **enquêtes sous pseudonyme** et, partant, d'investir dans la formation d'agents spécialisés. Elles ont également souligné l'importance de disposer de policiers spécialement formés pour lutter contre la traite. Les autorités norvégiennes considèrent que les enquêtes discrètes sont « les plus efficaces », en particulier associées à la collecte de mégadonnées tirées de recherches OSINT et de transferts/flux monétaires. Aux Pays-Bas, la police teste actuellement des « profils d'escrocs » pour identifier les trafiquants lorsqu'ils tentent de recruter des victimes potentielles. De leur côté, les autorités espagnoles ont mis l'accent sur la nécessité d'adapter la législation interne pour exploiter pleinement les possibilités offertes par les enquêtes d'infiltration en ligne.

Selon les autorités britanniques, la **structuration en couches de l'information** est primordiale pour enquêter sur la traite facilitée par les TIC. Il est considéré comme une bonne pratique de renforcer les connaissances de la situation fournies par le renseignement, en y associant des recherches issues des services répressifs et de l'OSINT. Les autorités ont également suggéré d'en finir avec les simples listes d'indicateurs. Elles ont en effet expliqué que, dans le contexte de l'exploitation sexuelle, les enquêteurs suivaient normalement un processus en trois étapes, et non une liste directive d'indicateurs, pour identifier les annonces à haut risque sur les sites web pour adultes. Selon ce processus, le risque est identifié lorsque des annonces de sites web pour adultes font partie d'un réseau, lorsque des indicateurs de travail forcé et de contrôle sont en place et lorsque l'authenticité du compte des annonces est douteuse.

Plusieurs pays préconisent d'améliorer la coopération transfrontalière et d'assurer un échange des données rapide au niveau opérationnel. Les autorités autrichiennes ont mentionné comme bonne pratique **l'échange d'agents** avec les pays d'origine des victimes. D'une manière générale, une coopération internationale renforcée avec les instances chargées des enquêtes dans les pays d'origine est perçue comme une bonne pratique.

Les autorités finlandaises ont souligné l'importance de mener une **analyse stratégique** qui fasse ressortir les tendances émergentes et des informations actualisées sur les modes opératoires des trafiquants (y compris les technologies et les sites web utilisés). Les autorités polonaises partagent ce point de vue. Il est admis que le suivi constant du phénomène est une activité difficile et chronophage pour des ressources policières (souvent) déjà tendues. Toutefois, l'accès à une base de connaissances actualisées, y compris sur les techniques de recrutement des trafiquants, est considéré comme un moyen très efficace de prévenir et combattre la traite. Cette collecte de connaissances devrait avoir une dimension internationale et s'appuyer dans une certaine mesure sur une coordination internationale. Munis de ces informations partagées, les pays peuvent lancer des interventions policières ciblées et, le cas échéant, établir des accords de coopération.

Plusieurs pays notent que les enquêtes pourraient être facilitées si l'on **simplifiait la conservation et l'accessibilité des preuves sur le plan transnational.** Cela peut se traduire par des procédures facilitées et rationalisées pour les demandes envoyées aux unités chargées de conserver les données dans les pays étrangers (demandes de conservation de données), et par la facilitation des demandes d'entraide judiciaire. Comme l'ont fait observer les autorités polonaises, entre autres, c'est « le secteur privé qui est le plus souvent détenteur d'informations intéressant les services répressifs (comme les données sur les abonnés) » et une « acquisition de données par la police rapide et efficace est essentielle pour la conclusion positive d'une enquête ».

3.3. Favoriser la coopération internationale

En s'appuyant sur leur expérience en matière de traite transnationale facilitée par les TIC, les pays ont recensé les « bons principes » qui suivent 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 ;
- établir le contact avec les autres parties intéressées **dès les premiers stades** de l'enquête. Il convient donc d'adopter des mesures organisationnelles qui facilitent ces échanges rapides (par des formalités simples et des points de contact faciles d'accès) ;
- **bien connaître le contexte juridique et les possibilités de coopération** avec un pays ou un ensemble de pays donné pour éviter les blocages et assurer une collaboration en temps utile ;
- 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 ; faciliter l'exécution des demandes d'aide judiciaire internationale et supprimer les obstacles à la recevabilité des preuves dans un pays donné ;

- développer la **compréhension commune** d'approches harmonisées et assurer l'**interopérabilité transnationale** des services répressifs au moyen de sessions de formation transnationales.

À ces principes généraux s'ajoutent plusieurs exemples précis de bonnes pratiques recensés par les États parties. Ces pratiques peuvent être regroupées dans les six grandes catégories ci-dessous.

Équipes communes d'enquête. Un exemple de bonne pratique mentionné par les autorités bulgares en matière de coopération juridique internationale est l'équipe commune d'enquête établie en 2019 avec la France – et le concours d'Eurojust – qui couvre la traite des êtres humains, les abus sexuels d'enfants et la traite de femmes enceintes pour qu'elles vendent leur enfant. De nombreuses activités d'investigation ont été menées par l'ECE en Bulgarie, en France, en Allemagne et en Grèce. Plus généralement, plusieurs pays ont mentionné dans leurs conclusions les ECE comme un exemple de bonne pratique. Comme l'ont indiqué les autorités autrichiennes, elles permettent « un échange d'informations moins bureaucratique pour les enquêtes transnationales, ainsi que la répartition des compétences entre les autorités judiciaires participantes ».

Coopération entre les inspections du travail. L'Agence exécutive bulgare de l'Inspection générale du travail a souligné l'importance de coordonner les inspections et les enquêtes menées conjointement par les pays sur des affaires transnationales complexes, qui concernent des situations potentielles d'exploitation par le travail de travailleurs détachés[16]. Les actions menées conjointement par les services d'inspection du travail bulgare et français (projet Eurodétachement) sont considérées comme un exemple de bonne pratique. Ces actions englobent des inspections conjointes d'entreprises de travail intérimaire qui envoient des travailleurs en France, ainsi que des réunions d'information pour les travailleurs bulgares détachés à l'étranger ou employés directement en France (principalement dans l'agriculture). Des réunions en ligne destinées à échanger des informations et de bonnes pratiques sur les inspections transnationales ont également été organisées. Cet exemple est particulièrement intéressant, car il met en avant l'**importance de la coopération non policière** (tout autant que celle de la coopération policière) dans la lutte contre la traite. Or, elle est moins souvent abordée dans les notes d'orientation. Les États parties pourraient rechercher les moyens d'améliorer la coopération entre les autorités autres que la police, notamment dans la lutte contre la traite aux fins d'exploitation par le travail.

Coopération stratégique. Les autorités allemandes ont souligné l'importance de la coopération stratégique, par exemple via l'action opérationnelle 7.1 du projet EMPACT d'Europol (*Plateforme pluridisciplinaire européenne contre les menaces criminelles*). Ce projet met l'accent sur la traite en ligne. Dans le cadre d'un projet EMPACT, les Pays-Bas et le Royaume-Uni brossent le tableau des TIC qui facilitent la traite.

Actions des cyberpatrouilles coordonnées dans l'UE/ au niveau international. Les autorités néerlandaises et portugaises ont mentionné les journées d'action commune EMPACT/actions des cyberpatrouilles coordonnées sur internet/le darknet comme exemple de

[16] En vertu de la Directive 96/71/CE et dans le cadre du système d'information du marché intérieur (IMI).

bonnes pratiques en matière de coopération internationale. Les renseignements sont d'abord collectés dans les différents pays, puis des actions coordonnées sont lancées.

Tirer parti du réseau d'agents de liaison. Les autorités polonaises et françaises ont souligné l'importance de faire appel à des agents de liaison accrédités pour faciliter l'échange d'informations. Les autorités françaises ont fait état d'une affaire dans laquelle l'aide apportée par les agents de liaison roumains basés en France avait permis de procéder à des arrestations simultanées dans les deux pays. Les autorités ont ainsi pu cibler l'ensemble du réseau criminel transnational, y compris son chef qui dirigeait les opérations en France depuis la Roumanie. Les autorités norvégiennes ont mis l'accent sur l'intérêt que représentait pour elles le fait d'avoir un point de contact aux Philippines pour partager leurs informations sur des affaires en cours, afin d'éviter les chevauchements dans les enquêtes, et les conflits. Grâce au point de contact, les autorités norvégiennes et philippines ont pu partager leurs expériences, les tendances et les études, en ce qui concerne notamment la traite facilitée par internet.

3.4. Identification et assistance des victimes

La présente section décrit la manière dont les États parties tirent profit des outils technologiques pour : a) identifier les victimes ; b) porter assistance aux victimes et c) renseigner les populations vulnérables.

3.4.1. Outils technologiques pour identifier les victimes de la traite

Les outils technologiques basés sur la **reconnaissance faciale** semblent largement utilisés pour lutter contre l'exploitation sexuelle des enfants ; parmi ces outils figurent, par exemple, les outils de vérification croisée d'images par rapport aux bases de données internationales existantes, telles que la base de données du NCMEC (Centre national américain pour les enfants disparus et exploités) ou la base de données internationale d'INTERPOL sur l'exploitation sexuelle des enfants (ICSE)[17]. Toutefois, l'utilisation de ces outils semble plus limitée dans les autres domaines d'exploitation. Les autorités finlandaises ont indiqué qu'elles testaient des outils de reconnaissance faciale pour identifier les victimes d'exploitation sexuelle en ligne, en particulier les webcams. Elles ont également suggéré que l'utilisation de ces outils pouvait être élargie pour couvrir un plus grand nombre de situations de traite. Les autorités lettones ont indiqué qu'elles utilisaient des logiciels spécialisés dans la reconnaissance d'images (PhotoDNA, Clear View) au cas par cas. En Hongrie, les outils de reconnaissance faciale peuvent faire l'objet d'une utilisation ciblée dans une enquête en vue d'identifier des victimes potentielles. Parmi les pays ayant indiqué qu'ils avaient recours à des outils technologiques pour identifier les victimes de la traite en utilisant des mégadonnées, l'Allemagne vient de présenter un outil destiné à explorer des sites web qui hébergent des offres de services sexuels pour aider à identifier les victimes de la traite. Des enquêteurs autrichiens recourent à des **robots d'exploration** et (dans certaines conditions) à des outils de reconnaissance faciale. Au Royaume-Uni, les autorités emploient des outils de collecte

[17] Parmi les outils technologiques utilisés par les pays dans la lutte contre l'exploitation sexuelle des enfants, on peut citer Gridcop et IcacCops. La police islandaise utilise Griffeye pour traiter, trier et analyser des images et des vidéos saisies pendant des enquêtes pour exploitation sexuelle d'enfants, et faire des vérifications croisées de ces images avec des bases de données internationales.

automatique de données en ligne pour extraire et analyser les données des sites web pour adultes pour faciliter l'identification des victimes de la traite.

S'agissant d'utiliser les **indicateurs de la traite (« drapeaux rouges »)**, plusieurs pays ont fait savoir qu'ils *s'appuyaient* sur des indicateurs pour identifier les cas de traite ; néanmoins, ce sont des indicateurs « généraux » de la traite et non des indicateurs spécifiques de la traite facilitée par les TIC. Ce n'est pas surprenant, car l'élaboration d'indicateurs (« drapeaux rouges ») spécifiques de la traite facilitée par les TIC est loin d'être simple, comme l'indique dans le détail le chapitre 2. Les autorités norvégiennes ont déclaré qu'« elles [disposaient] d'un ensemble d'indicateurs pour identifier les victimes de la traite », mais qu'il convenait de le réviser et de l'élargir pour l'adapter aux « enquêtes sur la criminalité liée aux TIC ». Cette tâche est actuellement réalisée par le Groupe national d'experts contre la traite de Norvège.

Les autorités britanniques ont déclaré qu'elles utilisaient une liste d'indicateurs pour faciliter l'**identification des victimes sur les sites web pour adultes**. Leur expérience relative à l'utilisation de ces indicateurs en combinaison avec un outil de collecte automatique de données en ligne est particulièrement instructive. D'après les informations fournies, ces indicateurs peuvent s'avérer précieux, mais « il faut les utiliser en combinaison avec l'analyse des réseaux sociaux et l'appréciation de l'authenticité des témoignages pour garantir une bonne pratique ». Cela met en évidence les difficultés d'automatiser l'identification des victimes – et les lacunes inhérentes au recours excessif à une liste d'indicateurs préétablie. En outre, l'expérience britannique montre l'importance de combiner différentes méthodes, notamment l'**analyse des réseaux sociaux** et l'**appréciation humaine** des preuves. Une fois de plus, le rôle essentiel des analystes/enquêteurs émerge clairement – de même que la nécessité de les former efficacement. Les outils peuvent être très utiles pour effectuer le dépouillement des données et gérer de gros volumes d'information ; ils doivent toutefois être employés par des opérateurs chevronnés qui maîtrisent le thème/la question traitée (la traite, par exemple).

Le recours à l'intelligence artificielle et à des outils technologiques pour identifier les victimes ne va pas sans poser des problèmes, y compris des **préoccupations éthiques** et un risque de discrimination (par exemple, le profilage fondé sur des critères discriminatoires ; voir également la discussion au chapitre 6). Les autorités policières suédoises ont fait part de leurs préoccupations relatives à « l'utilisation de l'intelligence artificielle pour identifier les victimes de la traite ».

Enfin, le Bureau du rapporteur national grec et le Rights Lab de l'université de Nottingham pilotent un projet qui consiste à utiliser des données satellite et de techniques de télédétection pour contrôler les conditions de travail et la mobilité des travailleurs migrants dans l'agriculture. Le rapporteur grec est en voie de développer des applications technologiques supplémentaires pour identifier les victimes de la traite dans le secteur agricole et a fait du développements de ces applications une composante essentielle du Plan d'action national 2019-2023.

3.4.2. Initiatives technologiques destinées à aider les victimes et à renseigner les populations vulnérables

La présente section donne une vue d'ensemble des initiatives technologiques conçues pour aider les victimes et renseigner les populations vulnérables. Il convient de noter que les initiatives décrites ci-dessous ont été recensées par les États parties.

Dispositifs de signalement et lignes d'assistance en ligne. Plusieurs pays ont mis en place des dispositifs pour signaler une victimation anonymement, et recevoir une première aide par des lignes d'assistance. Certaines lignes d'assistance offrent un appui 24 heures sur 24 et peuvent orienter les victimes vers les services sociaux, en leur expliquant les procédures à suivre et leurs droits. Aux Pays-Bas, plusieurs organisations offrent une **assistance numérique par la voie d'une fonction de conversation** (Fier et Slachtofferhulp Nederland sont les noms de deux de ces organisations). Ces organisations donnent les premiers conseils, une assistance et la possibilité de signaler anonymement les cas d'exploitation sexuelle. La fonction de conversation ne répond pas seulement à une situation, mais elle vise aussi à établir le contact avec des personnes vulnérables à des fins préventives. Le ministère néerlandais de la Justice et de la Sécurité examine actuellement comment cet outil peut être perfectionné en collaboration avec les acteurs pertinents. En France, le ministère de l'Intérieur gère une plateforme de signalement des violences sexuelles et fondées sur le genre. Les victimes peuvent entrer en communication avec un agent public par **messagerie instantanée/conversation en ligne**, faire un signalement et recevoir une aide de première urgence.

