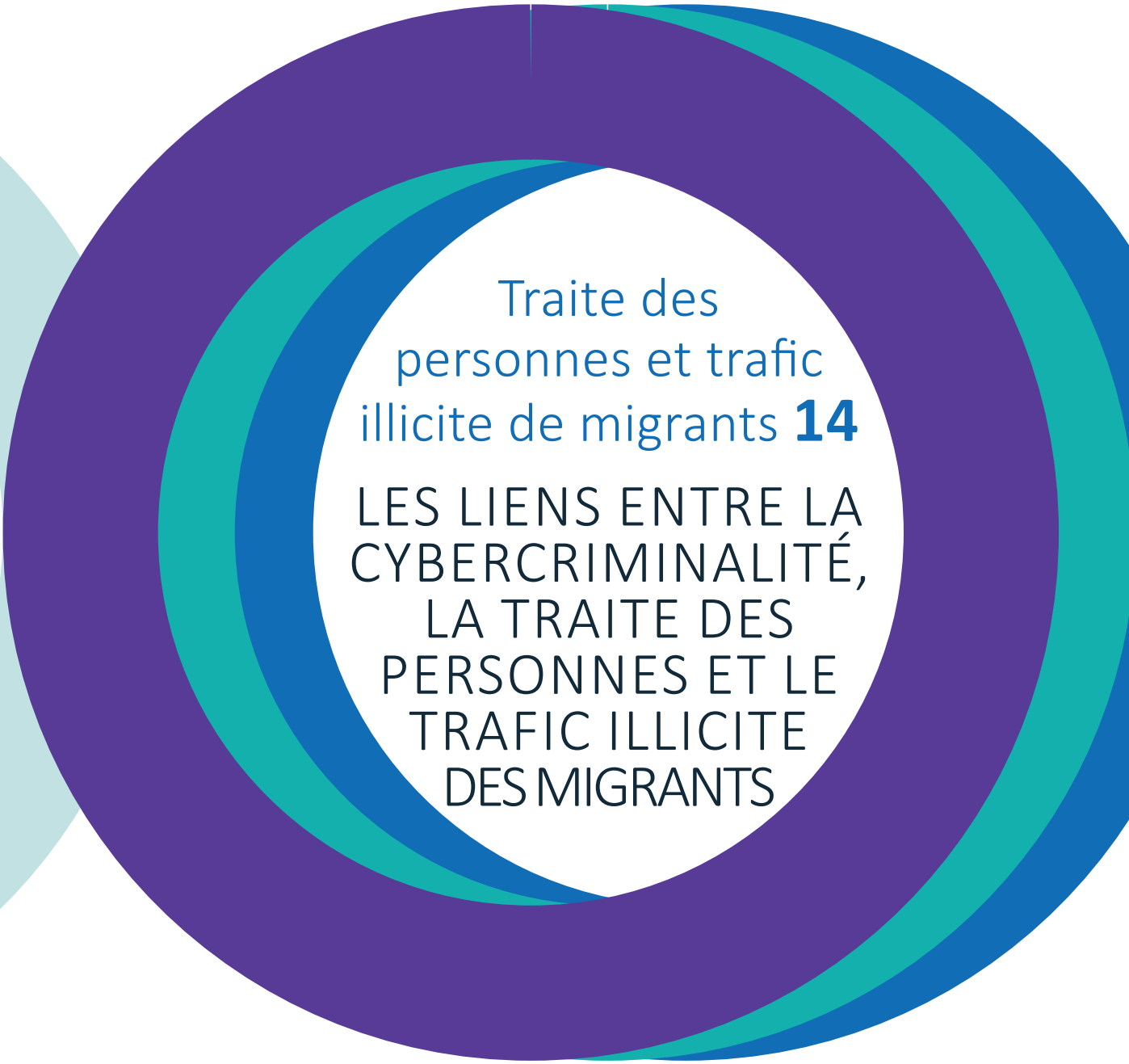
SÉRIE DE MODULES UNIVERSITAIRES



Traite des personnes et trafic illicite de migrants **14**

LES LIENS ENTRE LA CYBERCRIMINALITÉ, LA TRAITE DES PERSONNES ET LE TRAFIC ILLICITE DES MIGRANTS

ONUDC
La Déclaration de Doha:
PROMOUVOIR UNE CULTURE DE LA LÉGALITÉ

éducation pour la justice

OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME

ÉDUCATION POUR LA JUSTICE
SÉRIE DE MODULES UNIVERSITAIRES

Traite des personnes et trafic illicite de migrants

Module 14

LES LIENS ENTRE LA CYBERCRIMINALITÉ, LA TRAITE DES PERSONNES ET LE TRAFIC ILLICITE DES MIGRANTS

NATIONS UNIES
Vienne, 2019

Ce module est une ressource pour les enseignants.

Développés dans le cadre de l'initiative Education pour la justice (E4J) de l'ONUDC, une composante du Programme mondial pour la mise en œuvre de la Déclaration de Doha, ce module fait partie de la série de modules universitaires E4J sur la traite des personnes et le trafic illicite de migrants, accompagnée d'un Guide pédagogique. La gamme complète d'outils comprend des modules universitaires portant sur l'intégrité et l'éthique, la prévention du crime et la justice pénale, la lutte contre la corruption, le crime organisé, le trafic illicite d'armes à feu, la cybercriminalité, la criminalité portant sur la faune, les forêts et les pêcheries, l'anti-terrorisme ainsi que la traite des personnes et le trafic illicite de migrants.

Tous les modules universitaires E4J fournissent des suggestions pour des exercices à mettre en place en classe, des évaluations des connaissances des étudiants, des diapos et autres outils pédagogiques que les professeurs peuvent adapter aux contextes qui leurs sont propres, et intégrer dans les cours et programmes universitaires existants. Le module propose un plan de cours pour 3 heures d'enseignement, mais peut être utilisé pour des cours plus ou moins longs.

Tous les modules universitaires E4J font référence à la recherche et aux débats académiques actuels, et peuvent contenir des informations, opinions et déclarations provenant de sources variées, dont des articles de presse et le point de vue d'experts indépendants. Les liens aux sources externes furent testés au moment de la publication. Cependant, comme les sites web de tierces parties peuvent changer, merci de nous *contacter* si vous rencontrez des liens ne fonctionnant plus ou si vous êtes redirigés vers un contenu inapproprié. Merci également de nous informer si vous noter qu'une publication est liée à un site ou à une version non-officiels.

Bien que tous les efforts aient été engagés pour assurer la qualité de la traduction de ce module, merci de bien vouloir noter que la version anglaise des modules est celle qui fait foi. Ainsi, en cas de doute, merci de bien vouloir vous référer à la version anglaise correspondant.

Table des matières

Introduction

Ce module traite des liens entre la cybercriminalité, la traite des personnes et le trafic illicite de migrants. Le module reprend les articles pertinents de la Convention des Nations Unies contre la criminalité transnationale organisée (CNUCTO), du Protocole visant à prévenir, réprimer et punir la traite des personnes (Protocole contre la traite des personnes) et du Protocole contre le trafic illicite de migrants par terre, mer et air (Protocole relatif au trafic illicite de migrants). Ce module porte sur la manière dont la technologie est utilisée pour commettre des infractions dans le contexte de la traite et du trafic, en mettant l'accent sur l'utilisation d'Internet dans la cybercriminalité. Il reconnaît également que les enquêtes des États ne doivent pas porter atteinte aux droits sur les données et la vie privée, en particulier des victimes.

Les auteurs des infractions de traite des personnes et de trafic illicite de migrants peuvent exploiter Internet de différentes manières pour faciliter la criminalité organisée, telles :

- la communication entre les membres d'une organisation criminelle;
- la coordination des actions et des activités;
- la prédation sexuelle en ligne;
- le recrutement des victimes de la traite, notamment à des fins d'exploitation du travail et/ou d'exploitation sexuelle et de prélèvement d'organes;
- le recrutement de futurs migrants pour des opérations de trafic illicite de migrants;
- Commercialiser des biens et des services qui sont le produit d'activités liées à la traite, telles que des services sexuels ou des services de main-d'œuvre impliquant l'exploitation, notamment la traite d'enfants à des fins d'exploitation du travail (travail des enfants),
- contrôler les victimes par la menace ou la coercition, par exemple en menaçant de rendre public le contenu sexuel ou de le rendre accessible à des personnes particulièrement importantes pour la victime;

- le commerce de matériel pédopornographique;
- le comportement abusif retransmis en direct;
- prendre des paiements en ligne pour des services fournis par l'exploitation des victimes de la traite ou par le biais des activités de trafic illicite de migrants;
- le blanchiment des produits financiers de la traite et du trafic; et
- le choix de la juridiction, par exemple créer un contenu en ligne dans une juridiction pour la diffuser dans une autre juridiction afin de contourner la législation nationale. Ceci est particulièrement répandu dans les cas d'abus sexuel sur des enfants en direct.

La traite des personnes et le trafic illicite de migrants offrent des opportunités commerciales lucratives aux groupes criminels organisés (voir les Modules 1 et 6). Avec le développement et l'avancée des technologies modernes et le rôle sans cesse croissant d'Internet, il est essentiel que les organismes chargés de l'application de la loi, en particulier ceux spécialisés dans la cybercriminalité, conservent une compréhension à jour de la manière dont les criminels utilisent Internet pour commettre des infractions de traite et de trafic illicite de migrants et la manière dont les groupes criminels organisés utilisent des technologies de plus en plus sophistiquées pour échapper à toute détection, en particulier par le biais du dark web (internet sombre). Les crypto-monnaies représentent également un nouveau défi pour les forces de l'ordre, les criminels ayant adopté cette technologie pour blanchir les produits de la criminalité. Pour plus d'informations, consultez également la série de modules universitaires sur la cybercriminalité.

S'attaquer aux liens entre la traite des personnes, le trafic illicite de migrants et la cybercriminalité nécessite un engagement en faveur du développement et de l'adaptation de technologies modernes afin de combattre, de détecter, d'enquêter et de poursuivre en justice les auteurs des délits informatiques voir le Module 13 sur la cybercriminalité organisée de la série de modules universitaires sur la cybercriminalité). Par ailleurs, les autorités nationales doivent veiller à éviter les pratiques violant les droits des migrants et des victimes. Les étudiants doivent acquérir une compréhension des techniques d'enquête utilisées dans leur pays et des mécanismes disponibles pour la coopération internationale. Cela peut aider à identifier les lacunes dans la lutte contre la traite des personnes et le trafic illicite de migrants.

Objectifs d'apprentissage

- Identifier les liens entre la cybercriminalité, la traite des personnes et le trafic illicite de migrants.
- Évaluer les manières dont dans la pratique la traite et le trafic illicite de migrants convergent actuellement vers certains types de cybercriminalité.
- Évaluer de manière critique les cadres de lutte contre la cybercriminalité, le trafic et la traite.

- Identifier les potentielles innovations cybernétiques, les tendances et les futurs défis.

Questions clés

Utilisation de la technologie pour faciliter la traite des personnes et le trafic illicite de migrants

La traite des personnes, le trafic illicite de migrants et la cybercriminalité peuvent être plus que des délits individuels. Ce sont également des types de criminalité organisée (pour une définition de la criminalité organisée, voir le Module 1 de la série de Modules universitaires ainsi que le Module 1 sur les définitions de la criminalité organisée de la série de Modules universitaires sur la criminalité organisée). La première partie du présent module fournit un bref aperçu de la traite des personnes et du trafic illicite de migrants, la distinction entre eux et un aperçu de la cybercriminalité. Il évalue également la manière dont la technologie peut faciliter / permettre le trafic et la traite.

Deux des trois protocoles qui complètent la CNUCTO sont consacrés à la traite des personnes et au trafic illicite de migrants, établissant ainsi un lien explicite entre ces infractions pénales et le phénomène plus vaste de la criminalité organisée. La cybercriminalité n'est pas explicitement mentionnée dans la CNUCTO. Néanmoins, comme le souligne ce module 14, les activités criminelles changent et évoluent avec le temps et la CNUCTO, négociée et signée il y a plus de 15 ans, a été écrite pour durer et rendre compte de la nature en constante évolution de ce phénomène. Pour cette raison, afin de répondre aux besoins actuels et futurs en matière de justice pénale, la CNUCTO ne se limite pas à une liste d'activités menées par des groupes criminels organisés. Elle s'applique à tous les infractions graves, définis comme des infractions passibles d'une peine d'emprisonnement d'au moins quatre ans (voir le Module 1 sur les définitions de la criminalité organisé de la série de Modules universitaires sur la criminalité organisée. Ce seuil a des implications réelles et pratiques pour les États qui sont parties à la CNUCTO, dans la mesure où il contribue à invoquer les dispositions de la Convention relatives à la coopération internationale (voir le Module 11 sur la détermination de la peine et la confiscation dans le cadre de criminalité organisée de la série de Modules universitaires sur la criminalité organisée).

Les technologies n'influencent pas et ne modifient pas uniquement la traite de personnes et le trafic illicite de migrants, mais également diverses autres formes de criminalité organisée, telles que le trafic de drogue ou defaux médicaments, entre autres. De plus en plus, ces activités se produisent sur les marchés Web-souvent sur le dark web (l'internet sombre) plutôt que les marchés physiques. De même, de nouvelles structures de criminalité organisée, qui n'exigent aucun contact physique entre fournisseur et client, ni entre membres d'organisations, se sont mises en place conjointement aux technologies et à la mondialisation (voir par exemple le Module 7 sur les modèles de groupes criminels organisés de la série de Modules universitaires sur la criminalité organisée, le Module 1 sur l'Introduction à la cybercriminalité et le Module 2 sur les grands types d'infractions relevant de la cybercriminalité).

En résumé, malgré les différences examinées ci-après, la cybercriminalité, la traite des personnes et le trafic illicite de migrants ont un point commun fondamental: ils représentent une activité lucrative pour les groupes criminels organisés prêts à en tirer profit, nonobstant les effets sur les victimes de la traite ou sur les migrants qui paient et risquent leur vie pour échapper à la violence et aux conflits.

Aperçu de la traite des personnes et du trafic illicite de migrants

La traite des personnes est une combinaison de trois éléments: l'acte, les moyens et la finalité. L'article 3 du Protocole contre la traite des personnes la définit comme suit:

> " le recrutement, le transport, le transfert, l'hébergement ou l'accueil de personnes, par la menace de recours ou le recours à la force ou à d'autres formes de contrainte, par enlèvement, fraude, tromperie, abus d'autorité ou d'une situation de vulnérabilité, ou par l'offre ou l'acceptation de paiements ou d'avantages pour obtenir le consentement d'une personne ayant autorité sur une autre aux fins d'exploitation. L'exploitation comprend, au minimum, l'exploitation de la prostitution d'autrui ou d'autres formes d'exploitation sexuelle, le travail ou les services forcés, l'esclavage ou les pratiques analogues à l'esclavage, la servitude ou le prélèvement d'organes".

Il est important de noter que lorsque la victime est un enfant, l'élément de moyens n'est pas nécessaire (pour une explication plus détaillée de l'infraction de traite des personnes, voir le Module 6).

Le trafic illicite de migrants est défini à l'article 3 du Protocole relatif au trafic illicite de migrants comme " le fait d'assurer, afin d'en tirer, directement ou indirectement, un avantage financier ou un autre avantage matériel, l'entrée illégale dans un État Partie d'une personne qui n'est ni

un ressortissant ni un résident permanent de cet État " (pour une explication plus détaillée de l'infractionde trafic illicite de migrants, voir le Module 1). Contrairement à la traite des personnes, qui peut avoir lieu dans un État, le trafic illicite de migrants requiert le franchissement des frontières nationales. Les passeurs de migrants agissent dans le but d'obtenir un avantage financier ou matériel, tandis que les trafiquants agissent dans le but de les exploiter. Les différences et les similitudes entre les deux infractions sont examinées plus en détail dans le Module 11.

Aperçu de la cybercriminalité

La cybercriminalité est un terme utilisé pour décrire les infractions commises en utilisant les technologies de l'information et de la communication. Le Programme mondial de lutte contre la cybercriminalité de l'ONUDC décrit la nature complexe de la cybercriminalité, «comme une infractioncommise dans le royaume sans frontières du cyberespace, et qui est exacerbé par la participation croissante de groupes criminels organisés. Les auteurs des cyberdélits et leurs victimes se trouvent souvent dans des régions différentes et leurs effets se répercutent dans les sociétés du monde entier ». Bien qu'il n'existe pas de définition unique et universelle de la cybercriminalité (Maras, 2016), le rôle des technologies de l'information et de la communication dans la cybercriminalité est inclus dans la plupart des définitions (voir le Module 1 sur la cybercriminalité dans l'Introduction à la cybercriminalité). Il y a une distinction entre les cyberdélits en fonction du fait que les technologies de l'information et de la communication sont la cible d'un acte illicite (cyberdépendants) ou des moyens utilisés pour commettre un acte illicite (facilités par l'internet) (Europol, 2018). Les délits cyberdépendants incluent les délits contre les technologies de l'information et de la communication (accès non autorisé aux technologies de l'information et de la communication, création, diffusion et le déploiement de programmes malveillants, par exemple) (voir le Module 1 sur l'Introduction à la cybercriminalité et le Module 2 sur les grands types d'infractions relevant de la cybercriminalité pour plus d'informations). Les délits facilités par l'internet sont ceux qui peuvent être commis «hors ligne», mais qui peuvent également être facilités par les technologies de l'information et de la communication, comme la fraude en ligne, le blanchiment d'argent, l'exploitation des enfants, le trafic illicite de migrants, la traite des personnes et d'autres formes de traite (voir les cyberdélits dans le Module 2 sur les grands types d'infractions relevant de la cybercriminalité, le Module 12 sur la cybercriminalité interpersonnelle, et le Module 13 sur la cybercriminalité organisée pour plus d'informations sur ces délits).

Malheureusement, les recherches empiriques sur l'utilisation de la cyber-technologie pour commettre des infractions de traite et de trafic sont limitées, comme c'est souvent le cas pour les activités criminelles en général. Cela est dû en partie au fait que l'activité de cybercriminalité est par nature difficile à détecter et à surveiller. L'utilisation du dark web, de profils en ligne anonymes et de dispositifs jetables facilite la dissimulation des transactions et

des réseaux criminels (Stalans et Finn, 2016). Les tentatives de mesure de la cybercriminalité nécessitent un traitement substantiel et des ressources informatiques sophistiquées. Celles-ci ne sont disponibles que dans certains pays, où les forces de l'ordre chargées de faire appliquer la loi sur la cybercriminalité sont mieux équipées et où les cadres juridiques leur confèrent l'autorité légale nécessaire (voir le Module 5 concernant les enquêtes sur la cybercriminalité et le Module 6 sur les aspects pratiques des enquêtes sur la cybercriminalité et de la criminalistique numérique).