Documents officiels en ligne. Les sites web officiels publient souvent des documents d'information produits par les autorités. En Autriche par exemple, des informations destinées aux victimes de la traite fournies par le ministère fédéral de l'Intérieur et par des ONG sont disponibles dans plusieurs langues sur des plateformes en ligne et divers médias sociaux. Sur le site web du ministère fédéral de la Justice, les victimes de la traite peuvent accéder à des documents rédigés dans 16 langues sur leurs droits à une assistance juridique et psychosociale. En Pologne, le ministère de l'Intérieur et de l'Administration et le ministère des Affaires étrangères ont lancé une campagne en ligne sur le site web « e-konsulat » avec un bandeau qui affiche des informations sur la traite dans plusieurs langues et renvoie les visiteurs du site vers le Centre de consultation et d'intervention pour les victimes de la traite (KCIK). Outre ces canaux officiels, plusieurs pays ont souligné le rôle important joué par les ONG dans la diffusion d'informations au moyen de leurs sites web et de leurs comptes officiels sur des médias sociaux tels que Facebook, Instagram et YouTube.

Outils en ligne et applications. La Commission nationale bulgare de lutte contre la traite des êtres humains a lancé un outil de prévention en ligne dans le cadre de la campagne annuelle de prévention de la traite aux fins d'exploitation par le travail. Créé en coopération avec une ONG tchèque, cet outil en ligne a été conçu pour les Bulgares à la recherche d'un emploi en République tchèque. Il fournit des renseignements sur les conditions de travail et les risques de violation des droits des travailleurs. Comme l'a noté la commission bulgare, « cet outil s'est avéré efficace à l'usage, car peu de temps après sa mise en fonctionnement, une contrefaçon a été créée pour attirer les victimes potentielles de l'exploitation par le travail ». En Lituanie, une application nommée Raktas (disponible sur Google Play) a été développée récemment pour sensibiliser les Lituaniens qui vivent et travaillent à l'étranger

aux signes précurseurs de la traite. Dans une version améliorée, l'application comprendra une fonction de conversation qui permettra aux Lituaniens victimes ou victimes présumées de la traite de contacter une ONG lituanienne en temps réel et de demander de l'aide. L'Autorité pour les conditions de travail au Portugal a développé l'application ACT, *Agir Contra o Tráfico*. Les autorités estoniennes signalent que des notifications en masse ont été envoyées sous la forme de SMS/messages textuels dans le cadre d'une campagne contre l'exploitation sexuelle. En 2017, l'Espagne a lancé l'application mobile « Chicas Nuevas 24 horas: Happy » pour que les jeunes gens découvrent le voyage d'une jeune fille (Happy) par le biais d'un jeu vidéo, depuis son départ de sa ville natale au Nigéria jusqu'à son expérience d'exploitation sexuelle en Espagne.

Campagnes de sensibilisation en ligne. En Bulgarie, la Commission nationale de lutte contre la traite des êtres humains mène chaque année trois campagnes de prévention et d'information à l'échelle nationale, qui englobent des événements pour prévenir la traite tant aux fins de travail forcé que d'exploitation sexuelle. Des documents sont également distribués en ligne. Plus de deux millions d'utilisateurs actifs bulgares ont pu être informés sur Facebook et sur Instagram pendant la campagne d'octobre/novembre 2018. Plus généralement, des informations sur les activités de cette commission nationale et les outils de prévention en ligne associés sont régulièrement mis à disposition sur les médias sociaux. Ces messages atteignent environ 100 000 utilisateurs par an. En outre, des discussions sur les TIC, internet, les médias sociaux et l'impact des nouvelles technologies sur la traite, ainsi que leur utilisation pour recruter et exploiter les victimes, sont incluses dans différentes activités de sensibilisation à l'échelle locale et nationale, ciblant les jeunes et les élèves. L'Agence exécutive de l'Inspection générale du travail organise des campagnes d'information sur les risques liés au fait de travailler à l'étranger, et y participe ; de plus, elle gère une ligne téléphonique de conseil et de signalement qui est aussi ouverte aux citoyens bulgares travaillant à l'étranger.

En Irlande, la campagne Blue Blindfold menée par le Département de la justice adresse régulièrement des informations aux populations vulnérables par le biais d'un site web dédié, de documents imprimés et des médias sociaux.

En Allemagne, le ministère fédéral de la Coopération économique et du Développement a élaboré des projets avec des pays partenaires pour prévenir et combattre la traite. Par exemple, dans le cadre du projet « Prévenir la traite dans les Balkans occidentaux et soutenir les victimes », l'Initiative régionale en matière de migration, d'asile et de retour des réfugiés (MARRI) a permis d'élaborer des notes d'orientation et des supports d'information pour des campagnes de sensibilisation du public, et de les mettre à disposition en ligne. Étant donné qu'internet est de plus en plus utilisé pour recruter les victimes de la traite, l'une des boîtes à outils mettait l'accent sur les menaces auxquelles les enfants sont exposés lorsqu'ils naviguent sur le web[18].

En Roumanie, l'Agence nationale de lutte contre la traite des personnes (ANITP) dirige des campagnes sur Facebook, YouTube et, depuis 2020, Instagram, Twitter et LinkedIn. Les messages Facebook ont atteint 2,5 millions d'utilisateurs en 2020 (+300 % par rapport à l'année précédente). Parmi les initiatives déployées figurent :

[18] « Mineurs exposés au risque de cybertraite » (https://toolboxes.marri-rc.org.mk/tips/minors-at-risk-of-cyber-trafficking).

a. l'envoi quotidien sur les réseaux sociaux de messages de prévention anti-traite sur différents types d'exploitation (exploitation sexuelle, exploitation par le travail et mendicité forcée) ;

b. la campagne en ligne intitulée « The perfect Job – one way illusion », organisée en partenariat avec OLX Romania (service web d'hébergement d'annonces) pour prévenir la traite en sensibilisant les personnes en recherche d'emploi sur les plateformes en ligne ;

c. la mise à contribution de deux vidéoblogueurs roumains bien connus sur YouTube, qui regroupent à eux deux 1,3 million d'abonnés, pour accroître la visibilité et l'efficacité des messages anti-traite de l'ANITP. Les vidéoblogueurs ont enregistré deux vidéos sur la traite, qui ont compté environ 100 000 vues sur YouTube dès leurs premières heures de diffusion.

En conclusion, il convient de relever que, comme l'ont fait remarquer les autorités bulgares, une campagne efficace exige « beaucoup de travail préparatoire » pour bien cerner sa cible et préparer un message adéquat. Finalement, cela requiert des investissements. Une bonne pratique consiste à collaborer avec des entreprises privées pour diffuser des **annonces à caractère social**. Cela peut se faire, par exemple, par la voie de publications élaborées sous le parrainage de réseaux sociaux tels que Facebook et Instagram. (La plateforme peut fournir des espaces et son expertise en matière de conception d'une campagne ou d'un message.) Les campagnes en ligne ciblées et bien conçues peuvent clairement constituer un outil précieux. L'exemple d'une campagne menée par la Commission nationale bulgare de lutte contre la traite des êtres humains est éloquent. Dans le cadre de la campagne conçue pour sensibiliser à la traite aux fins d'exploitation par le travail, une offre d'emploi trompeuse a été produite et diffusée. Certains internautes se sont leurrés et ont commencé à appeler le bureau de la Commission nationale pour en savoir plus (voir section 1.1.2 pour en savoir plus sur la campagne). Cet exemple montre bien la portée/l'impact potentiel de ces offres d'emploi trompeuses, mais il a également donné à la Commission « une bonne occasion d'informer les demandeurs d'emploi qui sont prêts à accepter des offres douteuses ».

Toutefois, comme l'ont signalé les autorités bulgares, il existe un **risque de recourir excessivement à des campagnes en ligne** pour atteindre les victimes potentielles. Dans certains cas, les victimes sont issues de « groupes vulnérables » qui se caractérisent par un faible niveau d'instruction et une connaissance limitée des outils et des ressources technologiques. Dans ces circonstances, une action locale, fondée sur un contact (personnel) direct a (encore) un rôle crucial à jouer dans la stratégie de prévention.

Enfin, les initiatives peuvent s'inspirer de projets traitant de problèmes similaires à celui de la traite en ligne et facilitée par la technologie. En Finlande par exemple, l'ONG Women's Line a lancé un projet nommé *Turv@verkko,* qui vise à prévenir les cyberviolences à l'égard des femmes et des filles, et à porter assistance aux victimes. De la même façon, Youth Exit et *Sua varten* ciblent les jeunes internautes pour les protéger contre le harcèlement sexuel en ligne. Bien qu'elles ne soient pas directement liées à la traite, ces initiatives pourraient offrir des suggestions utiles pour élaborer des projets en faveur des victimes de la traite.

3.5. Informations communiquées par les ONG

Les ONG ont présenté un certain nombre de stratégies conçues pour améliorer la détection, l'assistance aux victimes et la sensibilisation à la traite en ligne et facilitée par la technologie.

La Strada International, KOK (Allemagne), Astrée (Suisse) et La Strada Moldova ont souligné l'importance, pour les personnes soumises à la traite et celles vulnérables à l'exploitation et aux abus, d'accéder facilement à des **informations adéquates et actualisées**, portant notamment sur les organismes de soutien et leurs permanences téléphoniques. Ces plateformes en ligne devraient également **permettre l'auto-identification** des victimes. D'après la Strada International, les ONG devraient partager les informations pertinentes dont elles disposent avec les services répressifs – sous réserve d'avoir obtenu le consentement des personnes concernées. Des initiatives visant à encourager les victimes elles-mêmes à faire connaître les cas d'exploitation par le travail sont également prévues, par exemple sous la forme de plateformes en ligne et d'applications qui permettent de signaler anonymement les abus liés aux conditions de travail sur site (informations fournies par la Sustainable Rescue Foundation, Pays-Bas).

La mise à disposition d'informations en ligne et les mécanismes d'auto-identification devraient être accompagnés de **campagnes de sensibilisation**. La Strada International considère que deux types de campagnes sont particulièrement importantes : a) celles qui s'adressent directement aux victimes potentielles et aux personnes exposées à un risque d'exploitation et d'abus ; et b) celles visant à encourager les différents acteurs à reconnaître les risques liés à la traite facilitée par la technologie et à signaler les cas observés. Les organisations « Différents et égaux » (Albanie) et KOK (Allemagne) ont souligné l'importance de sensibiliser les utilisateurs de TIC aux risques inhérents à la technologie. Les deux organisations ont préconisé le lancement de campagnes plus vastes pour **que le public comprenne la façon dont les trafiquants peuvent exploiter la technologie** et les risques auxquels les personnes vulnérables sont exposées (les jeunes en particulier). L'accent devrait être mis sur le recrutement, et notamment sur la façon dont une situation d'exploitation peut s'amorcer (c'est-à-dire la façon dont les trafiquants établissent le premier contact). Les entreprises qui fournissent des services en ligne et liés aux TIC devraient participer à ces efforts. Le Centre irlandais des droits des migrants a également relevé que les entreprises de médias sociaux devraient renforcer la dissuasion.

En outre, plusieurs ONG, dont La Strada International et Sustainable Rescue Foundation, ont souligné l'importance d'accroître et d'améliorer les **échanges de données** entre les acteurs concernés. Ces échanges doivent englober des connaissances actualisées sur les risques liés à la technologie.

Par ailleurs, les ONG ont insisté sur l'importance de développer les connaissances des organisations qui apportent une aide aux victimes, y compris des services de conseils, à propos des risques liés aux TIC et, plus généralement, de 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 sont les premiers intervenants doivent impérativement connaître des méthodes de préservation des preuves électroniques (par exemple, la sauvegarde de l'historique des chats). Il est considéré comme crucial de dispenser

des formations complètes sur la sécurité et la traçabilité des données sur internet aux conseillers et aux ONG.

FIZ (Suisse) a fait observer que les TIC, notamment les médias sociaux et les informations en ligne, peuvent aider les ONG à établir des contacts avec les victimes présumées et à rassembler des informations supplémentaires sur les circonstances de l'exploitation. Si elles sont averties d'une situation suspecte, les ONG peuvent ainsi **tirer parti des informations disponibles en ligne pour prendre contact avec une victime présumée**.

Le Centre irlandais des droits des migrants et Astrée (Suisse) ont proposé de créer des services d'enquête spécialisés dans la criminalité numérique et particulièrement la traite facilitée par la technologie. Praksis (Grèce) a recommandé que les compétences des services répressifs soient améliorées dans le domaine des TIC et de leurs risques. En outre, l'organisation a préconisé une coopération et des échanges améliorés entre les autorités et les entreprises privées.

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 précisent qu'elles utilisent des indicateurs standard, mais demandent une **révision de ces indicateurs**, afin que soient prises en compte les spécificités de la traite facilitée par la technologie, et particulièrement le recrutement et l'exploitation par le biais des TIC. KOK (Allemagne) a suggéré que le suivi des sites web où les clients partagent leur expérience en matière d'achat de services sexuels pourrait fournir des indices de prostitution forcée/traite. La révision des « drapeaux rouges » pourrait prévoir l'ajout d'indicateurs applicables à ces sites web.

3.5.1. Le point sur les initiatives technologiques

La Strada International constate que ses membres et d'autres ONG ont « de plus en plus » recours à la technologie. Néanmoins, bien que « les ressources et les possibilités techniques augmentent considérablement », leur utilisation par les ONG reste « limitée ». D'après La Strada International, la technologie est principalement employée pour enregistrer les données avant de les analyser, et assurer le suivi des activités d'assistance. Les ONG recourent de plus en plus à la technologie, y compris les médias sociaux, pour mener des campagnes (à des fins de sensibilisation, par exemple ; voir ci-dessous) et fournir des informations, ainsi que pour « entrer en contact avec les groupes vulnérables ou se joindre à des communautés en ligne » (document soumis par La Strada International). Dans le cadre de l'étude en cours, les ONG ont été invitées à donner des exemples d'initiatives technologiques destinées à améliorer la détection des infractions de traite en ligne et facilitée par la technologie, l'identification des victimes et la prévention des infractions. Vous trouverez ci-après un bref aperçu de ces initiatives, fondé sur les informations communiquées par les ONG.

Dispositifs d'autosignalement en ligne et prise de contact avec des victimes potentielles

- La Strada Moldova a mentionné des dispositifs en ligne d'autosignalement par les enfants de problèmes de cybersécurité rencontrés (www.siguronline.md). Ces problèmes comprennent des situations désagréables auxquelles les enfants peuvent être confrontés sur internet. L'enfant est ensuite mis en contact avec un conseiller spécialisé et, si des preuves

d'exploitation ou d'abus sexuels en ligne sont établies, l'affaire est transmise aux services répressifs.