Technologie facilitant la traite des personnes

La technologie accroît la facilité avec laquelle les trafiquants peuvent localiser, recruter, contraindre et contrôler leurs victimes. La technologie et Internet, deux outils de la cybercriminalité, sont exploités à des fins sophistiquée par les trafiquants (Latonero, Wex et Dank, 2015; Latonero, 2012; Latonero, 2011). Ils peuvent utiliser ces outils à chaque étape du processus, depuis l'identification et le recrutement de victimes potentielles jusqu'au processus de coercition et de contrôle, en passant par la publicité et la vente de biens et services produits à partir de leur exploitation, jusqu'au blanchiment des profits. L'utilisation de la technologie peut s'appliquer à tous les types de trafic. Les possibilités de communication offertes aux trafiquants par la technologie au sein, et au-delà de leurs propres groupes organisés, ont été reconnues. L'un de ces exemples concernait la publication par un pédophile de conseils à l'intention de pédophiles sur des sites Web tels que Love Zone (Davies, 2016). La prolifération de l'information va au-delà de la simple communication entre les groupes criminels individuels. Cela facilite les activités illicites et les occasions d'abus. L'utilisation de la technologie peut s'appliquer à tous les types de traite.

Recrutement

Internet offre aux trafiquants l'accès à un plus grand nombre de victimes potentielles via des téléphones, des courriels, des messages instantanés, des sites Web et des applications téléphoniques (ou applications).

Les tactiques de recrutement des trafiquants incluent (sans toutefois s'y limiter):

- Profiter des vulnérabilités émotionnelles ou psychologiques
- des promesses ou menace.
- le vol de documents d'identité
- l'enlèvement

Au stade du recrutement, les trafiquants sont beaucoup plus susceptibles d'utiliser les sites Web «clearnet (web classique)» pour établir un premier contact avec les victimes. L'utilisation

de sites sur le 'clearnet' (les sites Web visibles ou de surface indexés par des moteurs de recherche, tels que Google ou Bing, (voir le Module 5 concernant les enquêtes sur la cybercriminalité et le Module 13 sur la cybercriminalité organisée pour plus d'informations) permet aux trafiquants d'entrer en contact avec un plus grand nombre d'utilisateurs d'internet, qui sont moins susceptibles d'avoir une connaissance approfondie de la technologie. Ces sites web qui facilitent le chat textuel et vidéo, l'échange d'images, les rencontres et d'autres activités interpersonnelles, offre aux trafiquants un accès sans précédent aux victimes potentielles. Les forums fournissent au trafiquant des informations qui peuvent être utilisées pour identifier les vulnérabilités des victimes et qui peuvent être exploitées pour gagner leur confiance (par exemple, la prédation sexuelle en ligne) (Latonero, 2012). Sur les sites Web et les applications de réseaux sociaux, les trafiquants peuvent effectuer des recherches sur leurs victimes et surveiller facilement leurs goûts. Cela signifie que les trafiquants sont en mesure d'adapter leur approche à chaque victime, améliorant ainsi l'efficacité de leurs manipulations. Dans le contexte de la traite à des fins d'exploitation du travail, les victimes peuvent être recrutées par le biais d'offres de travail, généralement par le biais de faux sites Web d'emplois, de publicités en ligne ou d'agences de recrutement, ainsi que par le biais de réseaux sociaux. Par exemple, en 2018, le département d'État des États-Unis, dans son rapport annuel sur la traite des personnes, révélait que «les ressortissants cubains à l'étranger [recrutaient] des victimes à Cuba par téléphone et par Internet avec de fausses offres d'emploi, des promesses de gains financiers, et des relations amoureuses" (Rapport sur la traite des USA).

Bien que difficile à mesurer avec précision, le recrutement se produit à la fois dans le contexte du trafic et de la traite. Les téléphones intelligents peuvent faciliter le recrutement dans diverses communautés. Il semble exister une corrélation entre le niveau de pénétration de la téléphonie mobile et d'Internet dans un pays et les taux de traite, en particulier lorsque la diffusion des technologies de l'information et de la communication ne s'accompagne pas d'une éducation appropriée sur les risques associés, comme en témoigne une étude au Rwanda (John 2018).

En fonction des connaissances des utilisateurs et de l'utilisation des paramètres de confidentialité et de sécurité, ainsi que de leur empreinte numérique en ligne (c.-à-d. L'étendue des données les concernant disponibles sur Internet; voir le Module 4 sur l'introduction à la criminalistique informatique pour plus d'informations), les applications, les médias sociaux et d'autres plates-formes en ligne pourraient fournir aux trafiquants l'accès à une gamme d'informations utiles pouvant être utilisées pour cibler et amadouer leurs victimes, notamment:

- les données de localisation;
- les détails d'identité et les informations sur le mode de vie, les routines et les habitudes;

- les images; et
- les contacts.

Dans les pays plus développés, l'omniprésence des smartphones parmi la population d'enfants et de jeunes adultes a pour conséquence que les applications jouent un rôle de plus en plus important dans l'exploitation des jeunes victimes. Les applications disposent souvent d'une fonction de suivi GPS, permettant aux trafiquants de localiser les cibles potentielles. Les applications sociales destinées aux adolescents encouragent les interactions imprudentes et la divulgation d'informations privées, souvent sans vérification de l'identité de l'autre partie à la communication.

Le tableau ci-dessous présente un aperçu des sites Web de connexion et de recrutement couramment utilisés pour la traite des personnes.

	SITES D'IMAGES ET DE COMMENTAIRES	SITES DE DISCUSSION-	SITES AVEC UNE CAMERA WEB	SITES DE VENTES ET DE PUBLICITES
sites couramment utilisés	Facebook, Instagram (publier des photos sur leur profil, possibilité de commenter d'autres photos, de recevoir des messages privés et de disposer d'un deuxième compte que les parents ne connaissent pas, appelé "finstagrams" ou faux instagrams.) Snapchat (la messagerie photo et l'affichage public disparaissent après avoir été ouverts, et une fonction de partage de message privé / photo / vidéo)	Tinder (application de rencontres pour discuter avec les personnes compatibles, message privé pour communiquer et se rencontrer) Blendr (application de rencontre avec un chat privé, et une localisation GPS pour localiser les autres personnes) WhatsApp (application de messagerie cryptée dans laquelle les fournisseurs de services ne conservent pas de copies des messages sur leurs serveurs et	Chat roulette (webcam avec des étrangers où, individuellement, les utilisateurs peuvent naviguer entre plusieurs étrangers et webcams, avec une boîte de discussion privée sous l'écran de la webcam) Omegle (webcam avec des étrangers où, individuellement, les utilisateurs peuvent naviguer entre plusieurs étrangers et webcams, avec une boîte de discussion privée sous l'écran de la webcam)	City guide (petites annonces, site d'accompagnement avec publicité) Skipthegames (site d'accompagnement avec des publicités individuelles de services de personnes) Bedpage (nouveau site Web après la fermeture de la page d'accueil, des annonces classées, un site d'accompagnement avec des publicités individuelles de services de personnes)

		où seules les deux personnes qui communiquent peuvent accéder à ces messages) KIK (application de messagerie qui n'est pas connectée à un numéro de téléphone, les messages ne sont pas enregistrés sur un serveur pour un accès hors du chat)		Seekingarrangement.com (sites de rencontres, sites 'Sugar Daddy' similaires aux profils de rencontres avec messagerie) Sugar-babies.com (site d'annonces de 'sugar babies' avec des profils pour que les clients/sugar daddies le parcourent et envoient des messages)
sites moins utilisés	YikYak (publication anonyme avec section de commentaire, localisation GPS permettant aux autres utilisateurs de déterminer où se trouvent les utilisateurs situés dans un certain périmètre) Whisper (Publication anonyme avec possibilité de commenter et d'utiliser les messages privés anonymement)	Yellow (application de rencontres / amis pour les jeunes avec fonction de glissement vers «tinder pour les enfants» #1 Chat Avenue (salle de discussion pour les enfants avec des étrangers dans un grand groupe, on peut envoyer des messages dans un grand groupe ou un message privé)	Monkey (webcam avec des inconnus pour un nombre limité de secondes, les jeunes doivent ajouter des utilisateurs en tant qu'amis pour une durée illimitée, destinés spécifiquement aux jeunes)	Les sites moins souvent utilisés ne peuvent pas être identifiés car le paysage est en train de changer rapidement après la législation FOSTA / SESTA: «*la scène est devenue sombre et maintenant tout est dispersé ... cela va prendre un certain temps avant qu'un autre site ne revienne, mais un autre site reviendra* "- Officier de police de l'Ohio
Processus	Les trafiquants potentiels peuvent vouloir commenter, demander à être amis et rassembler des informations qu'ils peuvent ensuite	Discuter avec un jeune, éventuellement après avoir rassemblé des informations sur un site de photos et de commentaires. La	Profiter de leurs vulnérabilités, développer la confiance et leur demander de partager davantage de photos de leur	Les amener à passer du partage à la vente de leurs photos en ligne.

	utiliser à des fins de recrutement et de prédation des jeunes.	prédation peut avoir lieu sur ces applications et sites de messagerie, en convainquant une personne d'envoyer une image compromettante et en l'utilisant ensuite pour les extorquer.	corps. Les déplacer de la page surveillée vers des pages moins surveillées.	

Source: Ryan Kunz, Meredith Baughman, Rebecca Yarnell et Celia Williamson (2018), les réseaux sociaux et les réponses à la traite à des fins d'exploitation sexuelle, Université de Toledo.

L'utilisation de plateformes de jeux en ligne est une autre tendance liée au recrutement de victimes. Les consoles de jeu avancées offrent les mêmes fonctionnalités que les ordinateurs de bureau et sont de plus en plus utilisées pour commettre des infractions (Dorn et Craiger, 2010). La forte concentration de jeunes sur les sites de jeux en ligne les rend particulièrement vulnérables à l'exploitation. (Dorn and Craiger, 2010).

Contrôle

Le contrôle peut prendre plusieurs formes, parmi lesquelles contraindre, attirer physiquement et transporter les victimes loin de chez elles, contrôler leurs finances et faire du chantage. La technologie permet aux trafiquants d'éviter les contacts physiques et en face à face avec les victimes, ce qui rend les enquêtes sur la traite des personnes encore plus difficiles. Néanmoins, le «contrôle virtuel» des victimes est un outil commun.

Le contrôle peut inclure la surveillance des victimes via un examen manuel des enregistrements téléphoniques, l'accès à des applications téléphoniques via des applications en nuage ou le déploiement de logiciels espions. Même lorsqu'une victime n'est plus sous le contrôle du trafiquant (si par exemple, elle a réussi à s'échapper), elle peut être suivie à l'aide d'applications de localisation sur son téléphone portable. Les trafiquants peuvent également envoyer des communications menaçantes aux victimes qui parviennent à s'échapper afin de conserver ou de reprendre le contrôle de leur situation.

Les trafiquants peuvent avoir recours à la fraude, aux menaces et à la tromperie pour obtenir des informations compromettantes sur la victime (telles que des images ou des vidéos) comme moyen de contrôle. Par exemple, en promettant un travail de mannequin et en demandant des photographies de nu des mannequins, suivies de menaces. Cela n'exige pas un contact face à face entre les trafiquants et les victimes; tout peut être réalisé dans l'espace virtuel.

Une autre modalité qui a moins attiré l'attention du milieu universitaire est celle où les trafiquants détournent les médias sociaux des victimes et ajoutent un contenu suggérant un consentement à l'exploitation, associé à un contenu sexuellement explicite qui porte atteinte à la réputation et à la crédibilité de la victime en tant que plaignant. Cela peut entraîner la fermeture du compte par le fournisseur de services, l'isolement et la perte de l'identité numérique, ainsi que la perte de contact avec la famille et la communauté.

Exploitation

Les êtres humains sont considérés comme une marchandise hors ligne et en ligne (Maras, 2016; Maras, 2018). À des fins de profits, les trafiquants font de la publicité pour les êtres humains et les services qu'ils peuvent fournir, et cherchent des clients qui achètent ces services. Ces trafiquants font de la publicité sur le « clearnet (le web classique) » et sur la 'dép. web (l'internet sombre)'.

La 'deep web ' ou 'dark web' fait partie du' World Wide Web (toile à l'échelle mondiale)' et n'est pas détectable par les moteurs de recherche ouverts (voir aussi le Module 5 de la cybercriminalité sur les enquêtes en matière de cybercriminalité). Le contenu est souvent protégé par un mot de passe et crypté. Il a été utilisé pour des activités illicites et entrave les enquêtes des forces de l'ordre sur la traite des personnes en rendant plus difficile l'identification des trafiquants par les enquêteurs. Le cryptage est encouragé dans les activités commerciales légitimes (telles que les services juridiques ou les archives médicales) et diverses juridictions autorisent des niveaux différents d'accès et de surveillance par l'État. Voir, par exemple, les Opérations d'infiltration en ligne d'Europol, Europol, 2017.

Cependant, les êtres humains sont principalement vendus sur des sites Web facilement accessibles car les trafiquants veulent s'assurer que leurs annonces soient accessibles au plus grand nombre de clients, dont beaucoup ne maîtrisent peut-être pas la technologie (Maras, 2018). Aux États-Unis, par exemple, des trafiquants ont utilisé des sites Web tels que *Craigslist*, *Reddit, adultsearch.com, meet4fun.com et backpage.com* pour publier des annonces sur leurs victimes. Sur ces sites et sur d'autres sites publicitaires, de rencontres et d'accompagnement, les trafiquants font de la publicité pour les services de leurs victimes sous le couvert d'un travail légitime (par exemple, un service de massage) de sorte qu'ils sont presque indiscernables des annonces légitimes qui sont publiées. Les publicités sur ces sites cachent le fait que des êtres humains sont vendus - toutefois, certains mots de code utilisés («frais»), des emojis (comme une cerise et une fleur de cerisier identifiant la victime comme vierge) et d'autres expressions dans des descriptions de publicités indiquent que les rapports sexuels sont en vente (par exemple, «expérience de petite amie») ou qu'un mineur est annoncé (par exemple, «j'ai un ami plus jeune») (Maras, 2018).

Une enquête du Sénat des États-Unis (2017) a révélé que *Backpage*, un site d'annonces classées en ligne, facilitait sciemment la traite de personnes en publiant des annonces qui offraient ouvertement des services sexuels, et les mettaient en ligne au lieu de leur refuser l'accès à la plateforme. Néanmoins, les tentatives visant à engager la responsabilité pénale de *Backpage* aux États-Unis pour ces publicités ont échoué (Maras, 2017). Cela a conduit à l'adoption de la loi autorisant les États et les victimes à lutter contre le trafic sexuel en ligne en 2018, qui responsabilise les fournisseurs de plate-forme pour le contenu publié par des tiers enfreignant la législation sur la décence. Après l'adoption de la loi, Backpage.com a été fermé et le PDG et ses co-conspirateurs ont plaidé coupables pour les infractionsde trafic de personnes et de blanchiment d'argent, entre autres chefs d'accusation (Jackman, 2018).

L'exploitation des enfants peut également se produire par le biais d'abus sexuels diffusés en direct. En 2018, 'Internet Watch Foundation' du Royaume-Uni a mené une étude de trois mois sur la diffusion en direct, qui permettait de suivre les images dans 78 domaines différents. Ceux-ci comprenaient des sites de bannières de publicité, des blogs, des forums, des réseaux de médias sociaux et des 'cyberlockers (plateforme de partage de contenus)'. L'étude a révélé que 73% des images sont apparues sur 16 forums consacrés à la publicité pour des téléchargements payants d'abus sexuels sur mineurs par le biais de webcam. Dans certains cas, les enfants étaient contraints de participer à des activités sexuelles dans le but d'obtenir des «j'aime» ou des commentaires des téléspectateurs.

En tant que conférencier, vous pouvez encourager vos étudiants à déterminer si, et de quelle manière, le développement de techniques d'enquête algorithmiques pourrait aider les forces de l'ordre sans compromettre l'utilisation légitime d'Internet.

Profits

Les crypto-monnaies (traitées en détail dans le module 13 sur la Cybercriminalité organisée) sont beaucoup plus volatiles que les monnaies physiques, car elles ne sont ni réglementées ni protégées par les banques.

Les monnaies numériques, ou «crypto-monnaies», telles que le Bitcoin, sont des monnaies virtuelles ou électroniques négociées en ligne. Ces monnaies ont créé un moyen par lequel les criminels peuvent recevoir un paiement et cacher ou déplacer les produits du crime. L'Agence de l'Union européenne pour la coopération en matière de détection et de répression (Europol) indique que les crypto-monnaies constituent le principal moyen de paiement des services criminels (Europol, 2018, p. 58).

L'utilisation des monnaies numériques par rapport aux espèces présente plusieurs avantages, qui vont au-delà de la traite des personnes et englobent d'autres activités criminelles organisées:

- Les monnaies numériques éliminent le besoin de blanchir de l'argent, ce qui est plus difficile dans la plupart des pays en raison de la réglementation de plus en plus stricte en matière de déclaration des espèces et de lutte contre le blanchiment d'argent. Des sommes d'argent considérables en espèces constituent un «drapeau rouge», attirant l'attention des autorités sur l'entreprise. La plupart des pays dotés d'une législation en matière de lutte contre le blanchiment d'argent imposent aux institutions financières des obligations en matière d'enquête et de déclaration pour les mouvements en espèces d'un montant maximal de 10 000 USD environ.
- les fonds sous forme numérique peuvent être facilement déplacés à travers les frontières internationales, contournant ainsi les limites en matière de transferts d'espèces entre les juridictions.
- l'utilisation de plusieurs «portefeuilles» numériques (un portefeuille distinct pour chaque transaction) crée des difficultés supplémentaires pour la police et les autorités de lutte contre le blanchiment d'argent pour suivre les transactions et de surveiller les tendances.
- les monnaies numériques fournissent un anonymat relatif.
- Il existe une réduction des risques qu'une contrepartie à une opération n'honore pas ses engagements par rapport à des transactions financières plus classiques. En effet, de nombreuses transactions en devise numérique sont irréversibles et ne peuvent être remboursées que par la partie destinataire (voir Bitcoin: Tout ce que vous devez savoir).
- Ainsi, des sommes d'argent élevées font des trafiquants des cibles potentielles pour d'autres criminels. Il existe des exemples de criminels volant d'importantes sommes de devises numériques dans les échanges: En juin 2018, la plateforme sud-coréenne Bithumb d'échange de crypto-monnaie a annoncé que 35 millions USD avaient été volés par des pirates informatiques (voir le rapport de CCN ici).

En ce qui concerne les crypto-monnaies, il convient de mentionner que leur utilisation implique de nouveaux acteurs dans le domaine de la traite, tels que les «crypto-négociants», les «mixeurs de crypto-monnaies», les «changeurs crypto» et les «crypto-échanges». Les responsables de l'application de la loi et les décideurs du monde entier devront s'efforcer de trouver un moyen d'ajouter ces nouveaux acteurs aux enquêtes.