- En Suisse, l'organisation Astrée a observé un nombre croissant de victimes qui se présentent d'elles-mêmes auprès de ses services, et de victimes potentielles orientées par des amis ou des clients grâce à la présence en ligne de l'organisation. Astrée propose aussi un formulaire en ligne permettant aux victimes d'entrer en contact et de demander de l'aide. De son côté, FIZ a indiqué que les plateformes de médias sociaux facilitaient la prise de contact avec les victimes potentielles de la traite si le nom de la personne est connu. Le site web de la Plateforme suisse contre la traite des êtres humains contient des liens vers un certain nombre d'organisations qui peuvent apporter une assistance.

- Fair Work (Pays-Bas) s'appuie sur les médias sociaux pour atteindre les communautés migrantes en vue d'identifier les personnes soumises à la traite ou à des situations d'exploitation. L'organisation commence par repérer des pages Facebook qui intéressent un groupe cible spécifique, puis partage des informations sur ces pages. Elle crée des comptes personnels anonymes, gérés par des bénévoles, qui ont un rôle de prévention. Étant donné que les travailleurs migrants s'informent souvent par la voie des médias sociaux, ceux-ci peuvent être employés pour aider les personnes en danger « à sortir de l'isolement et à acquérir de l'autonomie » ainsi que pour réduire les risques de traite (document présenté par La Strada International). Néanmoins, il n'est pas toujours « aisé pour les victimes, surtout si elles connaissent mal le pays et les droits dont elles y jouissent, de savoir où trouver des informations adéquates et de déterminer lesquelles sont fiables ; d'identifier parmi les personnes à contacter celles qui sont le mieux à même de les aider ».

- La Strada International a indiqué que l'un de ses membres avait élaboré des services de consultation en ligne permettant de recevoir des conseils et de signaler les cas d'exploitation et d'abus – en sus des services d'assistance téléphonique.

- La Strada International a également expliqué que ses membres utilisaient normalement des plateformes en ligne, telles que Facebook, Instagram, LinkedIn et autres sites web, pour faire connaître leur action. De la même façon, KOK (Allemagne) a fait savoir que ses membres avaient recours à des sites web, Facebook et WhatsApp pour diffuser des informations et ouvrir des voies de communication avec les victimes potentielles. Point important, une organisation offre un numéro WhatsApp aux clients, afin qu'ils puissent signaler l'exploitation potentielle de travailleurs du sexe.

Applications mobiles de sensibilisation et d'aide/information

- La Strada République tchèque a participé à la création de SAFE, une application élaborée par l'OIM Slovaquie sous la forme d'un jeu interactif conçu pour prévenir la traite. Dans ce jeu, les utilisateurs évaluent leur risque en matière de traite ; l'application contient également des informations sur la sécurité des voyageurs, le travail à l'étranger et des contacts utiles en cas d'urgence. Astra (Serbie) a développé BAN Human Trafficking, une application conçue pour sensibiliser les jeunes aux situations pouvant conduire à une exploitation, et pour donner des conseils pour apprendre à les repérer. L'organisation prévoit de la mettre à niveau avec une fonction permettant de signaler les pratiques d'exploitation.

- La Strada International a mentionné plusieurs applications créées par des ONG pour signaler les cas d'exploitation et d'abus, comme celle développée par Unseen (Royaume-Uni). En Albanie, l'ONG « Différents et égaux » participe à l'élaboration de diverses applications mobiles (par exemple, "*#raporto #shpeto*") destinées à aider les victimes de la traite et de violences fondées sur le genre ("*#GjejZa*").

- La Strada International a en outre noté que des applications étaient développées pour soutenir les groupes vulnérables, en leur donnant par exemple accès à l'information, comme les droits en matière d'emploi dans le pays de destination. On peut citer Workeen App – A Game for Labour Market Integration of Migrants, application produite dans le cadre du projet Sirius pour aider les migrants en recherche d'emploi. Hors d'Europe, la plateforme Apprise Audit, développée par le Mekong club et l'Institut universitaire de l'ONU de Macao, permet de mener des entretiens avec les travailleurs en toute sécurité et en toute confidentialité dans la langue des personnes interrogées.

Campagnes de sensibilisation en ligne

- En 2019, à l'occasion de la Journée internationale pour un internet plus sûr, la Strada Moldova a organisé une campagne pour sensibiliser les jeunes à la sextorsion. Les citoyens ont été encouragés à signaler les infractions au moyen d'un mécanisme de signalement en ligne sûr (www.siguronline.md). La campagne a atteint environ 70 000 utilisateurs en ligne. La même organisation a testé des stratégies de profilage pour que ses messages en ligne atteignent un public cible, défini en fonction de l'âge, des centres d'intérêt et du profil des utilisateurs en ligne.

- L'ONG « Différents et égaux » (Albanie) a mené plusieurs campagnes de sensibilisation en ligne à l'aide de réseaux sociaux et d'applications (notamment Facebook, Instagram, Twitter, des sites internet et YouTube), en mettant l'accent sur la prévention de la traite, des abus sexuels et de la violence domestique (atteignant environ 15 000 utilisateurs). Une campagne a été lancée, avec le concours d'autres d'ONG, pendant la pandémie de covid-19.

- Novi put (Bosnie-Herzégovine) a déployé plusieurs campagnes de sensibilisation centrées sur l'utilisation de la technologie relative à la traite et à l'exploitation sexuelle des enfants.

- Astra (Serbie) a mené des campagnes de sensibilisation sur les principales techniques de recrutement, à savoir les offres d'emploi sur internet et la sollicitation d'enfants à des fins sexuelles via Facebook et les réseaux sociaux ; ses campagnes décrivaient aussi les stratégies visant à contrôler et exploiter les victimes (y compris en les géolocalisant à l'aide d'options de localisation disponibles sur de nombreuses applications couramment utilisées).

Autres initiatives

- En 2018, Astra (Serbie) a réalisé une expérience nommée « fille virtuelle » – profil d'une jeune internaute de 15 ans. En 24 heures, ce profil a reçu plus de 3 000 demandes, notamment des offres d'emploi et des offres sexuelles explicites émanant d'hommes adultes (document soumis par La Strada International).

- Dans le cadre de son programme de réintégration, l'ONG « Différents et égaux » (Albanie) dispense des formations sur l'utilisation des technologies informatiques, qui englobent des techniques de protection des données.

- La Strada International a relevé certaines initiatives public-privé auxquelles des ONG participent, par exemple un projet lancé par l'université d'Amsterdam avec de grandes banques néerlandaises pour identifier les cas de traite. Des ONG basées aux Pays-Bas, notamment FairWork, CoMensha et La Strada International, ont été consultées dans le cadre de cette initiative.

Une vision à long terme pour résoudre des problèmes cruciaux

De nombreuses ONG s'accordent 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. FIZ (Suisse) a suggéré de perfectionner les outils conçus pour dénoncer anonymement les actes de violence et d'exploitation, et faciliter les contacts avec les ONG qui offrent aux victimes des services de protection et de conseil. KOK (Allemagne) a souligné l'importance de développer des ressources visuelles, par exemple des vidéos, des images et des applications, qui serviront dans le cadre des formations, et pourront être diffusées en ligne auprès des populations vulnérables.

Des ONG ont également soulevé des **questions cruciales** portant sur les initiatives et les outils technologiques. La Strada International a indiqué que les outils technologiques étaient généralement produits dans le cadre de projets autonomes et « n'étaient pas souvent soumis à des périodes d'essai ». Il y a donc très peu de preuves de leur efficacité. En outre, lorsque le financement d'un projet prend fin, la plupart du temps, aucune stratégie financière à long terme n'est mise sur pied pour promouvoir et utiliser les outils produits. Cela pose particulièrement problème avec des outils qui nécessitent « constamment des mises à jour et des formations ».

La Strada International a également constaté que « souvent, les ONG et autres parties prenantes qui devraient utiliser les outils dans la pratique et s'en approprier la maîtrise ne participent pas suffisamment aux initiatives ». Selon l'organisation, il reste « difficile de déterminer dans quelle mesure la technologie a contribué à prévenir ou à combattre la traite » ; les questions de savoir si « la surveillance et le profilage aux frontières et à d'autres endroits [ont] réellement mené à l'identification de victimes de la traite » et si les personnes identifiées par des moyens technologiques ont ensuite reçu « assistance et protection » restent ouvertes. L'organisation a réclamé que « tous les outils technologiques mis au point » fassent l'objet d'**une évaluation et d'une analyse d'impact plus poussées**. Elle a demandé « si ces outils – souvent coûteux – répondaient aux besoins des acteurs de la lutte contre la traite et s'ils avaient été de fait testés et bien employés, et si non, pour quelle raison ».

Avant toute chose, les ONG ont affirmé que, d'une manière générale, il existait peu d'outils technologiques à la disposition des professionnels. Pour répondre aux besoins des ONG, **les outils doivent être « peu coûteux et faciles à utiliser »**. La Sustainable Resource Foundation a également prévenu que les outils « engendrent un excédent de données pour

différents utilisateurs » ; lors de leur élaboration, il est donc essentiel de garder à l'esprit les besoins spécifiques et une stratégie globale, afin d'éviter la duplication d'outils assurant des fonctions (simples) et, dans le même temps, le manque d'outils dotés de fonctions complexes et plus stratégiques.

3.6. Informations communiquées par les entreprises de technologie

Facebook a fait état de diverses **collaborations dans le monde avec des ONG** destinées à concevoir des campagnes d'éducation visant à mieux faire connaître aux jeunes internautes, en particulier, les risques d'exploitation sexuelle en ligne, et les droits des victimes potentielles de l'exploitation par le travail et de la servitude domestique. Ces campagnes apportent également des informations sur les services d'assistance téléphonique qui proposent aide et soutien aux victimes de la traite. Facebook a cité en exemple une campagne de sensibilisation lancée en mars 2021, en partenariat avec Stop the Traffik, sur l'exploitation par le travail et la servitude domestique ; son objectif est d'informer les employés de maison et les travailleurs peu qualifiés aux Philippines de leurs droits, des directives relatives au recrutement local pour les demandes d'emploi à l'étranger, et des permanences téléphoniques disponibles pour éviter le recrutement illégal et les abus.

Facebook a également mentionné la création d'un raccourci pour fournir des informations et des ressources supplémentaires aux personnes qui recherchent des termes liés à l'exploitation sexuelle. Ces termes ont été définis par des experts internes et externes.

Pour faire face à des signalements qui restent insuffisants, les responsables de Facebook ont indiqué qu'ils préparaient « des mesures de prévention par rapport aux contenus relatifs à la traite ». Ils ont mis en avant « l'accroissement » de leurs capacités de « détecter les contenus illégaux [qui] témoignait directement de l'investissement majeur de [leurs] équipes techniques et opérationnelles ».

IBM et Stop the Traffik, une ONG basée au Royaume-Uni, ont établi un partenariat en 2014 pour créer le Traffik Analysis Hub ; cette nouvelle entité gère une **plateforme collaborative de partage des données** qui s'appuie sur l'analyse sécurisée d'un contenu multilingue en nuage ou fondé sur l'intelligence artificielle, et sur l'analyse géospatiale. Le Hub regroupe 95 organisations dans le monde. La plateforme vise à perturber le fonctionnement de la traite à l'échelle mondiale, en réunissant des ONG (par exemple, Stop the Traffik, Liberty Shared, CrimeStoppers et Save the Children (Royaume-Uni)), des services répressifs (Europol, Interpol et plusieurs autorités policières des États-Unis) et des institutions financières (Western Union, Barclays, Standard Chartered, Lloyds et Paypal). Comme l'a expliqué IBM, le Traffik Analysis Hub utilise des modèles d'intelligence artificielle (IA) personnalisés propres à un domaine pour localiser les sources des données recueillies à grande échelle et pour trier ces informations en s'appuyant sur un système de classification élaboré par la communauté d'experts du Hub. Les données sont ensuite partagées entre les organisations participantes. L'un des principaux produits est le « Red-Flag Accelerator », une bibliothèque de typologies, élaborée à partir des transactions « drapeaux rouges » relevées sur les comptes des victimes. Ces indicateurs « drapeaux rouges » doivent être intégrés dans les systèmes de suivi des institutions financières participantes. En outre, le Hub vise à développer un outil prévisionnel de

corrélation, afin d'identifier les caractéristiques des communautés vulnérables qui sont exposées au risque de traite.

En outre, IBM a récemment lancé la **feuille de route d'une formation en ligne gratuite** à destination des personnes qui souhaitent devenir analystes de données dans le domaine de la traite. La formation comprend des modules sur la traite (introduction à la traite ; comment repérer des signes de traite) et d'autres sur la science des données et l'utilisation des technologies pour l'analyse des données.

IBM parraine également les compétitions DataJam en ligne, au cours desquelles ses experts travaillent avec des équipes multisectorielles pour trouver des innovations technologiques au service de la lutte contre la traite. Les exemples englobent :

- des outils destinés à extraire les informations contenues dans les sites d'annonces en ligne pour adultes, à appliquer les marqueurs d'une participation forcée (par exemple, la langue d'une tierce partie, plusieurs annonces utilisant le même identifiant de contact, des annonces relatives à la nationalité des victimes connues historiquement) et à effectuer une analyse typologique géospatiale sur les annonces « retenues » ;
- des outils destinés à extraire les informations contenues dans les marchés du web profond/dark web et les messages des forums, à appliquer des marqueurs spécifiques de la traite via l'IA, à identifier les tendances et les pseudonymes, à créer des modèles réseau de rubriques en vue des analyses futures des services répressifs ;
- des outils permettant de valider les offres d'emploi en ligne sur les smartphones, afin que les utilisateurs puissent vérifier la légitimité des offres d'emploi en ligne avant de s'engager.

Pour ce qui est de la **coopération avec les services répressifs**, Facebook a fait état de son engagement dans plusieurs partenariats public/privé (PPP), comme le groupe d'experts sur la traite des êtres humains (HTEG) d'Interpol. La société a également indiqué qu'elle avait mis en place un système de demandes en ligne pour les services répressifs (LEORS, Law Enforcement Online Requests System), destiné à simplifier les demandes juridiques de données de compte Facebook (y compris les demandes liées à la traite). Les demandes soumises par le biais de LEORS sont gérées par des équipes basées aux États-Unis, en Irlande et à Singapour.

3.7. Autres informations issues de l'analyse contextuelle

Outre les informations communiquées par les États parties, par les ONG et par les entreprises technologiques, les auteurs de la présente étude ont effectué une recherche documentaire sur la base d'informations factuelles disponibles concernant les stratégies et les outils employés pour lutter contre la traite en ligne et facilitée par la technologie.

L'OSCE et Tech against Trafficking (2020) ont mené une étude sur les outils TIC et les initiatives développés pour combattre la traite. Ils ont recensé 305 outils et initiatives élaborés par des entreprises du secteur privé, des associations caritatives et des gouvernements (en anglais pour la plupart). Sur ces outils : 26 % ont été conçus pour identifier victimes et trafiquants ; 16 % dans un but de sensibilisation ; 14 % pour la gestion de la chaîne

d'approvisionnement ; 13 % pour les tendances de données et la cartographie ; 10 % pour l'identification des risques collectifs ; 9 % pour la motivation et l'autonomisation des travailleurs, et 12 % à d'autres fins. Les outils et les initiatives examinés par l'OSCE et Tech against Trafficking visent les objectifs suivants : a) la diffusion d'informations auprès de populations vulnérables, y compris des migrants; b) l'éducation relative aux risques de traite, à la recherche d'une aide et au signalement de cas potentiels ; c) la suppression des possibilités d'exploitation ; d) l'identification des victimes ; e) la collecte d'informations accessibles au public pour lutter contre la traite ; f) l'évaluation des risques de traite ; g) le suivi et la conformité ; h) l'identification et la gestion de typologies. Dans le même esprit, Raets et Janssens (2018) ont recensé les (multiples) moyens suivants d'utiliser les outils technologiques dans la lutte contre la traite : a) l'agrégation et l'analyse de données ; b) la chaîne de blocs (*blockchain*) pour la traçabilité et la provenance (contrôle des chaînes d'approvisionnement) ; c) l'intelligence artificielle (IA) et l'apprentissage automatique pour obtenir une puissance de calcul élevée ; d) la reconnaissance faciale (exploration du web) ; e) la technologie au service des victimes et des survivants : identifier et soutenir les victimes, sensibiliser le public dans différentes langues. Muraszkiewicz (2018) a cité des moyens supplémentaires d'employer des outils technologiques pour lutter contre la traite : l'exploration du web ; l'analyse des données ; la prévision policière ; l'utilisation de la *blockchain* ; les systèmes d'information géographique (SIG) ; les bases de données en ligne ; et les initiatives de production participative. Il est parfois difficile de déterminer lesquels de ces outils fonctionnent réellement, lesquels peuvent être exploités à plus grande échelle et lesquels apportent de réels avantages aux victimes de la traite. (Certains outils examinés semblent recueillir des informations qui sont ensuite difficiles à traiter.) Les informations obtenues par des moyens technologiques doivent être exploitables. Dans le cas exposé par Rende Taylor et Shih (2019), les signalements de travailleurs sous la forme de commentaires d'applications évoquant l'exploitation par le travail dans les chaînes d'approvisionnement n'ont guère été exploitées.

La littérature indique que la technologie ne peut pas se substituer aux connaissances sur le terrain. En outre, selon les agents des services répressifs interrogés par Elliott et McCartan (2013), les technologies de la téléphonie mobile, applications incluses, peuvent faire partie d'une boîte à outils de lutte contre la traite, mais ne sont pas une solution miracle. Étant donné que, sur le plan opérationnel, les fournisseurs de services internet sont considérés comme des entités qui détiennent une grande part des preuves électroniques, plusieurs sources ont souligné l'importance d'une étroite coopération avec le secteur privé. Cette coopération devrait comprendre des dispositifs facilitant l'obtention de preuves, l'élimination de ces preuves le cas échéant, et le signalement rapide aux services répressifs dans des cas précis. Dans le même temps, plusieurs obstacles au partage de l'information entre les différents acteurs ont été identifiés. Ils englobent des questions relatives à la confidentialité des données à caractère personnel et à la sécurité. Des appels ont également été lancés en faveur de normes (multilatérales) communes internationales qui sous-tendraient la collaboration entre les services répressifs, les ONG et le secteur privé.

Seul un très petit ensemble d'outils spécifiques a fait l'objet de plusieurs mentions dans diverses sources. Ces outils englobent : a) le projet Artemis de Microsoft, qui a développé un outil pour détecter les techniques de sollicitation d'enfants à des fins sexuelles en créant un score de risques pour les conversations basé sur les affaires passées, afin de signaler les

conversations les plus suspectes que les modérateurs humains inspecteront ; b) PhotoDNA de Microsoft, qui crée une empreinte numérique unique (hachage) pour chaque image, et sert à détecter l'exploitation sexuelle d'enfants.

La Confédération internationale du travail indique qu'une campagne de sensibilisation a été menée par AidRom pour informer les personnes qui recherchent des emplois à l'étranger sur internet. Cette campagne comprenait des conseils pour repérer les annonces suspectes et présentait les consignes suivantes : « 1. Prêtez attention à la provenance des offres. La plupart des sites de recherche d'emploi spécialisés ne vérifient pas l'authenticité des offres émises par des agences de recrutement. 2. N'acceptez jamais les offres de particuliers. 3. Lisez attentivement l'accord de médiation. Si vous payez une cotisation, veillez à comprendre ce que vous payez exactement et quelles sont les conditions que vous acceptez. Une fois votre accord signé, il est difficile, voire impossible, de le dénoncer. 4. Obtenez autant de détails que possible sur l'emploi proposé. 5. Si l'offre semble trop belle pour être vraie ...elle est probablement fausse ! ». Internet peut servir d'outil de protection contre les recrutements abusifs. L'on ne sait pas combien de temps cette campagne a été menée ni si elle a été déployée à plus grande échelle ou adoptée dans d'autres pays.

Deux projets sont aussi souvent cités comme des exemples de bonnes pratiques : Spotlight de Thorn et le projet Polaris, basés tous deux aux États-Unis. Spotlight est un outil basé sur le web, élaboré pour aider les enquêteurs à identifier les enfants victimes de la traite, en tirant parti d'indices en ligne. Néanmoins, il existe très peu d'informations sur ce logiciel dans le domaine public. Le projet Polaris analyse des données principalement recueillies par le biais d'une permanence téléphonique nationale contre la traite, complétées par d'autres sources d'information (non indiquées).

La détection participative des victimes est mentionnée comme une initiative citoyenne facilitée par la technologie, dont TraffickCam est souvent considéré comme un bon exemple. Elle invite les citoyens à prendre des photos de chambres d'hôtel, afin de les utiliser ensuite pour localiser des victimes. Il est cependant difficile de déterminer si ces initiatives sont efficaces. En outre, elles ne vont pas sans soulever des questions relatives à la vie privée et aux risques d'autodéfense. 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 d'autodéfense virtuels (et non virtuels).

D'une manière générale, le Groupe interinstitutions de coordination contre la traite des personnes (2019) a identifié plusieurs façons dont la technologie peut jouer un rôle positif dans la lutte contre la traite. Elles englobent : a) la contribution aux enquêtes ; b) l'amélioration des poursuites ; c) la sensibilisation ; d) la fourniture de services aux victimes ; et e) l'apport d'un nouvel éclairage sur la création et l'exploitation des réseaux de la traite. Plusieurs sources ont souligné l'importance des **« empreintes numériques »**, ce qui signifie que les contenus en ligne et les appareils connectés offrent une source d'informations exceptionnellement riche (Myria 2017 ; Mitchell et Boyd 2014). Point essentiel, il est possible de cartographier **les réseaux criminels** à l'aide des réseaux sociaux (Myria 2017 ; ainsi que le Groupe interinstitutions de coordination contre la traite des personnes (2019) et TRACE 2015 [La traite en tant qu'activité criminelle]). La collecte et l'analyse de preuves numériques peuvent **alléger la charge qui pèse sur les victimes**

lorsqu'elles doivent fournir des preuves contre des trafiquants (et des preuves nécessaires à leur défense).

4. Formation

4.1. Formation des agents des services répressifs : formations dispensées et formations requises

L'étude a d'abord examiné les formations actuellement dispensées aux agents des services répressifs sur la détection et les enquêtes dans les affaires de traite en ligne et facilitée par la technologie. Ensuite, elle a mené une « analyse des besoins » pour déterminer les nouvelles offres de formation qui permettraient d'améliorer l'efficacité de la détection et des enquêtes, et l'identification des victimes.

D'une manière générale, les niveaux et les types de formations dispensés aux services répressifs varient d'un pays à l'autre. La grande majorité des pays indiquent qu'ils dispensent des formations sur la traite. Certains exigent que tous les policiers susceptibles d'entrer en contact avec une victime présumée suivent une formation sur la traite, tandis que d'autres réservent ces formations aux unités spécialisées.

Quels sont les éléments de formation que les pays jugent essentiels en matière de traite en ligne et facilitée par les TIC ? Il est largement reconnu 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 des ordinateurs et d'autres supports numériques, et c) l'utilisation d'applications pertinentes, y compris les **Big Data Analytics** (processus d'analyse de grands ensembles de données) 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 furtives en ligne** sont également considérées comme jouant un rôle crucial.

La grande majorité des pays ont indiqué qu'ils fournissaient de tels éléments de formation, tout en mettant l'accent sur certains besoins, notamment a) la nécessité d'actualiser les formations, voire de remanier les éléments de formation actuels ; et b) la nécessité d'accroître la proportion du personnel qui reçoit une formation. Certains pays constatent avec préoccupation le caractère souvent lacunaire des formations dispensées dans le domaine des TIC et, plus précisément, dans le domaine de la traite facilitée par les TIC. Il a été suggéré d'**élaborer et de dispenser des formations intensives sur la traite facilitée par les TIC**, portant également sur des questions techniques. Une fois de plus, les services répressifs n'ont pas les mêmes compétences numériques selon les pays, mais plusieurs pays ont indiqué qu'il était nécessaire de dispenser **des formations supplémentaires sur l'utilisation des TIC** pour améliorer la détection des cas de traite.

Des pays ont également insisté sur la nécessité de fournir à la fois des formations initiales et des formations continues qui tiennent compte de l'évolution rapide des techniques d'enquête. Il convient donc de constituer des ressources supplémentaires pour préparer les modules de formation (comme des recherches sur les nouveaux développements en matière de traite facilitée par les TIC) et pour les mettre en œuvre.

Il n'est pas rare que les États parties envoient leurs agents suivre des formations organisées par des organisations internationales ou d'autres pays. L'échange d'informations et de connaissances à l'échelle internationale est sans conteste une bonne pratique. En outre, les pays qui ont des budgets et des ressources limités peuvent en tirer des avantages considérables. Malgré cela, comme certains éléments de formation conservent un aspect largement contextuel, tous les pays doivent être en capacité de développer les connaissances en interne et de dispenser des formations qui tiennent *également* compte des particularités locales du phénomène. (Aujourd'hui, seul un nombre restreint de pays n'organise aucune formation sur la traite en général ou sur la traite facilitée par les TIC, par exemple une formation OSINT, et s'appuie uniquement sur des formations assurées par des organisations externes.)

Les pays configurent différemment l'usage de leurs connaissances, et particulièrement celles portant sur les TIC. Or, il est essentiel de prévenir les goulets d'étranglement dans les opérations quotidiennes dus à une mauvaise répartition des compétences. Ainsi, il est important que les **connaissances ne soient pas cloisonnées** pour la bonne conduite des enquêtes. L'une des solutions envisagées consiste à mettre en place un système de formation bidirectionnel entre les agents spécialistes de la traite et les experts en TIC. Une autre stratégie consiste à transmettre un certain degré de compétences en TIC aux différentes unités, y compris les unités anti-traite. Dans cette perspective, le **risque d'engorgement du système** est particulièrement aigu. Sachant que les infractions facilitées par les TIC, dont la traite, risquent fort d'augmenter, il conviendra de ne pas trop solliciter les centres de cybercriminalité centralisés. Dans l'idéal, ces centres devraient uniquement être sollicités pour les affaires caractérisées par un niveau très élevé de complexité technologique – *or, cela ne semble pas être le cas des affaires habituelles de traite facilitée par les TIC*. Le meilleur moyen d'éviter les engorgements consisterait à intégrer les **cyber-connaissances générales/de base dans la formation habituelle** des enquêteurs plutôt que de les considérer comme un « domaine de spécialisation ».

Munis des éléments d'information communiqués par les États parties, nous pouvons identifier six grands domaines qui sont considérés comme critiques en matière de renforcement des capacités. Ces domaines englobent :

- 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 stockage de l'information et de communication, y compris celles supprimées par les utilisateurs, et des 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 potentielles.

4.1.1. Élaboration des futures formations et bonnes pratiques

Les informations communiquées par les États parties mentionnent un certain nombre d'initiatives concrètes qui pourraient être adoptées pour renforcer les formations dispensées dans le cadre de la lutte contre la traite en ligne et facilitée par la technologie. La liste ci-dessous présente quelques suggestions pour l'élaboration des futures modules de formation.

- Création d'études de cas et de scénarios liés à la traite à joindre à une **formation sur les « enquêtes numériques »**. Cette formation peut être divisée en deux niveaux : le niveau 1 peut être dispensé à tous les agents de terrain, tandis que le niveau 2 se compose de modules destinés à un ensemble plus réduit d'apprenants. On peut imaginer qu'au moins une partie de cette formation prendrait la forme d'un petit module destiné à favoriser les échanges d'idées et les discussions sur les pratiques.

- **Ajout d'un module TIC aux formations existantes en matière de traite**. Plusieurs pays ont fait savoir qu'ils dispensaient des formations sur la traite, mais seule une minorité d'entre eux a explicitement indiqué que leurs formations contenaient des modules TIC. Comme de plus en plus d'échanges se déroulent en ligne, il est essentiel d'intégrer des modules TIC dans les formations sur la traite « traditionnelles ». Les formations techniques peuvent inclure des modules sur les bonnes pratiques en matière d'enquêtes relatives à la traite facilitée par les TIC, ainsi que les expériences nationales et internationales.

- Déploiement d'activités communes de formation faisant intervenir plusieurs pays et fondées sur des tendances concrètes. Ainsi, en présence d'éléments indiquant que des victimes sont souvent recrutées dans le pays A puis exploitées dans le pays B, il pourrait être bénéfique d'organiser une activité commune de formation pour les agents des deux pays. Pour faire écho aux équipes communes d'enquête, ces activités pourraient être baptisées **« activités communes de formation ».**

- Recrutement d'agents non assermentés dotés de compétences techniques. Ces agents peuvent intégrer des unités spécialisées (des unités anti-traite, par exemple), améliorer leurs connaissances *en interne* dans le domaine des TIC et les diffuser au sein de l'unité/organisation.

- Organiser des sessions communes de formation qui **rassemblent des enquêteurs et des procureurs spécialisés** pour qu'ils connaissent mieux les possibilités offertes par les nouvelles méthodes d'enquête, par exemple la cyber-infiltration ou des enquêtes furtives en ligne, ainsi que la collecte de preuves électroniques (y compris la saisie d'actifs virtuels). Ces formations peuvent englober à la fois des aspects techniques et juridiques afin que les enquêteurs et les procureurs apprennent à mieux exploiter les nouvelles méthodes axées sur les TIC.