La technologie dans le trafic illicite de migrants

Il existe peu de données et de recherches disponibles sur l'utilisation de la cyber-technologie pour faciliter les infractions de trafic illicite de migrants. Cependant, selon la Commission européenne (2016), «l'utilisation des médias sociaux dans le trafic illicite de migrants a connu une croissance exponentielle ces dernières années». En 2016, dix États membres de l'UE ont confirmé au Réseau européen des migrations que des plateformes de médias sociaux avaient été utilisées pour faire la publicité des services de trafic illicite de migrants, fournir des informations sur les itinéraires de migration et faciliter la communication entre les passeurs. En 2017, le HCR a publié une recherche sur l'utilisation par les médias sociaux des réfugiés et des migrants arabophones et afghans. Les chercheurs ont surveillé des centaines de pages Facebook pendant une période de dix mois, enregistrant des données qualitatives sur les échanges d'informations entre migrants, les offres des passeurs et les informations sur la falsification de documents.

De plus, certaines données suggèrent que la technologie - en particulier l'accès à Internet fourni par les smartphones - est en train de modifier la dynamique entre passeurs et migrants et la forme de la migration irrégulière, comme l'explique une étude portant sur les migrants afghans, iraniens et syriens. (Zijlistra et un van Liempt, 2017). Il est prouvé que les technologies de l'information et de la communication sont utilisées dans le trafic illicite de migrants de nombreuses façons, décrites plus en détail ci-dessous.

La publicité

Les passeurs peuvent choisir de commercialiser leurs services en ligne par le biais de sites de médias sociaux et de publicités «bouche à oreille» entre migrants et passeurs utilisant des smartphones. Selon Brunswasser (2015), les passeurs annoncent leurs services sur Facebook comme «une agence de voyage légitime». L'étude 2017 du HCR montre qu'il existe des centaines de pages Facebook, proposant des services légaux et illégaux avec des numéros de contact complets. Bien que difficile à mesurer avec précision, le recrutement se produit clairement en ligne dans le contexte du trafic illicite de migrants. La technologie peut accroître la portée des services des passeurs, ce qui facilite le recrutement dans un plus grand nombre de communautés sans que la présence physique des passeurs soit nécessaire. Comme pour la traite, il existe probablement une corrélation entre le niveau de pénétration du téléphone mobile et d'Internet dans un pays et le taux de trafic illicite de migrants.

La communication

Les passeurs utilisent les smartphones, les courriels, les plateformes de médias sociaux et les applications pour communiquer avec les migrants, et les migrants les utilisent pour

communiquer avec les passeurs, les autres migrants, les familles et d'autres contacts. La technologie permet aux passeurs de communiquer grâce à la technologie, ce qui leur permet de faciliter le processus de trafic, de faire face plus rapidement aux difficultés et de diriger les migrants de loin. Il est probable que les technologies de la communication réduisent l'obligation des passeurs d'accompagner physiquement les migrants à travers les frontières.
Il est important de noter que la communication électronique permet également aux migrants faisant l'objet du trafic (et à ceux qui l'envisagent) de discuter et d'examiner les services des passeurs de migrants. Les sites de médias sociaux en ligne donnent aux migrants un moyen d'en savoir plus sur les expériences d'autres personnes avec des passeurs particuliers, y compris des commentaires sur leur fiabilité et leur loyauté. Les migrants peuvent également utiliser Internet pour vérifier les informations obtenues auprès des passeurs grâce à des recherches en ligne. Cela pourrait concerner les prix (tarif plus élevé que le prix demandé habituel), la sécurité de l'itinéraire à suivre, l'opportunité d'un État de destination et rigueur de ses contrôles aux frontières (le projet de trafic est-il susceptible de réussir?).

Le financement

Les paiements aux passeurs se font principalement en espèces, avec des tiers garants (membres de la famille) ou des versements sur des systèmes de paiement en ligne (Initiative mondiale contre la criminalité transnationale organisée, 2017). L'utilisation de «hawala», un système informel de transfert de valeur existant en dehors des systèmes bancaires traditionnels, en est un exemple. Ce système fait appel à des courtiers tiers pour effectuer des virements sans trace écrite reliant le passeur et le migrant (Legorano et Parkinson, 2015). Le tableau suivant indique les moyens de paiement les plus souvent utilisés, selon le rapport conjoint d'Europol et d'INTERPOL sur les réseaux de trafic illicite de migrants en 2016. Les cryptomonnaies peuvent accroître la facilité avec laquelle les passeurs et les groupes criminels organisés dans lesquels ils opèrent, peuvent recevoir, cacher et déplacer de l'argent. Ces monnaies peuvent contribuer au blanchiment d'argent et au transfert de fonds d'un pays à l'autre, et permettre aux passeurs d'éviter les enquêtes et les appréhensions des autorités en garantissant l'anonymat et en réduisant le besoin de transporter de grandes quantités d'argent.

La logistique

Les passeurs utilisent les technologies de l'information et de la communication pour fournir des informations et/ou communiquer sur les services logistiques, tels que les types de services offerts, les horaires, les dates et les prix des services, les options et les plans de voyage et les articles, les fournitures et les équipements nécessaires. Elles peuvent également être utilisées pour mener des recherches sur les itinéraires de migration. Par exemple, pour rechercher les frontières dont la sécurité est moins stricte et les moments de la journée où l'arrivée attirerait

moins l'attention. Des recherches sont également menées pour savoir à quoi s'attendre pendant la migration et les mesures à prendre dans certaines situations (par exemple que faire en cas d'être appréhendé par les forces de l'ordre) (Zijlstra et van Liempt,2017). Trois tendances semblent émerger du changement apporté par la technologie:

1. Moins de dépendance vis à vis des passeurs - de nombreux migrants continuent à dépendre des passeurs pour obtenir de faux documents et une assistance pour franchir les frontières, en raison du degré d'isolement culturel des migrants, des barrières linguistiques et des difficultés à se soustraire à l'application de la loi. Cependant, grâce à la technologie, un nombre croissant de migrants est autonome tout au long du processus de migration. Cela donne aux migrants une plus grande autonomie et réduit leur vulnérabilité à l'exploitation. Brunwasser (2015) signale l'existence de groupes de Facebook en arabe, tels que «migrer vers l'Europe sans passeur» et «migrer vers l'UE». La technologie peut également aider les migrants faisant l'objet du trafic à tenir leur famille au courant de leurs déplacements et à obtenir des conseils et des informations sur leur destination. De plus, les applications de traduction, telles que Google Translate, peuvent aider à éliminer les barrières linguistiques et à aider les migrants à communiquer avec les autres migrants et les responsables de l'application de la loi. La cartographie électronique et les systèmes GPS ont permis de réduire la dépendance des migrants vis-à-vis de ceux qui leurs faisaient franchir illicitement les frontières, en leur permettant de naviguer plus facilement et de manière plus autonome grâce à la technologie mobile, aux services et aux applications pour smartphone (par exemple, Google Maps qui cartographie les itinéraires et fournit les directions depuis le point d'origine jusqu'à la destination envisagée).
2. Fossé numérique / de classe - les inégalités entre migrants peuvent maintenant être mesurées en termes de fracture numérique. Ceux qui possèdent à la fois les moyens d'acquérir un smartphone et la culture numérique pour l'utiliser de manière efficace ont un avantage notable (voir Amran et Imran, 2015).
3. Une démarcation estompée entre le passeur et le migrant - il semble y avoir une augmentation du nombre de migrants en situation irrégulière qui aident des passeurs plus professionnels et / ou leurs pairs pour subventionner leur propre voyage.

Utilisation de la technologie pour prévenir et combattre la traite des personnes et le trafic illicite de migrants

Les progrès technologiques, en particulier les technologies de communication de l'information rendues possibles par les smartphones et Internet, façonnent et facilitent les infractions de trafic et de traite et créent de nouveaux obstacles pour leur détection et les enquêtes. Cette partie du Module examinera la manière dont les technologies peuvent être utilisées pour prévenir, détecter, intervenir et finalement contrecarrer ces crimes. Elle examinera également un autre aspect crucial de cette utilisation de la technologie; c'est à ire la manière dont les États, les organismes chargés de l'application de la loi et les organismes privés collectent, conservent et utilisent les informations recueillies au cours de ces processus d'enquête. Ces actions soulèvent toutes des préoccupations potentielles concernant la confidentialité des données personnelles (pour plus d'informations, consultez le Module 10 de la cybercriminalité sur la protection de la vie privée et des données).

Il y a un intérêt croissant pour trouver des moyens «d'exploiter la technologie» pour perturber les réseaux de traite de personnes et de trafic illicite de migrants. Par exemple, les autorités répressives utilisent la technologie pour identifier les trafiquants et les passeurs et l'exploration de données pour identifier les transactions suspectes (Latonero, 2012, p. V; Commission européenne, 2016). La technologie aux frontières est de plus en plus utilisée. Cela influence la facilité de circulation mais offre également une opportunité de lutter contre le trafic illicite de migrants, à condition que les forces frontalières aient une formation suffisante en la matière et puissent identifier les indicateurs de trafic. La technologie peut également faciliter l'enregistrement, le stockage, l'analyse et l'échange d'informations relatives aux victimes identifiées de la traite. En outre, des éléments de preuve indiquant que des suspects ont apposé de faux identifiants d'appels ou des logiciels espions peuvent être utilisés pour réfuter les allégations d'association innocente et prouver une intention criminelle. Les réservations de vol et les registres bancaires des retraits d'espèces à l'étranger aident à prouver le trafic transnational.