- **Partage des connaissances à l'échelle internationale**, par exemple par la participation à des formations internationales/régionales centrées sur des aspects spécifiques des enquêtes sur la traite facilitée par les TIC. (Parmi les exemples cités par les États parties figure le séminaire sur la coopération internationale sur la cybercriminalité et les preuves électroniques, organisé par le Conseil de l'Europe et le projet conjoint CyberEast de l'Union européenne, qui s'est déroulé du 7 au 9 décembre 2020.)

Les pays ont recensé un certain nombre d'initiatives concrètes comme des exemples de bonnes pratiques :

- En Autriche, le bureau opérationnel commun de lutte contre le trafic de migrants et la traite des êtres humains (une unité de l'Office de police criminelle) organise des formations et des séminaires sur la traite, l'exploitation transfrontière de la prostitution et l'identification des victimes. Des formations spécifiques ont été dispensées à la police autrichienne, aux autorités judiciaires, à l'Office fédéral de l'immigration et de l'asile (BFA), à la Cour administrative fédérale (BVwG), aux autorités financières, aux inspections du travail et aux services de conseil juridique sur la détection des cas de traite en ligne, y compris les médias sociaux. Point essentiel, ces formations n'étaient pas seulement destinées aux services répressifs, mais aussi à l'inspection du travail, aux services de conseil et aux autorités financières. En outre, les policiers spécialisés dans les TIC ont reçu des formations spécifiques centrées sur la traite aux fins d'exploitation sexuelle. À leur tour, les agents spécialisés ont dispensé des formations à leurs collègues sur la traite/l'exploitation transfrontière de la prostitution avec l'Office de police criminelle. Il s'agit là d'un bon exemple du système bidirectionnel de formation mutuelle mentionné ci-dessus – et d'un modèle qui pourrait éventuellement être reproduit ailleurs.

- En Bulgarie, en 2020, une série d'ateliers spécialisés pour les policiers, les procureurs et les juges ont porté sur les enquêtes et les poursuites relatives aux affaires de traite à l'aide de sources de données ouvertes, y compris des données en ligne.

- Dans le cadre d'accords de partenariat avec la Roumanie et la Bulgarie dans le domaine de la traite, la Norvège organisera deux activités communes de formation sur les renseignements issus de sources ouvertes (OSINT) pour les participants roumains et norvégiens. L'objectif de ces formations est de renforcer la capacité des enquêteurs norvégiens, bulgares et roumains à détecter les cas de traite facilitée par les TIC et à enquêter sur ces cas.

- En Grèce, les initiatives de formation et d'éducation à la cybercriminalité comprennent deux volets : a) un ensemble de formations universitaires destinées à aider les prochaines générations de scientifiques et de juristes à comprendre la cybercriminalité et b) un ensemble de formations plus courtes destinées à aider des agents des services répressifs et des autorités judiciaires, et des employés du secteur privé, à mieux comprendre la cybercriminalité et à mieux y répondre chaque jour.

- En Grande-Bretagne, les services répressifs suivent des procédures opérationnelles standard ou d'autres recommandations sur la surveillance proactive, la détection, les enquêtes et le démantèlement des réseaux de traite en ligne facilitée par les TIC. Celles-ci englobent : le recensement des plateformes en ligne où le risque de traite est élevé ; la conduite d'opérations d'infiltration en ligne ; l'utilisation d'indicateurs spécifiques de cas de traite potentiels sur les plateformes en ligne ; l'analyse et la gestion des signalements reçus par la voie de permanences téléphoniques qui concernent les abus sexuels et l'exploitation d'enfants sur internet ; l'utilisation d'outils technologiques spécifiques pour lutter contre la traite. En outre, les enquêteurs reçoivent des formations sur la façon d'organiser efficacement en couches les informations issues de sources ouvertes avec plusieurs formes de renseignements.

- En France, la formation de premier niveau des policiers comprend des modules sur : l'initiation aux enquêtes numériques ; l'anonymat, les *darknets* et les monnaies virtuelles ; l'analyse contextuelle des cybercrimes ; les enquêtes sur internet et les réseaux sociaux (module généralement suivi d'une spécialisation sur un thème, par exemple la fraude ou les abus sexuels sur les enfants) ; les premiers intervenants en cybercriminalité (par exemple, la préservation d'une scène de crime numérique). Des formations plus spécialisées portent sur : les enquêtes sur la cybercriminalité (collecte, traitement et analyse d'éléments d'information tirés de téléphones mobiles et d'ordinateurs ; enquêtes judiciaires relatives aux technologies numériques, y compris les problèmes juridiques, la coopération internationale et les stratégies d'enquête) ; la formation d'analystes de traces numériques ; l'obtention de données téléphoniques ; les enquêtes sous pseudonyme. Une formation d'une semaine consacrée à la traite aux fins d'exploitation par le travail est en voie d'élaboration (et devrait être lancée au premier semestre 2022). Elle englobera un module consacré à l'utilisation des outils technologiques.

4.2. Formation des procureurs et des juges

D'après certains éléments fournis, la formation des procureurs et des juges sur la traite facilitée par les TIC est plutôt inégale d'un État partie à l'autre. Plusieurs pays ont indiqué qu'actuellement, leurs 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. Un autre ensemble de pays ont indiqué qu'ils organisaient des formations sur la manière d'utiliser les instruments juridiques internationaux dans le contexte de la cybercriminalité, par exemple la Convention de Budapest et la législation interne associée, et/ou sur la manière de monter des dossiers liés à la cybercriminalité. Enfin, un groupe de pays ont intégré dans leur formation des composantes sur les cryptomonnaies et des informations sur des outils technologiques spécifiques. Dans l'idéal, tous les pays devraient **progressivement mettre en place des formations sur la traite facilitée par les TIC, sur l'utilisation d'instruments juridiques internationaux dans le contexte de la cybercriminalité**, et sur l'impact de certains outils technologiques spécifiques dans les enquêtes relatives aux affaires de traite (par exemple, les robots d'exploration ou les logiciels de décryptage).

Une minorité de pays semble intégrer des études de cas sur la traite dans les formations à la lutte contre la cybercriminalité. De la même façon, peu de pays ont indiqué qu'ils dispensaient des formations dotées de composantes sur la traite et sur les TIC.

Des pays ont mentionné dans leurs réponses au questionnaire plusieurs initiatives concrètes comme exemples de bonnes pratiques :

- En République de Moldova, pendant le premier semestre 2021, l'Institut national de la justice a dispensé une formation à 110 personnes, couvrant certains aspects propres aux enquêtes sur la traite facilitée par les TIC. La formation comprenait des sessions sur a) les particularités des enquêtes et des procès concernant des infractions en rapport avec la traite et des éléments corporels ; b) les particularités des enquêtes et des poursuites dans le domaine de la lutte contre la traite ; c) les particularités des enquêtes et des procès afférents aux affaires concernant la criminalité organisée, transfrontière et transnationale.

- En Bulgarie, le parquet de la Cour suprême a organisé des séminaires pour les enquêteurs et les procureurs sur la traite et l'utilisation des TIC dans la traite. Le représentant du parquet a indiqué que « les ateliers animés par des experts dans le domaine des TIC étaient particulièrement efficaces, car ils présentaient des exemples pratiques de l'utilisation des logiciels ainsi que les possibilités et les outils opérationnels liés à l'utilisation des applications mobiles pour découvrir des infractions graves ».
- En Suède, il y a des procureurs spécialisés dans les TIC, dont certains gèrent les affaires de traite. L'autorité chargée des poursuites organise des formations internes sur la conduite d'enquêtes relatives à la criminalité liée aux TIC (comme l'utilisation des cryptomonnaies dans les activités criminelles). De nombreux procureurs qui travaillent sur des affaires de traite ont participé à ces sessions de formation. En outre, l'École de la magistrature, qui fait partie de l'Administration judiciaire nationale et qui est responsable de la formation judiciaire des juges et des autres membres du personnel judiciaire, dispense des formations de différents niveaux sur la criminalité facilitée par les TIC.
- Les autorités lettones ont mentionné la formation internationale sur la traite et la cybercriminalité que le parquet polonais a proposée aux procureurs spécialisés dans la lutte contre le crime organisé (21-23 octobre 2019 à Cracovie).

Enfin, quelques pays ont souligné l'importance d'améliorer la formation des juges et des procureurs relative aux preuves électroniques.

ENCADRÉ | Formation des ONG

Les ONG apportent des formations et des compétences spéciales cruciales, fondées sur leur expérience quotidienne de l'assistance et du conseil aux victimes – y compris aux membres des services répressifs et aux populations et personnes vulnérables. Toutefois, elles ont aussi souligné la nécessité de recevoir une formation 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 et sur le partage d'expériences entre les pays. Ces thèmes sont particulièrement importants pour l'élaboration et la coordination des campagnes auxquelles participent à la fois les pays d'origine et les pays de destination.

Certaines ONG ont des spécialistes des questions de sécurité en ligne mais, d'une manière générale, les formations sur la technologie restent insuffisantes, y compris l'utilisation d'outils spécifiques pour identifier les victimes et leur venir en aide. D'après La Strada International, cela s'expliquerait par « le manque de ressources et de capacités », car il est « déjà difficile d'obtenir suffisamment de fonds pour les principaux programmes d'aide ».

5. Instruments juridiques

Le présent chapitre étudie les instruments juridiques internationaux pertinents pour la lutte contre la traite en ligne et facilitée par les TIC. L'annexe sur le web donne une vue d'ensemble des cadres juridiques propres à chaque pays pour l'identification et le retrait des contenus liés à la traite, ainsi que des instruments juridiques nationaux qui s'appliquent plus généralement à la lutte contre la traite.

5.1. Instruments juridiques internationaux

Les États parties ont recensé un certain nombre d'instruments juridiques présentant un intérêt pour la lutte contre la traite facilitée par les TIC. La plupart des instruments sont d'ordre général et visent à combattre la traite, indépendamment du mode opératoire des trafiquants. La Convention de Budapest du Conseil de l'Europe (Convention sur la cybercriminalité) constitue l'instrument le plus pertinent consacré à la cybercriminalité facilitée par les TIC ; il est cité par plusieurs États parties comme un outil « important ». Compte tenu de sa pertinence, l'utilisation de la Convention sur la cybercriminalité dans le contexte de la traite fait l'objet d'une section spécifique ci-dessous. Les États parties ont également mentionné les instruments suivants :

- la Convention des Nations Unies contre la criminalité transnationale organisée et son Protocole additionnel visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants (2000) ;
- la Convention européenne d'extradition du Conseil de l'Europe (STE n° 024) ;
- la Convention européenne d'entraide judiciaire en matière pénale du Conseil de l'Europe (STE n° 030) ;
- la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains (STCE n° 197) ;
- la directive 2011/36/UE du Parlement européen et du Conseil du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes ;
- l'Acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne.

Sur les questions relatives aux abus sexuels sur des enfants :

- la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote, STCE n° 201) ;
- 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 ;
- la décision du Conseil de l'Union européenne du 29 mai 2000 relative à la lutte contre la pédopornographie sur l'Internet (2000/375/JAI).

Sur l'exploitation par le travail :

- Organisation internationale du travail, convention n° 189 et recommandation n° 201 concernant le travail décent pour les travailleuses et travailleurs domestiques, 2011 ;
- Organisation internationale du travail, Protocole de 2014 relatif à la convention sur le travail forcé, 1930.

De plus, les États parties ont recensé plusieurs agences et programmes internationaux qui contribuent à améliorer la coopération juridique internationale, y compris dans le contexte de la lutte contre la traite facilitée par les TIC. Ces organismes sont les suivants :

- Interpol
  - projet IWOL (blocage des domaines relatifs à l'exploitation sexuelle d'enfants)
- Europol
  - EMPACT (traite)
  - Journées d'action conjointes
- Eurojust
- Selec (Centre de maintien de l'ordre de l'Europe du Sud-Est).

Enfin, une série d'instruments opérationnels spécifiques ressort des éléments d'information fournis par les États parties. Cette série comprend les instruments suivants :

- les demandes d'assistance juridique ;
- le mandat d'arrêt européen ;
- la décision d'enquête européenne ;
- les équipes communes d'enquête ;
- le système Prüm de l'UE (échange des données nationales relatives aux profils ADN, aux empreintes digitales et à l'immatriculation des véhicules) ;
- les dossiers passagers de l'UE ;
- l'application de réseau d'échange sécurisé d'informations (SIENA) d'Europol ;
- les agents de liaison ;
- le système de notices d'Interpol.

5.1.1. Lacunes dans le cadre existant

Globalement, les États parties ont émis un avis positif et favorable sur les instruments juridiques qui facilitent la coopération entre les pays dans la lutte contre la traite. Les conventions du Conseil de l'Europe sur a) l'entraide judiciaire en matière pénale et b) la cybercriminalité sont considérées comme des instruments figurant parmi les « plus couramment utilisés » et, dans l'ensemble, « adéquats ». Les États parties ont toutefois identifié quelques lacunes potentielles, ainsi que des domaines dans lesquels la législation

actuelle pourrait être améliorée. Le lecteur notera que ces lacunes confirment – et complètent – les difficultés relatives aux enquêtes et poursuites en matière de traite facilitée par les TIC déjà évoquées au chapitre 1, et devraient être lues en lien avec cette analyse.

Les principales lacunes relevées par les États parties concernent :

- l'absence de cadre juridique commun (harmonisé) sur lequel reposeraient les échanges entre les FSI et les autorités dans le contexte d'enquêtes spécifiques ;
- la nécessité d'accélérer la réponse des entreprises privées aux demandes de données, sachant toutefois que des délais trop serrés pourraient pénaliser les petits fournisseurs au bénéfice des gros, puisque ces derniers peuvent plus aisément financer des systèmes automatisés et/ou des services de permanence coûteux (comme l'ont souligné les autorités suisses) ;
- 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 partagées pour la conservation des données ;
- des dispositions visant à faciliter le recueil de témoignages de victimes et leur utilisation dans un autre pays. Cela réduirait les obstacles auxquels se heurtent les pays pour convaincre les victimes de témoigner aux procès pour une multitude de raisons, y compris la mobilité des victimes, la difficulté de les localiser et leur vulnérabilité persistante ;
- des dispositions relatives au cryptage (par exemple, les fournisseurs ne sont pas tenus de décrypter les matériels lorsqu'ils les remettent aux autorités) ;
- des problèmes relatifs à des mesures transnationales contre les sites web qui hébergent des éléments pouvant faciliter l'exploitation des victimes. La question est d'autant plus complexe qu'elle est étroitement liée aux différences entre les États parties en matière de traitement des activités de prostitution – et aux différents régimes adoptés dans les différents pays ;
- des dispositions introduisant un devoir de vigilance des entreprises sur l'ensemble de leur chaîne d'approvisionnement, ciblant par exemple l'utilisation des TIC pour les recrutements (comme la loi française n° 2017-399 sur le devoir de vigilance et la loi britannique de 2015 sur l'esclavage moderne introduisant un devoir de transparence dans les chaînes d'approvisionnement) ;
- l'emploi d'une terminologie qui ne permet pas toujours d'actualiser la législation au rythme des changements de mode opératoire des trafiquants ;
- des différences en ce qui concerne la transposition de l'infraction de traite (conformément au Protocole de Palerme des Nations Unies) dans les législations internes. Ces différences pourraient compromettre la coopération internationale, notamment autour de questions liées à l'absence de consentement et à la contrainte exercée sur la victime ;
- le mandat d'arrêt européen est considéré comme un outil très utile, mais les pays d'origine se trouvent souvent en dehors du cadre juridique de l'Union européenne ;
- les décisions d'enquête européenne peuvent manquer de souplesse ; ainsi, une nouvelle décision peut s'avérer nécessaire si l'enquête emprunte de nouvelles voies et les délais de réponse peuvent être trop longs ;
- les équipes communes d'enquête sont considérées comme des ressources « efficaces », mais a) elles peuvent être complexes à mettre en place et b) elles requièrent une enquête en miroir dans le ou les pays partenaires.