Parmi les autres sources de preuves numériques utiles et souvent incriminantes figurent :

- les données téléphoniques - la dépendance des trafiquants et des passeurs modernes envers leur smartphone signifie que de nombreux éléments de preuve sont disponibles sur ces appareils s'ils sont accessibles;
- les publications sur les médias sociaux - des images, des vidéos, des contacts, des associés, des lieux et d'autres informations peuvent être glanées à partir de comptes de médias sociaux; et

- les empreintes numériques, y compris l'historique du navigateur sur les ordinateurs personnels et les adresses IP.

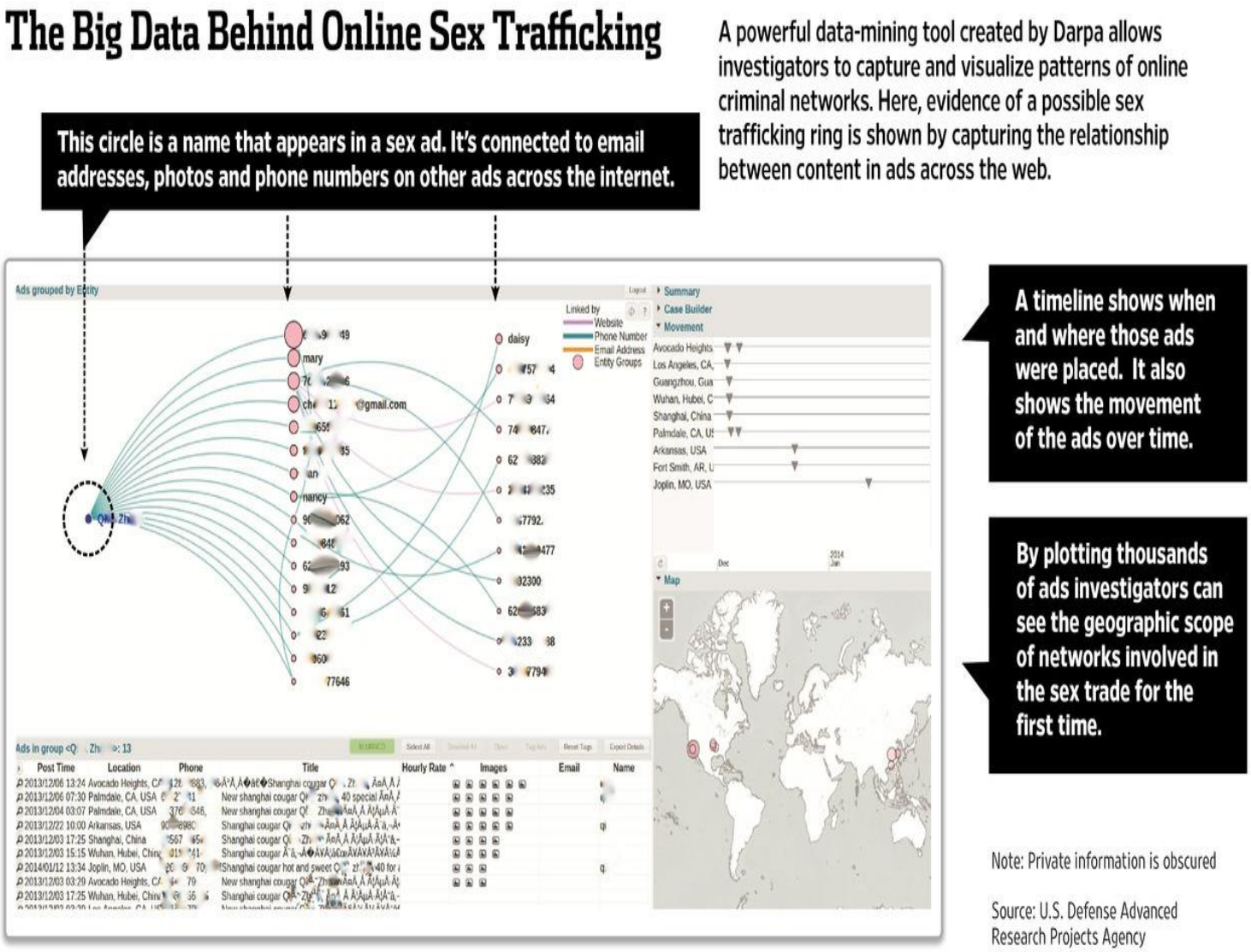
L'utilisation de ces preuves numériques permet de construire des cas plus solides. Cela peut également appuyer les récits des victimes et des témoins lorsqu'ils déposent. En l'absence de victimes ou de témoins pour témoigner, les procureurs et les autorités peuvent utiliser uniquement les éléments de preuve numériques pour porter les affaires devant les tribunaux et obtenir des condamnations (voir le Module 4 sur l'introduction à la criminalistique informatique, le Module 5 concernant les enquêtes sur la cybercriminalité et le Module 6 sur les aspects pratiques des enquêtes sur la cybercriminalité et de la criminalistique numérique de la série de Modules universitaires sur la cybercriminalité).

Les preuves numériques peuvent provenir des pièces à conviction saisies sur des migrants ou des victimes de la traite, ou de suspects. Les enquêtes des forces de l'ordre sont menées dans le but d'identifier, d'enquêter et d'obtenir des preuves qui aboutiront finalement à des poursuites contre les trafiquants et à la protection des victimes. En ce qui concerne la criminalité transnationale organisée, la coopération est nécessaire. Par exemple, l'opération Cross Country du FBI des USA, qui a été menée pour la 11ième fois en 2017 en coopération avec d'autres pays (Canada, Royaume-Uni, Philippines, Thaïlande et Cambodge), a effectué hors ligne les activités de l'opération (par exemple dans des bars, des casinos et des relais routiers) et en ligne, et cela a entraîné l'arrestation de 120 trafiquants (FBI, 2017).

Les concepts d'enquête et de dissuasion convergent lorsqu'il s'agit de la présence virtuelle des forces de l'ordre, souvent sous la forme de profils « catfish (faux profils) » créés pour piéger les criminels organisés opérant en ligne. L'utilisation de faux profils peut permettre de rassembler des preuves numériques dans le cadre d'une enquête. Ils peuvent également avoir un effet dissuasif: si un trafiquant potentiel craint d'être en contact avec un policier, il est moins susceptible de prendre ce risque. Cependant, il faut tenir compte des juridictions qui interdisent les opérations de provocation ou d'infiltration.

Le principal obstacle aux enquêtes est le temps requis pour les mener et l'impossibilité de se livrer à des activités criminelles, à l'exception des opérations «d'infiltration» autorisées. La technologie peut être mise à profit pour réduire le temps requis pour identifier les auteurs des infractions et les victimes et pour supprimer de manière proactive le contenu relatif à la traite et au trafic. Par exemple, les 'chatbots (agents conversationnels)' peuvent être utilisés pour engager des conversations simultanées avec des milliers d'auteurs d'abus en ligne. Il convient de noter que l'approbation éthique pour certaines techniques de recherche peut être difficile à obtenir, ce qui peut affecter les progrès des enquêtes, en particulier lorsque les juridictions n'ont pas la volonté politique de coopérer.

L'utilisation de robots d'exploration de sites Web et d'outils d'exploration de données constitue un autre moyen de surmonter les obstacles aux enquêtes. Dans le cadre de son programme Memex, la DARPA (Agence pour les projets de recherche avancée de défense) a développé des outils permettant d'identifier les trafiquants de personnes et les victimes de la traite. Dans le cadre de Memex, des robots d'exploration de sites Web et des outils d'exploration de données ont été développés pour répertorier les publicités en ligne (sur le Web visible et profond) et créer des bases de données contenant ces informations. En particulier, ces outils (tels que DIG et TellFinder) combinent des publicités, téléchargent du contenu, identifient des liens entre des éléments téléchargés, ajoutent des bases de données, et permettent des requêtes de base de données (Karaman, Chen et Chang, ND; Pellerin, 2017). Les informations contenues dans ces bases de données sont exploitées pour identifier les tendances et les modèles, lesquels sont cartographiés dans des formats visuels. Cette cartographie permet d'identifier les échéances et les mouvements des victimes (voir l' image ci-dessous).



Source: site web DeepDive

Les photos

Les photos prises avec un téléphone portable ou un appareil photo numérique contiennent des métadonnées (voir également le Module 4 de la cybercriminalité: sur l'introduction à la criminalistique informatique). Ces métadonnées, appelées données Exif, contiennent des informations sur l'appareil photo utilisé ainsi que sur l'image elle-même, telles que ses dimensions et son format. Les données Exif peuvent faire correspondre des images à des périphériques en la possession d'un suspect. De même, les données Exif peuvent aider à fournir les dates auxquelles les images ont été capturées et les crimes commis. Les photos et la géolocalisation peuvent également être utilisés pour déterminer le lieu où un événement important s'est produit.