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

Les États parties s'accordent largement à saluer l'importance de la Convention sur la cybercriminalité, et ils sont nombreux à indiquer qu'elle constitue un « outil très utile ». Plusieurs États parties considèrent la Convention sur la cybercriminalité comme un **outil de soutien** essentiel pour la lutte contre la traite facilitée par les TIC.

D'après les éléments d'information fournis, les États parties considèrent que les dispositions relatives au **droit procédural**, présentées au chapitre II, section 2, de la Convention, sont des instruments plus efficaces pour la lutte contre la traite facilitée par les TIC que les mesures de droit pénal matériel présentées au chapitre II, section 1. En outre, et c'est un élément essentiel, le champ d'application des dispositions de droit procédural ne dépend pas de la commission d'une infraction pénale répertoriée dans la section 1 du chapitre II. Les affaires de traite facilitée par les TIC se classeront probablement sous la rubrique « infractions pénales commises au moyen d'un système informatique » ou, au moins, sous la rubrique des infractions qui requièrent la « collecte des preuves électroniques » (article 14, paragraphe 2). De la même façon, l'article 23 énonce que les principes qui sous-tendent la coopération internationale dans le cadre de la Convention s'appliquent à « des investigations [...] concernant les infractions pénales liées à des systèmes et des données informatiques » *ou* visent à « recueillir les preuves, sous forme électronique, d'une infraction pénale ». Des États parties ont souligné **l'importance de ne pas limiter l'application des mesures procédurales aux infractions explicitement énumérées** (dans le chapitre II, section 1) ; néanmoins, tous les pays ne partagent pas cette interprétation élargie du champ d'application de la Convention.

La Convention ne produit clairement ses pleins effets que lorsqu'elle ne se limite pas aux infractions explicitement répertoriées dans le chapitre II, section 1. Cette considération vaut particulièrement dans le contexte de la traite facilitée par les TIC. Comme l'ont noté les autorités finlandaises, entre autres, « les dispositions de la Convention de Budapest relatives au droit pénal matériel [qui] visent les infractions informatiques, telles que l'accès illégal, l'atteinte à l'intégrité des données, la falsification informatique et les atteintes à la propriété intellectuelle et d'autres infractions comparables, ne sont que rarement (voire jamais) pertinentes dans le contexte de la traite facilitée par les TIC ». À l'inverse, plusieurs États parties ont indiqué que, dans le cadre d'enquêtes sur la traite, ils s'étaient appuyés sur les dispositions de la Convention relatives à la conservation des données (en particulier sur les articles 16 à 21).

Plusieurs pays ont insisté sur l'utilité des dispositions énoncées au chapitre III, consacré à la coopération internationale, qui servent de base légale permettant aux pays de rassembler et de partager des preuves électroniques. Les procédures d'entraide décrites au chapitre III de la Convention (articles 29 à 34) sont jugées « utiles ». Quelques pays ont expressément indiqué qu'ils les avaient déjà utilisées. Les articles 29 et 31 ont été le plus fréquemment mentionnés ; l'article 30 n'a pas été explicitement cité dans les documents soumis, mais il peut constituer un outil utile dans le contexte de la traite facilitée par les TIC.

La disposition préconisant l'établissement d'un **réseau de points de contact** joignables vingt-quatre heures sur vingt-quatre et sept jours sur sept (article 35) est également importante, en particulier pour ce qui est de recueillir des preuves électroniques. Il est

toutefois essentiel que ces points de contact soient aisément accessibles *depuis chaque pays*. Cela se rapporte au **risque d'engorgement d'un système** : l'emplacement du point de contact dans le système de justice pénale est crucial et peut avoir des conséquences majeures. Les modalités diffèrent d'un pays à l'autre. En République de Moldova par exemple, ce point de contact se trouve au sein de la Direction des enquêtes sur la cybercriminalité ; à Malte, dans l'unité de police chargée de la lutte contre la cybercriminalité et, en Pologne, dans le Bureau de lutte contre la cybercriminalité de la Direction nationale de la police. En France, il se trouve à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et, en Lettonie, ce point de contact est situé dans le Service de la coopération internationale de la police nationale. En Bosnie-Herzégovine, les autorités ont explicitement mentionné leur « expérience très positive » d'un point de contact accessible vingt-quatre heures sur vingt-quatre, sept jours sur sept, « non situé au sein de l'unité chargée de lutter contre la cybercriminalité ». Dans le long terme, compte tenu du rôle de plus en plus central que les TIC et les preuves électroniques seront probablement amenées à jouer, ces points de contact subiront une pression croissante et seront rapidement débordés si les effectifs sont insuffisants. Des unités de soutien autonomes, dotées d'experts dans différents domaines et types d'infractions, y compris la traite facilitée par les TIC, seraient peut-être préférables aux unités de lutte contre la cybercriminalité. Toutefois, quelles que soient les modalités choisies, le pays devrait tenir compte des risques d'engorgement.

5.2.1. Pour l'avenir, une utilisation renforcée de la Convention sur la cybercriminalité dans la lutte contre la traite

Plusieurs pays ont souligné l'importance du Deuxième Protocole additionnel à la Convention. Divers documents soumis ont indiqué que l'instrument fournirait de précieux outils aux services répressifs. Il sera notamment utile pour lutter contre la traite facilitée par les TIC, en améliorant les enquêtes pénales transfrontalières et en renforçant la coopération en matière d'obtention de preuves électroniques. Les articles mis en exergue comme étant particulièrement pertinents concernent les dispositions relatives aux enquêtes communes, y compris les équipes communes d'enquête ; la divulgation rapide de données ; la demande d'entraide urgente et la divulgation directe des données relatives aux abonnés.

En outre, les États parties ont proposé de prendre les mesures suivantes pour améliorer la lutte contre la traite facilitée par les TIC à l'aide de la Convention sur la cybercriminalité :

- l'harmonisation de toutes les législations nationales avec la Convention sur la cybercriminalité pour que celle-ci produise ses pleins effets ;
- une formation élargie et améliorée sur les possibilités offertes par la Convention sur la cybercriminalité. Il ressort des documents soumis que les États parties n'utilisent pas tous pleinement les outils prévus par la Convention ;
- plus de clarté sur le champ d'application des dispositions procédurales déjà comprises dans la Convention et ses Protocoles additionnels, car un certain désaccord apparaît entre les États parties sur l'application des dispositions en vigueur aux cas de traite. Certains États parties sont d'avis que, dès lors que des preuves électroniques sont en jeu, la Convention peut produire ses pleins effets, tandis que d'autres affirment que le recours à la Convention et aux protocoles, y compris le Deuxième Protocole additionnel, exige des « cas qui s'y prêtent » (sans préciser ce qui peut faire qu'un cas « s'y prête »).

- Certains États parties ont exprimé l'avis que le Deuxième Protocole additionnel devrait comporter des dispositions qui renforcent le partage de preuves électroniques, améliorent les modalités d'entraide judiciaire, favorisent la coopération avec les fournisseurs de services internet et facilitent l'accès transfrontière aux données.
- Seule une minorité d'États parties estime que la Convention devrait être complétée ou modifiée pour inclure explicitement la traite dans son champ d'application. Les autorités bulgares ont évoqué la nécessité d'établir un « catalogue des infractions » auxquelles les outils compris dans la Convention sur la cybercriminalité et dans ses protocoles additionnels peuvent s'appliquer. Toutefois, cette opinion ne semble guère partagée au sein des États parties et une large préférence semble plutôt se dessiner en faveur d'une interprétation élargie du champ d'application de la Convention, fondée sur l'exigence plus générale de la « collecte des preuves électroniques » (voir également ci-dessus).
- Les autorités slovaques ont recommandé la mise en œuvre d'une procédure qui accélère l'entraide judiciaire en autorisant l'envoi direct d'une demande à une entité située dans une juridiction étrangère à la condition que l'autorité judiciaire de ce pays en soit informée.

ENCADRÉ | Difficultés relevées par les ONG

D'une manière générale, les ONG sont d'avis que les difficultés ne tiennent pas tant au libellé des dispositions en vigueur qu'à l'application des dispositions, qui pâtit notamment du manque de moyens des services répressifs et des organisations de soutien.

La Strada International a mentionné des **« restrictions claires » introduites par le RGPD et les règles de confidentialité des données à caractère personnel**. Elle a donné l'exemple de la « législation proposée par l'UE sur la vie privée et les communications électroniques, qui interdit aux entreprises technologiques de rechercher systématiquement les cas d'exploitation sexuelle d'enfants en ligne » (restrictions à présent provisoirement suspendues suite à l'opposition de nombreuses organisations de la société civile). La Sustainable Rescue Foundation a mis l'accent sur la « le passage manifeste des preuves physiques aux preuves numériques », qui engendre la nécessité pour « la criminalistique informatique d'obtenir des preuves recevables pour la police et le parquet » dans toutes les juridictions. D'autres difficultés relevées concernent le RGPD de l'UE ; l'actualisation de la réglementation et de la jurisprudence pour prendre en compte la cybercriminalité et internet ; l'élaboration de lois et de règles de fonctionnement adaptées aux enquêtes numériques.

La Sustainable Rescue Foundation a également proposé de voir dans la législation contre la délinquance financière une solution permettant de convertir ces renseignements en preuves recevables. Par exemple, le groupe de travail intégré sud-africain contre le blanchiment de capitaux, qui est un partenariat entre des entités privées et le secteur financier, peut demander un mandat judiciaire qui l'autorise à accéder à des informations pertinentes détenues par des institutions financières et autres. Confirmées sous serment, ces informations (c'est-à-dire l'analyse financière de données financières obtenues par la voie judiciaire) peuvent être utilisées par les services répressifs.

6. Droits humains, éthique et protection des données

6.1. Informations communiquées par les États parties

S'agissant du **traitement des données et de la protection des données**, tous les États parties ont mentionné l'adoption de lois y afférentes – souvent harmonisées avec le règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (également désigné comme le règlement général de l'Europe sur la protection des données : RGPD) et/ou la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel (STE n° 108, révisée en 2018 sous la forme de la Convention 108+). Les principes qui sous-tendent la protection des données sont similaires dans tous les États parties. Ils englobent la légalité, la limitation des finalités, la minimisation des données et la proportionnalité, l'exactitude, la limitation de la conservation, l'intégrité et la confidentialité. Les réponses au questionnaire ne permettent pas d'évaluer l'application de ces principes.

S'agissant des **droits humains** et 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 : par exemple, des mesures autorisant l'audition des témoins par visioconférence pour empêcher tout contact avec les défendeurs et, dans certains cas, la possibilité pour les victimes de faire une déposition anonyme. Les victimes peuvent être hébergées dans des **foyers** et recevoir une **assistance.**

En France, lorsqu'ils se connectent pour la première fois à la plateforme de signalement des violences sexuelles et fondées sur le genre, les utilisateurs doivent **consentir à la collecte de données à caractère personnel**. Ce consentement est renouvelé au fil de la conversation. Toutefois, il est possible d'accéder à la salle de chat sans décliner son identité, ce qui revient à autoriser les contacts anonymes.

S'agissant des **données recueillies pendant le travail de la police**, y compris pendant les enquêtes, les États parties ont souligné que les lois et les règlements précisent généralement que ces informations sont soumises à la confidentialité et ne peuvent être partagées que dans des circonstances très limitées et dans le respect de procédures et d'autorisations strictes. Les États parties ont indiqué que les règles en vertu desquelles les forces de police peuvent enregistrer des données dans des bases de données spécifiques sont normalement adaptées à la directive de l'UE sur la police. Certains pays peuvent avoir des dispositions nationales beaucoup plus strictes. Comme l'ont souligné les autorités norvégiennes, des catégories particulières de données à caractère personnel concernant, par exemple, l'orientation sexuelle, la religion et les opinions politiques, peuvent faire l'objet d'exigences supplémentaires et « ne peuvent être traitées que lorsqu'elles sont 'strictement nécessaires' à des fins bien définies ». Généralement, toutes les enquêtes et activités de renseignement, y compris celles relatives à la traite facilitée par les TIC, obéissent au même ensemble de règles et garanties. Les services répressifs doivent impérativement recevoir une formation appropriée sur les dispositions réglementaires et éthiques qui régissent le traitement des données à caractère personnel.

Les services de police doivent également trouver le **juste équilibre entre les droits et les besoins**. Ainsi, comme l'ont fait observer les autorités finlandaises, une ordonnance limitant

l'accès aux communications électroniques « ne peut être émise que s'il est établi que l'interdiction de l'accès à l'information produit de meilleurs résultats que les restrictions à la liberté de l'information et à d'autres droits fondamentaux des utilisateurs de réseaux » (section 185 de la loi relative aux services de communications électroniques 917/2014). En outre, sa « mise en œuvre pratique ne doit en aucune façon compromettre la protection de la confidentialité des communications ». Plus généralement, la section 226c de la même loi dispose que « les mesures relatives aux conditions d'utilisation des plateformes de partage de vidéos seront proportionnées à la nature du contenu concerné et prendront en compte, par exemple, les préjudices potentiels et les droits des fournisseurs de services et des utilisateurs ». Le Bureau national d'enquête finlandais a recensé des problèmes de respect de la vie privée liés à l'utilisation d'outils techniques externalisés et les a signalés au Conseil national de la police.

Des États parties ont indiqué qu'ils avaient mis en place des **protocoles tenant compte de l'âge**, c'est-à-dire des jeux de procédures et de garanties différents lorsque la victime est mineure (âgée de moins de 18 ans). Par exemple, les enfants sont généralement hébergés dans des centres de soutien particuliers ; ils sont entendus selon des techniques et dans des salles d'interrogatoire spécifiques, souvent en présence de psychologues. Dans certains pays, les procédures pénales impliquant des enfants sont exclusivement conduites par des policiers spécifiquement formés pour travailler avec des enfants et des adolescents.

6.2. Informations communiquées par des ONG

Les ONG ont souligné l'importance des règles de protection des données, de la confidentialité, d'un stockage sécurisé des données et des procédures de consentement, et la nécessité de faire connaître ces exigences au grand public.

Les éléments d'information fournis par plusieurs ONG montrent que, dans le cadre d'une procédure standard, les organisations demandent le consentement de la victime avant de partager leurs informations avec les services répressifs. Comme l'a souligné FIZ (Suisse), ce consentement couvre également le partage de détails des cartes SIM et des informations d'identification réseau. Selon la Strada International, ses membres « ne transmettent pas d'informations à la police sans le consentement de la victime, sauf en cas de situation dangereuse où il est urgent de passer à l'action ». Une question se pose lorsque les victimes ne souhaitent pas porter plainte « en raison des risques encourus, y compris le risque de faire connaître leur situation à d'autres personnes, ainsi que les risques de représailles ». La Strada International estime que c'est le cas de « nombreuses victimes de la traite ».

L'ONG « Différents et égaux » (Albanie) a mentionné l'utilisation de protocoles de sécurité dans toutes les communications avec les services répressifs, y compris le cryptage. Les protocoles internes sont élaborés en tenant compte de la nécessité de préserver la confidentialité des données à caractère personnel des victimes et leur vie privée. De la même façon, FIZ (Suisse) a indiqué qu'une bonne coopération avec les services répressifs nécessitait impérativement de protéger la confidentialité des données. Astra (Serbie) a noté que le respect de la **confidentialité des données des victimes** représentait « une part essentielle de son travail » et que le fait d'y renoncer « n'était pas et ne devait pas être une condition pour recevoir soutien et assistance ». KOK (Allemagne) a insisté sur le fait que « la protection

d'une personne est plus précieuse que la nécessité de recueillir des preuves ». Praksis (Grèce) a insisté sur le fait que, lors du partage des informations avec les services répressifs dans le respect des règles de protection des données (partage fondé sur le consentement), sa « principale préoccupation était toujours la protection immédiate et efficace d'une victime potentielle ».

Les questions de protection des données et de partage des données peuvent poser des **dilemmes moraux**. Comme l'a fait observer La Strada International, le partage des données avec les services répressifs et le dépôt de plaintes facilitent *effectivement* les enquêtes, ce qui peut sauver des victimes et les protéger dans le long terme. Toutefois, cela ne va pas sans un certain coût pour les plaignants pris individuellement, qui peuvent être exposés à des risques et à des menaces, y compris l'exclusion sociale. En outre, des questions peuvent se poser quant à l'effet à long terme de l'enregistrement d'une victime et du partage de données à caractère personnel, y compris les poursuites et les sanctions éventuelles. (Cet effet peut être encore plus important lorsque la victime est en situation irrégulière dans le pays au moment de l'enregistrement.) La Strada International et La Strada Moldova considèrent qu'il peut être « très difficile » de trouver le juste équilibre entre le besoin de confidentialité des victimes dans l'accès aux services et la nécessité de recueillir des preuves pour faciliter plus largement la lutte contre la traite. La question est encore plus sensible lorsque la victime est un enfant : d'après La Strada Moldova, les enfants ont souvent peur d'accorder leur consentement et de déposer une plainte en bonne et due forme, y compris parce qu'ils craignent la réaction de leurs parents.

Selon La Strada International, les règles de protection des données « ont complexifié le partage de données entre les ONG et d'autres acteurs concernés ». Dans le même temps, les ONG savent qu'il peut être difficile pour les « victimes de la traite ou les groupes vulnérables de connaître l'endroit où les données sont stockées, et/ou de faire en sorte qu'elles soient rectifiées, effacées, bloquées ou supprimées, et de faire respecter ce droit », en dépit des protocoles de protection des données en place.

D'autres questions se posent lorsque des informations personnelles identifiables sont recueillies avec des **techniques d'extraction de données**. La Sustainable Rescue Foundation (SRF) a mentionné deux projets distincts qui sont actuellement déployés aux Pays-Bas : RIVET (SRF) et *Lovitura 10 Elenas* (laboratoire de police néerlandais). Les deux projets sont centrés sur la traite aux fins d'exploitation sexuelle de femmes roumaines aux Pays-Bas. RIVET (SRF) utilise l'extraction des données centrée sur les victimes à partir d'entretiens menés auprès de 10 travailleuses du sexe roumaines, et explore la possibilité d'employer les technologies pour la découverte, la collecte, le nettoyage et l'analyse des données en vue d'établir la taxinomie des modes opératoires. *Lovitura 10 Elenas* suit par la voie numérique dix travailleuses du sexe roumaines pour comprendre le fonctionnement des réseaux criminels. Comme l'a souligné RSF, le problème consistait à garantir à toutes ces femmes roumaines qui collaboraient aux deux projets le respect de leur anonymat ». Les foyers sont sensibles à la protection de l'anonymat des travailleuses du sexe et la police ne peut pas partager leur base de données opérationnelle. SFR a proposé comme solution possible d'opérer des calculs multipartites basés sur des données comparées. Cette méthode consiste à anonymiser les données issues de différents sources (des ONG et de la police, par exemple)

pour qu'elles puissent être partagées et consultées par différents systèmes pour vérifier, par exemple, les doublons de noms.

La Strada International a attiré l'attention sur les risques et les dommages potentiels inhérents à la collecte de données (à grande échelle) et aux outils technologiques, mettant en garde contre un éclairage qui reste aujourd'hui centré sur « les aspects positifs et les opportunités » de ces outils. L'organisation a également préconisé d'« adopter des mesures de contrôle supplémentaires sur l'utilisation des données et leur stockage sécurisé, et [le respect] de toutes les règles de protection des données ». Les victimes, les groupes vulnérables et les ONG devraient avoir davantage de possibilités de […] rejeter les demandes de données et de restreindre la collecte de données ».

Les ONG ont tendance à mettre en place des protocoles différents selon que la victime est mineure ou majeure (**protocoles tenant compte de l'âge**).

6.3. Autres informations issues de l'analyse contextuelle

Les TIC peuvent avoir une incidence considérable sur les **droits humains**, y compris les droits à la vie privée, la liberté d'expression et la protection contre la discrimination. La littérature fait état de plusieurs problèmes dans ce sens.

Selon l'OSCE (2020), nous pouvons retenir plusieurs **questions éthiques** à examiner concernant le développement de la technologie pour lutter contre la traite. Ces questions englobent : a) la protection de la confidentialité des données à caractère personnel ; b) les protocoles de consentement signés par des victimes ; c) la formation destinée aux personnes qui traitent des données sensibles, en particulier les données des victimes ; d) le stockage de données sécurisé ; 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 des technologies de façon à ne pas bafouer les droits fondamentaux des victimes et de la population générale. Le Groupe interinstitutions de coordination contre la traite des personnes (ICAT) (2019) met aussi en exergue des questions relatives à la **confidentialité des données à caractère personnel, l'éthique, la transparence, la responsabilisation et le consentement éclairé**. Il souligne la nécessité de veiller à ce que les données soient stockées de façon sécurisée ; à ce que des protocoles de consentement soient en place ; et à ce que ceux-ci tiennent compte du genre et de l'âge. En outre, les informations publiées par les services répressifs doivent être évaluées pour ne pas mettre en danger les victimes et leurs familles.

L'ICAT (2019) et d'autres sources ont mis l'accent sur les risques inhérents au **partage de 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. Il est noté qu'un conflit éventuel pourrait surgir entre la nécessité de protéger les données à caractère personnel lorsque les victimes accèdent aux services et reçoivent un soutien d'un côté, et la nécessité de disposer d'informations/de preuves pour monter des dossiers d'enquête solides, de l'autre. Gerry *et al.* (2016) ont souligné l'importance des principes juridiques essentiels – la déontologie de l'information – pour le traitement des données à caractère personnel (qui

comprend le principe de limitation des finalités). Il est suggéré que ces principes restent également importants dans le cas de la traite, et particulièrement eu égard aux victimes.

Gerry *et al.* (2016) ont également 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 situation de traite, mais elle constitue également une **forme de surveillance qui peut s'avérer très intrusive** pour la vie privée d'une personne . Comme l'écrivent les chercheurs, elle « peut révéler une multitude d'informations relatives à la vie privée, comme l'adhésion à une religion particulière, l'établissement de relations personnelles et d'associations avec d'autres individus ainsi que les habitudes quotidiennes », exposant ainsi les groupes vulnérables au risque de discrimination et de profilage. Le suivi global de populations vulnérables entières, par exemple les groupes de migrants, peut avoir de graves répercussions sur la vie privée des personnes. Gerry *et al.* (2016) soulignent la nécessité d'établir des **mécanismes permettant de veiller à ce que la technologie de traçage ne soit pas utilisée de manière excessive ou abusive**. Ils suggèrent d'éviter les systèmes de stockage centralisé pour les données à caractère personnel des victimes ou des victimes potentielles. D'une manière plus générale, les outils technologiques destinés à lutter contre la traite doivent être **élaborés et utilisés de façon responsable et éthique**. Ces obligations doivent être prises en compte à chaque stade, de l'élaboration à l'utilisation finale. Les solutions technologiques doivent également être jaugées à l'aune de leur capacité d'intrusion dans la vie privée des gens. Certains spécialistes, notamment Milivojevic *et al.* (2020), ont mis en garde contre les conséquences néfastes pour les populations marginalisées de l'utilisation à grande échelle des techniques de reconnaissance faciale, et ont insisté plus généralement sur ce qu'ils définissent comme « l'impératif moral de 'protéger et sauver' ». Ils reconnaissent la place potentielle de la technologie dans la lutte contre la traite, mais soulignent également l'importance de placer **l'intérêt supérieur des victimes** au centre de toute action.

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 pour elles 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.

Enfin, les publications **prennent rarement en compte les dimensions de genre**. Chacun sait que ce type d'exploitation s'appuie sur des distinctions de genre, les femmes étant plus souvent exploitées pour les services sexuels, le travail domestique et les soins aux personnes, et les hommes davantage exploités dans l'agriculture, le bâtiment et d'autres travaux manuels (commerces de proximité, lavage de voitures, etc.). En outre, il semble que la sollicitation d'enfants à des fins sexuelles génère davantage de victimes féminines que masculines ; toutefois, d'autres éléments d'information laissent aussi à penser que d'autres vulnérabilités pourraient entrer en jeu en cas de sollicitation d'enfants à des fins sexuelles, par exemple le fait qu'une personne est placée en institution (information préliminaire provenant de Roumanie figurant dans Di Nicola *et al.* 2017).

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.

Monde universitaire

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)

Annexe 2 | Questionnaire aux États parties

Première partie - L'impact des technologies de l'information et de la communication (TIC) sur la traite des êtres humains

1.1 En vous basant sur les données de votre pays, veuillez donner des exemples de la manière dont les TIC sont utilisées par les auteurs des infractions dans le contexte de la traite des êtres humains aux fins d'exploitation sexuelle. (Pour chaque exemple, veuillez fournir des détails sur le modus operandi des trafiquants et le type de technologie utilisée, par exemple Internet, sites web spécifiques, médias sociaux, applications).

1.2 Veuillez donner des exemples de la manière dont les TIC sont utilisées par les auteurs des infractions dans le contexte de la traite des êtres humains aux fins d'exploitation par le travail. (Pour chaque exemple, veuillez fournir des détails sur le modus operandi des trafiquants, le type de technologie utilisé, par exemple Internet, sites web spécifiques, médias sociaux, applications *et* le secteur économique dans lequel l'exploitation a lieu).

1.3 Quelles sont les tendances émergentes dans votre pays en ce qui concerne l'utilisation des TIC dans la traite des êtres humains (nouveaux types de technologie, nouveaux modes de fonctionnement, nouveaux types d'exploitation...) ? Avez-vous identifié les nouvelles pratiques en ligne susceptibles d'accroître le risque de devenir victime de la traite (à la fois pour l'exploitation sexuelle et l'exploitation par le travail) ?

1.4 Le DarkWeb joue-t-il un rôle dans la traite dans votre pays ? Si tel est le cas, pouvez-vous nous donner quelques détails ? (Par DarkWeb, nous entendons les pages Internet qui ne sont accessibles que par des navigateurs anonymes, tels que Tor).

1.5 Dans votre pays, les TIC sont-elles utilisées pour faciliter les flux financiers dans le cadre de la traite ? Si oui, de quelles manières ? Dans quelle mesure les cryptomonnaies ou les portefeuilles cryptos sont-ils utilisés ?

1.6 Globalement, sur une échelle de 1 à 5, comment jugeriez-vous l'impact des TIC sur la traite dans votre pays ?

Cocher la case pertinente

1	2	3	4	5
☐	☐	☐	☐	☐

Très limité Très important

Deuxième partie - Principaux défis dans la détection, l'enquête et la poursuite de la traite des êtres humains facilitée par les TIC

Détection

2.1 Quelles sont les stratégies adoptées par votre pays pour détecter les cas de traite en ligne ?

2.2 Plus généralement, quels sont les défis à relever pour détecter la traite facilitée par les TIC ?

2.3 Avez-vous des exemples de bonnes pratiques pour détecter les cas de traite facilités par les TIC ?

2.4 Quel type de formation dispensez-vous aux enquêteurs et autres acteurs de la justice pénale pour identifier les cas de traite facilités par les TIC ? Quelle formation supplémentaire pourrait être proposée pour accroître l'efficacité des stratégies de détection ? Comment renforcer l'identification en ligne des victimes ?

Enquêtes

2.5 En ce qui concerne les enquêtes sur la traite des êtres humains facilitée par les TIC, comment classifieriez-vous les problèmes suivants ?

	Normalement pas un problème	Un problème mineur	Un problème majeur
Cryptage des données			
Manque de connaissances techniques des forces de l'ordre			
Volume important de données entraînant des enquêtes longues			
La rapidité de l'évolution technologique (nouvelles technologies apparaissant rapidement, etc.)			
Manque d'équipement technique			
Manque d'aide du secteur privé			
Des outils législatifs inadaptés, notamment en matière d'entraide judiciaire			

2.6 Pour chaque problème que vous considérez comme « majeur », veuillez fournir quelques exemples et décrire les mesures déjà prises, le cas échéant, pour le surmonter/atténuer. Pour chaque problème « majeur », quelles solutions pourraient être envisagées pour le surmonter ?

2.7 Y a-t-il d'autres problèmes qui ne sont pas mentionnés dans le tableau ? (Pour chaque problème supplémentaire, veuillez fournir des détails sur le problème et les solutions qui pourraient être envisagées pour le surmonter).

2.8 Quelles sont, selon vous, les meilleures stratégies pour mener des enquêtes efficaces sur la traite des êtres humains facilitée par les TIC ?

2.9 Quelle est la formation actuellement dispensée aux forces de l'ordre en ce qui concerne les enquêtes sur la traite des êtres humains facilitée par les TIC ? Quels sont les besoins de formation supplémentaires des forces de l'ordre que vous avez identifiés en ce qui concerne la traite des êtres humains facilitée par les TIC ? Y a-t-il des exemples de pratiques de formation que vous considérez comme particulièrement efficaces ?