Données GPS

Les données GPS peuvent être utilisées pour suivre l'emplacement et l'historique des appareils. En 2011, dans un cas aux États-Unis, un homme a plaidé coupable pour des infractions de traite après avoir publié les services commerciaux d'un mineur sur *Backpage.* Les enquêteurs ont pu utiliser les données GPS de la voiture d'un trafiquant pour déterminer l'emplacement de plusieurs clients (Latonero, 2011). Un autre exemple d'utilisation de la technologie par satellite est le projet d'observatoire géospatial de l'esclavage entrepris par l'Université de Nottingham, qui utilise des renseignements géospatiaux pour détecter des cas d'esclavage. En 2016, le Telegraph a rapporté que cette recherche avait été utilisée pour découvrir cinq camps de travail inconnus au Bangladesh soupçonnés d'utiliser des enfants esclaves

Le secteur privé

Toute action visant à exploiter la technologie pour lutter à la fois contre le trafic illicite de migrants et la traite des personnes implique inévitablement une coopération entre le secteur privé - développement de logiciels et partage de données et d'informations - et les organes d'application de la loi et les services chargés des poursuites. En 2018, l'Initiative mondiale contre la criminalité transnationale a annoncé l'initiative Tech contre la traite (TAT), une collaboration entre des entreprises technologiques mondiales, des organisations de la société civile et les Nations Unies afin de soutenir l'éradication du travail forcé et de la traite des personnes en utilisant la technologie.

Parmi les contributions du secteur privé, il faut citer Microsoft, qui a organisé des forums universitaires dans ce domaine et mis au point un outil (PhotoDNA) en 2009 permettant d'analyser des images d'abus sexuels sur enfants, qui peut être utilisé (gratuitement) par les forces de l'ordre et les entreprises pour localiser et supprimer les images d'abus sexuels sur enfants. D'autres sociétés ont également mis au point un logiciel permettant d'identifier les enfants victimes de la traite grâce à une analyse des liens. Par exemple, Thorn's Spotlight est

utilisé pour identifier les publicités en ligne concernant les relations sexuelles avec des enfants mineurs en analysant de grandes quantités de données extraites de publicités en ligne afin d'identifier des modèles et des connexions (Thorn, non daté). Cet outil a été utilisé dans des opérations d'infiltration des forces de l'ordre, telles que l'opération Cross Country (Thorn, non datée).

Les banques peuvent également jouer un rôle dans le processus de détection. L'un des instruments par le biais duquel les institutions financières participent à la lutte contre la traite est l'initiative du Liechtenstein, qui encourage l'innovation dans le secteur financier pour lutter contre la criminalité. Toutefois une analyse complète de cette initiative, les modèles bancaires et les exigences en matière de rapports ne relèvent pas du cadre de ce module (voir l'article de l'Economist sur les logiciels de détection de la traite des personnes).

Les médias sociaux

Les organisations de lutte contre la traite utilisent des plateformes de médias sociaux, telles que Facebook et Twitter, pour communiquer des renseignements sur la traite des personnes et le trafic illicite de migrants, publier des informations et des liens sur des affaires de traite et de trafic et des actualités pertinentes, communiquer avec d'autres organisations ayant des objectifs similaires, et afficher les opportunités d'implication de la société civile dans les campagnes de lutte contre la traite et le trafic illicite de migrants(Latonero, 2012)., (Latonero, 2012).

Ces organisations utilisent également des plateformes de partage de vidéos (telles que YouTube) pour éduquer le public sur la traite des personnes et le trafic illicite de migrants. Par exemple, le projet Polaris - une ONG qui s'emploie à combattre et à prévenir la traite - utilise des plateformes de médias sociaux et de partage de vidéos pour sensibiliser le public, et a également lancé un service de messagerie texte (BeFree), disponible 24h / 24 et 7j / 7, où les victimes et les survivants de la traite de personnes peuvent recevoir une assistance.

Des mécanismes de signalement des témoins et des victimes par téléphone ou par Internet ont été mis en place. L'initiative conjointe de l'autorité régulatrice du marché du travail de Bahreïn et de la société de télécommunications VIVA, qui fournit des cartes SIM aux travailleurs expatriés qui arrivent dans le pays, permet de signaler les cas d'abus.

Crowdsourcing

Le crowdsourcing, c'est-à-dire «le fait d'accepter un travail traditionnellement exercé par un agent désigné (généralement un employé) et de le sous-traiter à un vaste groupe de personnes généralement indéterminé sous la forme d'un appel ouvert» (Howe, 2006), a été appliqué aux initiatives de lutte contre la traite (Latonero, 2012, p. 20-21). Une application particulièrement innovante, TraffickCam, invite le public à télécharger des photos des chambres d'hôtel dans lesquelles ils séjournent, afin de pouvoir créer une base de données participative avec les images et les caractéristiques des chambres pour localiser l'endroit où les victimes de la traite sont détenues et/ou maltraitées. Cette identification est rendue possible en examinant les environs des photos ou des vidéos postées représentant la victime.

C'est un domaine qui dépendra des niveaux de sensibilisation à la traite dans une juridiction donnée. En tant que conférencier, vous pouvez demander à vos étudiants de discuter des niveaux de sensibilisation actuels dans leur pays et de la manière dont cette sensibilisation pourrait être améliorée, si nécessaire.

Les préoccupations en matière de protection des données et de la vie privée

L'exploitation de la technologie pour lutter contre les infractions de traite et de trafic illicite de migrants doit être poursuivie avec vigueur, sans toutefois porter atteinte aux droits fondamentaux des victimes et du public (Gerry et al, 2016). Les considérations relatives à la protection de la vie privée et des données sont incluses dans le référentiel de l'ONUDC (2008, outil 9.15) sur «l'utilisation d'instruments normalisés de collecte de données» ou dans le projet interinstitutions des Nations Unies sur la traite des personnes (2008) le «Guide sur l'éthique et les droits de l'homme dans la lutte contre la traite». En raison de la nature mondiale de la traite des personnes et du trafic illicite de migrants, il convient de prêter attention aux mêmes préoccupations dans les différents lieux où les concepts de protection de la vie privée et des données sont moins développés (voir le Module 10 sur la protection de la vie privée et des données).

Parmi les exemples de technologies pouvant être utilisées pour lutter contre la traite et le trafic illicite de migrants, mais pouvant également créer des problèmes en matière de protection de la vie privée et des données, il faut citer (Gerry et al, 2016):

Le suivi de localisation:

- Comme mentionné précédemment, des États tels que Bahreïn ont distribué des cartes SIM aux travailleurs à leur arrivée dans le pays afin de leur permettre d'utiliser la

messagerie de texte pour contacter immédiatement l'autorité régulatrice en cas de problème avec leur employeur. De telles approches permettent aux États de localiser les migrants lorsqu'ils envoient des messages ou notifient les risques, mais peuvent également compromettre la protection de la vie privée et des données des personne en révélant leur affiliation politique ou religieuse ou leurs relations personnelles et en créant un risque de transfert de données à des fins commerciales.

Collecte de données:

- Les données peuvent aider à détecter, à enquêter et à poursuivre le trafic et la traite, et à prédire l'évolution de la criminalité et à anticiper les activités aux fins de la prévention de la criminalité.
- Les données collectées peuvent améliorer la coopération en matière d'enquête aux niveaux national et transnational, favorisant ainsi le partage de données et la collaboration entre les organismes chargés de l'application de la loi.
- La collecte de données personnelles sur les personnes victimes du trafic et de la traite peut aller au-delà de ce qui est spécifiquement requis pour une enquête pénale ou une entraide transnationale, en compromettant la vie privée des personnes victimes de la traite ou du trafic, y compris leurs données personnelles.
- L'accès aux données crée des risques pour la sécurité et compromet le rétablissement des victimes, y compris dans le contexte du profilage.
- La possession des données peut créer une stigmatisation affectant l'intégration dans un environnement sociétal et l'accès au marché du travail.
- La dépersonnalisation et l'anonymisation et le fait d'éviter l'enregistrement de données excessives ou le stockage centralisé peuvent représenter un fardeau financier, ce qui peut affecter à la fois les enquêtes et la protection.

Les drones:

- Leur utilisation inclut la non-détectabilité par les personnes surveillées, la flexibilité dans l'affectation des tâches et la capacité à faciliter la gestion des frontières et à couvrir les zones éloignées ou reculées.
- Une surveillance optimisée peut soulever de graves problèmes de confidentialité pour les individus surveillés. Toutes les juridictions ne reconnaissent pas la protection de la vie privée dans les espaces publics et, lorsqu'elles sont utilisées auxfrontières ou dans des zones urbaines, elles peuvent capturer et enregistrer des images d'individus légitimes, lesquels peuvent aussi être l'objet de contrôle potentiels.

Il convient également de noter que la technologie utilisée pour faciliter le trafic et la traite peut créer des problèmes de confidentialité et de données (Gerry et al, 2016). Par exemple, les trafiquants et les passeurs peuvent suivre et surveiller les activités des victimes /des migrants par interrogation directe ou à distance de leur téléphone. Cela peut également donner accès à une base de données de preuves. Dans le même temps, la sécurité d'une personne peut être

gravement compromise. Le retrait de la technologie peut conduire à une perte de pouvoir, un transfert de pouvoir et provoquer l'isolement.

Une compréhension des principes directeurs de l'OCDE sur la protection de la vie privée et les flux transfrontaliers de données à caractère personnel facilitera l'apprentissage dans ce contexte.