Poursuites

2.10 En ce qui concerne les poursuites engagées dans le cadre de la traite facilitée par les TIC, comment classifieriez-vous les problèmes suivants :

	Normalement pas un problème	Un problème mineur	Un problème majeur
Attribution de la compétence			
Extradition des suspects			
Obtention de preuves d'autres pays			
Assistance du secteur privé			
Des outils législatifs inadaptés, notamment en matière d'entraide judiciaire			
Manque de formation des procureurs			

2.11 Pour chaque problème que vous considérez comme "majeur", veuillez fournir quelques exemples et décrire les mesures déjà prises, le cas échéant, pour le surmonter/atténuer. Pour chaque problème "majeur", quelles solutions pourraient être envisagées pour le surmonter ?

2.12 Y a-t-il d'autres problèmes qui ne sont pas mentionnés dans le tableau ? (Pour chaque problème supplémentaire, veuillez fournir des détails sur le problème et les solutions qui pourraient être envisagées pour le surmonter).

2.13 Quelle est la formation actuellement dispensée aux procureurs et aux juges en matière de traite facilitée par les TIC ? Quels sont les besoins de formation supplémentaires des procureurs et des juges que vous avez identifiés en ce qui concerne la traite des êtres humains facilitée par les TIC ? Y a-t-il des exemples de pratiques de formation que vous considérez comme particulièrement réussies ?

2.14 Votre pays dispose-t-il d'unités spécialisées au sein des forces de l'ordre et du pouvoir judiciaire chargées de traiter les affaires de traite des êtres humains à forte composante technologique (par exemple, preuves électroniques et en ligne) ? Dans l'affirmative, veuillez décrire leurs pratiques.

Coopération internationale

2.15 Quels sont les défis des enquêtes transnationales et de la coopération judiciaire dans le contexte de la traite des êtres humains facilitée par les TIC ? Quels sont les principaux obstacles à l'efficacité, le cas échéant, et comment les surmonter ?

2.16 Y a-t-il des exemples de bonnes pratiques pour renforcer la coopération internationale à cet égard ?

Partie 3 - Outils existants pour aider à prévenir et à combattre la traite des êtres humains facilitée par les TIC

3.1 Veuillez décrire les instruments juridiques nationaux les plus pertinents utilisés dans la lutte contre la traite des êtres humains facilitée par les TIC. Votre législation est-elle en mesure de suivre l'évolution technologique ? Si oui, comment vous adaptez-vous à ces changements ? Si non, comment peut-elle être améliorée ?

3.2 Veuillez décrire les instruments juridiques internationaux les plus pertinents utilisés dans la lutte contre la traite des êtres humains facilitée par les TIC. Pensez-vous que les instruments existants sont adéquats ? De quelle manière peuvent-ils être améliorés ?

3.3 Y a-t-il des lacunes spécifiques dans la législation nationale ou internationale actuelle qui entravent la lutte contre la traite des êtres humains facilitée par les TIC ?

3.4 Disposez-vous de mécanismes visant à empêcher l'utilisation des TIC à des fins de traite, notamment sur les médias sociaux et en relation avec les offres d'emploi en ligne ? Dans l'affirmative, veuillez décrire les pratiques en place et indiquer l'autorité publique responsable de leur mise en œuvre.

Partie 4 - Tirer parti de la technologie

4.1 Quels sont les outils technologiques, s'il en existe, disponibles actuellement dans votre pays pour identifier les victimes de la traite ? L'intelligence artificielle, la reconnaissance faciale et/ou l'analyse de données volumineuses sont-elles utilisées pour identifier les victimes ? Disposez-vous d'un ensemble d'indicateurs ("drapeaux rouges") pour identifier les victimes ?

4.2 Quelles initiatives technologiques existent dans votre pays pour aider les victimes et diffuser l'information aux communautés à risque ?

4.3 Quelles initiatives technologiques existent dans votre pays pour soutenir les enquêtes et améliorer les poursuites ?

Partie 5 - Coopération avec les entreprises privées

5.1 De quelle manière les entreprises de TIC, y compris les fournisseurs d'hébergement Internet, les médias sociaux et autres plates-formes en ligne, contribuent-elles à l'identification et au retrait du contenu Internet lié à la traite ? Comment le filtrage est-il effectué ? Le mécanisme actuel de filtrage et de suppression est-il efficace ? Si ce n'est pas le cas, comment peut-il être renforcé ? Pouvez-vous fournir quelques exemples de bonnes pratiques ?

5.2 Votre cadre juridique prévoit-il des exigences en matière de filtrage et de retrait du contenu Internet lié à la traite, et quelles sont les sanctions en cas de non-respect ? Existe-t-il un code de conduite pour les fournisseurs ? Le cadre juridique est-il efficace ? Si ce n'est pas le cas, comment peut-il être renforcé ?

5.3 Quels sont les obstacles rencontrés par votre pays dans sa collaboration avec les entreprises de TIC et les fournisseurs de services Internet, y compris les hôtes de contenu et les médias sociaux, pour lutter contre la traite des êtres humains ? Comment établir un partenariat efficace avec les entreprises de TIC ? Quels sont les outils - tant juridiques qu'opérationnels - qui pourraient contribuer à renforcer la coopération avec les entreprises du secteur des TIC ?

5.4 De quelle manière les entreprises du secteur des TIC combattent-elles les transactions financières liées à la traite ? Comment la coopération peut-elle être renforcée dans ce domaine ?

5.5 Votre pays dispose-t-il d'un organisme/régulateur indépendant chargé de surveiller le contenu de l'internet ? Dans l'affirmative, sur quelle base cette activité est-elle exercée ? Si non, de quelle manière le contrôle est-il exercé ?

Partie 6 - Convention sur la cybercriminalité (Convention de Budapest)

6.1 De quelle manière, le cas échéant, votre pays utilise-t-il les dispositions de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) pour lutter contre la traite des êtres humains ? Si ce n'est pas le cas, pourquoi ?

6.2 Existe-t-il des moyens d'utiliser davantage la Convention sur la cybercriminalité (Convention de Budapest) et ses protocoles additionnels pour lutter contre la traite des êtres humains ?

Partie 7 - Protection des droits de l'homme

7.1 Quelles sont les mesures en place pour protéger les droits humains et civils des individus, y compris les droits à la protection des données et de la vie privée, dans le cadre de la lutte contre la traite des êtres humains facilitée par les TIC ? Si des outils technologiques sont utilisés, par exemple pour passer au crible l'internet, quels protocoles sont en place pour garantir que ces outils protègent les données sensibles, notamment en matière d'orientation sexuelle, de religion et d'opinions politiques ?

7.2 Disposez-vous de protocoles tenant compte de la dimension de genre liés à l'utilisation de la technologie pour lutter contre la traite ? Avez-vous des protocoles tenant compte de l'âge ? Si oui, pouvez-vous les décrire ?

7.3 Comment la confidentialité des données est-elle protégée lors du partage d'informations entre les forces de l'ordre et des tiers, y compris des entreprises privées et des organisations caritatives ? Comment le besoin de confidentialité des victimes dans l'accès aux services est-il mis en balance avec la nécessité de recueillir des preuves et des informations pour aider à lutter contre la traite des êtres humains ?

Enfin, y a-t-il d'autres éléments non couverts par ce questionnaire que vous jugez pertinents dans le contexte de la lutte contre la traite des êtres humains facilitée par les TIC ?

Autres documents

Veuillez nous faire part de tout matériel non confidentiel pertinent, y compris des données statistiques, des communiqués de presse, des résumés d'opérations policières, qui se rapportent à la traite facilitée par les TIC, notamment :

- Utilisation des TIC dans la traite ;
- Les défis de la détection de la traite des êtres humains facilitée par les TIC, y compris l'identification des victimes ;
- Les défis liés aux enquêtes et aux poursuites en matière de traite facilitée par les TIC ;
- Coopération entre pays dans le cadre de la traite facilitée par les TIC ;
- Coopération avec les entreprises du secteur des TIC ;
- Outils de lutte contre la traite des êtres humains facilitée par les TIC (outils juridiques et/ou opérationnels) ;
- Initiatives technologiques pour lutter contre la traite des êtres humains ;
- Exemples de bonnes pratiques.

Si le rapporteur national sur la traite des êtres humains de votre pays a étudié la question de la traite des êtres humains facilitée par les TIC, veuillez nous communiquer les rapports/matériels pertinents.

Annexe 3 | Questionnaire aux ONG

Ce questionnaire vise à comprendre l'impact de la technologie sur la traite des êtres humains en s'appuyant sur des éléments tirés de votre travail sur le terrain. Par technologie, nous entendons le vaste ensemble de technologies de l'information et de la communication (TIC) qui permettent aux utilisateurs d'échanger des informations numériques. Il s'agit par exemple de l'internet, des médias sociaux en ligne et des applications pour téléphones mobiles.

Partie 1 - L'impact de la technologie sur la traite des êtres humains

1.1 Sur la base de votre travail, pouvez-vous donner des exemples de la manière dont la technologie (TIC) est utilisée par les délinquants dans le contexte de la traite des êtres humains à des fins d'exploitation sexuelle, d'exploitation du travail ou d'autres types d'exploitation ? (Pour chaque exemple, veuillez fournir des détails sur le type d'exploitation et la technologie utilisée, par exemple Internet, sites Web spécifiques, médias sociaux, applications).

1.2 Avez-vous identifié des pratiques en ligne nouvelles qui peuvent augmenter le risque d'être victime de la traite des êtres humains ?

1.3 Quels sont les défis à relever pour détecter la traite des êtres humains facilitée par la technologie ? Comment l'identification des victimes peut-elle être renforcée ?

1.4 Avez-vous des exemples de bonnes pratiques que vous avez développées pour la détection de cas de traite facilités par la technologie et l'identification des victimes ?

1.5 Coopérez-vous avec les forces de l'ordre pour lutter contre la traite facilitée par la technologie ? Quels sont les obstacles à cette coopération, et comment les surmonter ?

1.6 Quel type de formation, le cas échéant, fournissez-vous au personnel et aux bénévoles en ce qui concerne l'impact de la technologie sur la traite des êtres humains ? Quelle formation supplémentaire pourrait être utile pour accroître l'efficacité des stratégies de détection ? Disposez-vous au sein de votre organisation d'une équipe spécialisée dans la traite facilitée par la technologie ?

1.7 Y a-t-il des lacunes spécifiques dans la législation nationale ou internationale actuelle qui entravent la lutte contre la traite facilitée par la technologie ?

Partie 2 - Utiliser la technologie pour lutter contre la traite des êtres humains

2.2 Quels outils technologiques, s'il y en a, sont actuellement disponibles pour vous aider à identifier les victimes de la traite des êtres humains (par exemple, des applications spécifiques, des analyses de données massives, l'exploration du Web) ? Disposez-vous d'un ensemble d'indicateurs ("clignotants") pour identifier les victimes potentielles ? Quels types d'outils technologiques vous seraient utiles ?

2.3 Quelles sont les initiatives technologiques dont vous disposez, le cas échéant, pour aider les victimes et diffuser des informations aux communautés à risque ? Quelles initiatives technologiques serait-il utile de développer ?

2.4 Avez-vous mené une campagne de sensibilisation axée sur l'utilisation de la technologie dans la traite ? Si oui, pouvez-vous fournir des détails sur cette campagne ?

2.5 Disposez-vous de protocoles sensibles au genre liés à l'utilisation de la technologie pour lutter contre la traite des êtres humains ? Avez-vous des protocoles sensibles à l'âge ? Si oui, pourriez-vous décrire ces protocoles ?

2.6 Comment la confidentialité des données est-elle protégée lors du partage des informations avec les forces de l'ordre ? Comment le besoin de confidentialité des victimes pour accéder aux services est-il mis en balance avec la nécessité de recueillir des preuves pour contribuer à la lutte contre la traite des êtres humains ?

2.7 Sur la base des preuves recueillies dans votre travail, comment évaluez-vous l'impact de la technologie sur la traite des êtres humains sur une échelle de 1 à 5 ?

1	2	3	4	5
☐	☐	☐	☐	☐
Très limité				Très important

Enfin, y a-t-il d'autres éléments non couverts par ce questionnaire que vous considérez comme pertinents dans le contexte de la lutte contre la traite des êtres humains facilitée par les TIC ?

Autres documents

Dans la mesure du possible, veuillez nous faire part de tout matériel non confidentiel pertinent, y compris les données statistiques, les communiqués de presse et les rapports se référant à la traite facilitée par les TIC.

Annexe 4 | Questionnaire aux entreprises de TIC

This questionnaire seeks to understand the impact of technology on trafficking in human beings (THB) based on evidence from your work in the field. By technology, we mean the broad set of information and communication technologies (ICTs) that allow users to exchange digital information. Examples of these are the Internet, online social media, and Apps for mobile phones.

Part 1 - Impact of ICTs on THB

1.1 Based on evidence from your company/sector, could you please describe the ways in which ICTs are misused by offenders in the context of THB (for sexual, labour or other types of exploitation)?

1.2 Have you identified emerging online practices that may increase the risk of becoming victim of THB?

1.3 What mechanisms have been developed by your company, or your sector more generally, to prevent the misuse of ICTs for THB purposes? 1.4 Does the DarkWeb play any role in THB in your country? If it does, could you please offer some details? (by DarkWeb we mean Internet pages that are only accessible through anonymising browsers, such as Tor).

Part 2 - Cooperation with law enforcement agencies and civil society

2.1 In what ways, if any, does your company cooperate with law enforcement agencies to facilitate the identification of victims and the investigations into ICT-facilitated THB?

2.2 What are the main obstacles to cooperation with law enforcement agencies in the context of ICT-facilitated THB?

2.3 Are there examples of good practices to enhance cooperation with law enforcement agencies?

2.4 What are the legal requirements that your company is subject to in the context of combatting THB?

2.5 What tools – both legal and operational – could help strengthen cooperation with law enforcement agencies?

2.6 In what ways, if any, does your company cooperate with civil society to facilitate the identification and assistance of THB victims?

Part 3 - Leveraging on technology

3.1 What technological tools, if any, are currently available to your company to identify victims of THB? Are artificial intelligence, facial recognition and/or big data analytics used to identify victims? Do you have a set of indicators ('red flags')?

3.2 What technology-based initiatives exist in your sector to support investigations and enhance prosecution?

3.3 What measures are in place to protect human and civil rights of individuals, including data and privacy rights, when combating ICT-facilitated THB? If technological tools are used, for instance to sift through the Internet, what protocols are in place to ensure that such tools are protective of sensitive data, including on sexual orientation, religion and political views? Do you have age-sensitive protocols in place?

3.4 What type of training, if any, do you provide to staff in relation to the impact of technology on THB? What additional training could help increase the effectiveness of anti-trafficking strategies?

Finally, is there anything else not covered in this questionnaire that you consider relevant in the context of combating ICT-facilitated THB?

Further materials

If possible, please share with us any relevant non-confidential materials, including statistical data, press releases and reports, that relate to ICT-facilitated THB.

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