Tendances émergentes

Un effort a été fait pour que ce module suive le rythme des changements technologiques, tout en reconnaissant la nécessité de comprendre les tendances en matière de technologie qui peuvent faciliter la criminalité organisée. En tant que conférencier, vous pouvez améliorer l'apprentissage de vos étudiants en leur demandant de rechercher et de réfléchir aux tendances émergentes, dont certaines peuvent être représentées, de manière générale, dans le tableau ci-dessous:

Apprentissage automatique	L'intelligence artificielle (IA) et l'apprentissage automatique peuvent être utilisés pour identifier des cibles potentielles, modifier le comportement humain et prévoir les incidences financières, en opérant potentiellement de manière autonome et en évitant toute responsabilité pénale directe.
Applications numériques	L'environnement de travail des personnes exploitées peut être dirigé par un logiciel d'assistant personnel virtuel. Il peut également être utilisé pour renforcer les activités d'exploitation et l'efficacité des entreprises, ainsi que pour améliorer les outils de sécurité, reflétant les activités commerciales légitimes et empêchant l'identification d'activités criminelles.
Outils technologiques, capteurs et jumeaux numériques	Des outils tels que la robotique, les drones et les véhicules autonomes peuvent améliorer la surveillance des travailleurs et la fourniture de services, ainsi que la sécurité pour entraver l'application de la loi. Les systèmes compatibles avec l'IA incluent potentiellement un comportement collaboratif entre les outils afin d'accomplir des tâches.

Registres distribués et systèmes de maillage	Les concepts de registre distribué et les structures numériques communicatives complexes telles que la chaîne de blocs et le maillage peuvent toutefois transformer les modèles opérationnels, ce qui entraîne des problèmes de transparence.
Architecture numérique	À mesure que les plateformes et les structures de sécurité deviennent de plus en plus sophistiquées, l'architecture numérique peut améliorer l'efficacité commerciale de la criminalité organisée, la rendant impossible à distinguer des entreprises légitimes.
Écosystèmes numériques, réalité virtuelle et réalité augmentée	Les environnements d'exploitation en ligne peuvent créer de nouvelles opportunités pour les criminels organisés.

Exercices

Exercice 1 – Participation au Module par la discussion

Les études de cas documentent rarement des liens avec la cybercriminalité ou l'utilisation de la technologie. Les étudiants devraient donc être encouragés à accéder à la base de données jurisprudentielle SHERLOC de l'ONUDC et à discuter des questions clés.

Il peut être utile de définir des tâches de recherche relatives aux questions suivantes:

(a) Quels rôles la technologie peut-elle jouer dans la traite et/ou le trafic illicite de migrants?
(b) Comment l'autonomie de la victime peut-elle être affectée par la collecte de données effectuée par les auteurs ou les enquêteurs?
(c) Quel est le mécanisme d'orientation pour la traite des personnes dans votre juridiction?
(d) Quels mécanismes existe-t-il dans votre juridiction pour que les victimes de la traite des personnes ne soient ni poursuivies ni sanctionnées?
(e) Quelles sont les méthodes d'enquête disponibles dans votre juridiction incluant des restrictions aux opérations d'infiltration ou à la coopération internationale?

(f) Quelles sont les nouvelles tendances technologiques dans le contexte de la traite et / ou du trafic illicite de migrants?
(g) Quels problèmes financiers peuvent être identifiés?

Exercice 2 – Débats

Débat 1
Débattre de la question de savoir si la loi sur la cybercriminalité devrait être une décision des juridictions individuelles dans le contexte des instruments existants relatifs aux droits de l'homme ou le sujet d'une nouvelle convention mondiale.

Débat 2
Débattre de la question de savoir si les questions relatives aux données et à la vie privée doivent être ignorées pour permettre la collecte de données biométriques auprès de victimes de la traite ou de migrants en situation irrégulière qui franchissent les frontières.

Exercice 3 – Questions axées sur la résolution de problèmes

Problème de fraude en ligne (le contexte de la « fraude » peut être adapté et inclure la traite à des fins d'exploitation sexuelle ou d'exploitation du travail)

Une fraude mondiale consiste à acheter des noms de domaine et à utiliser des sites Web pour attirer des investisseurs en actions et en marchandises.

- Les documents d'entreprise frauduleux sont obtenus dans la juridiction A et utilisés pour ouvrir des comptes bancaires dans la juridiction B.
- Un site Web construit dans la juridiction C attire des investisseurs internationaux.
- Les appels téléphoniques sont acheminés vers un centre d'appels de la juridiction C. Les gestionnaires d'appels donnent aux investisseurs des conseils prédéfinis. Les demandes de communication avec la direction et les superviseurs sont transférées à l'aide de la technologie cryptée à ceux qui se trouvent plus haut dans la chaîne de commandement, également dans la juridiction C.
- Les investisseurs des juridictions D à Z reçoivent une documentation par courrier électronique (connectée au domaine).
- Les investisseurs envoient leur argent par virement bancaire sur les comptes bancaires ouverts dans la juridiction B. Les investisseurs reçoivent périodiquement des mises à jour sur leur investissement et sont contactés pour effectuer de nouveaux «achats» de temps à autre. La documentation est préparée et les courriels sont envoyés de la juridiction C.

Aucun investissement n'est jamais fait. Tous les niveaux de communication sont frauduleux. Au moment de la découverte, tout l'argent avait disparu du compte bancaire. Les travailleurs recrutés pour s'acquitter des tâches relevant de la juridiction C travaillent pour des salaires très bas dans de très mauvaises conditions de travail. Certains sont des migrants faisant l'objet du trafic.

Il s'agit d'un problème juridique complexe qu'il est recommandé d'utiliser comme problème de discussion. Les étudiants se divisent en trois groupes et réfléchissent aux liens entre la cybercriminalité et le trafic illicite de migrants ou la traite dans ce contexte:

(a) Les enquêteurs – la manière dont la technologie est utilisée et la manière dont elle pourrait être utilisée pour enquêter.
(b) Les procureurs – les questions de compétence et de coopération.
(c) Les avocats de la défense – la manière dont la technologie pourrait être utilisée dans les enquêtes de la défense.

Problème relatif à la diffusion en direct d'abus

Imaginer le scénario ci-dessus mais cette fois dans le contexte de la diffusion d'abus en ligne impliquant la diffusion en direct d'abus sexuel sur un enfant. Un problème supplémentaire est que lorsque cesse la diffusion en direct, il n'y a plus de contenu et la preuve est perdue.

Répondre aux questions suivantes:

- La diffusion en direct relève-t-elle de la définition de la traite des personnes?
- Comment l'infraction peut-elle faire l'objet d'une enquête et être prouvé?
- Comment les enfants peuvent-ils être localisés et protégés?
- Quelles sont les nouvelles tendances en matière de techniques d'enquête?

Problème relatif à la traite des personnes / trafic illicite de migrants

Jane achemine de la drogue d'un pays A vers un pays B. Elle est appréhendée à la frontière et indique qu'elle a été trompée par un recruteur pour un travail de femme de chambre. Elle dit qu'elle ne savait pas que le sac qu'on lui a donné contenait de la drogue. Elle pensait que c'était son uniforme de femme de chambre. Elle est vulnérable et issue d'un milieu défavorisé dans un pays source de victimes de la traite.

Demandez à vos étudiantsde répondre aux questions suivantes: Quel rôle la technologie peut-elle jouer

a) dans le contrôle et l'exploitation de Jane
b) dans l'enquête sur ce crime et

c) dans la protection de Jane en tant que victime de la traite des personnes.

Puis formuler une réponse comme si au lieu d'avoir transporté de la drogue, elle avait franchi illicitement une frontière et avait été appréhendée par les autorités de l'État. Comment la technologie peut-elle aider l'enquête sur ce crime?

Structure de classe recommandée

- Pour briser la glace et éveiller l'attention – voir les ressources visuelles ci-dessous (10 minutes)

- Lecture en ligne avec la section relative à l'introduction et aux questions clés du présent Module (approx. 85 minutes)

- Pause (10 minutes)

- Exercices (60 minutes) Les arrangements dépendront des exercices choisis, mais les arrangements suggérés sont les suivants:

    - La classe doit être divisée en petits groupes, et l'un des exercices proposés sera assigné à chaque groupe (le choix de recourir à tous les exercices proposés ou de se concentrer sur un ou plusieurs exercices incombe au conférencier);
    - Chaque groupe devra examiner l'étude de cas ou le problème et préparer les réponses aux questions posées (15 minutes);
    - Chaque groupe présentera ses réponses au reste de la classe et la discussion sera ouverte (environ 2 à 5 minutes par groupe);
    - Conclusion du conférencier (5 minutes).

NOTE: la structure de classe proposée est purement indicative. Etant donné que les connaissances des étudiants et leur exposition à ces questions varient énormément, le conférencier devra adapter les contenus ainsi que les durées suggérées pour chaque élément du Module, en fonction du contexte éducatif et social et des besoins de l'audience.

Lectures essentielles

- Latonero, Mark, Browyn Wex et Meredith Dank (2015). La technologie et la traite à des fins d'exploitation du travail dans une société en réseau: aperçu général, innovations émergentes et étude de cas aux Philippines. Californie: Université de Californie du sud, centre Annenberg sur les séries de recherche sur le leadership et les politiques de communication.
- Kyo Yeon, Park et Yujin Park (2018) (La technologie en tant que catalyseur, facilitateur et intermédiaire dans la traite des êtres humains: études de cas récentes) 'Technology as a catalyst, facilitator, and intermediator in human trafficking: Recent case studies'
- Pendergrass, Melissa A. (2018). (L'intersection de la traite des êtres humains et de la technologie) 'The Intersection of Human Trafficking and Technology'. Diss. Utica College
- Raets, Sigrid et Jelle Janssens (2018). (la traite et la technologie : Le rôle des technologies de communication numériques dans la traite des êtres humains) 'Trafficking & Technology: The role of digital communication technologies in the human trafficking business'
- Thakor, Mitali et Dannah Boyd (2013). (la traite interconnectée: réflexions sur la technologie et le mouvement de lutte contre la traite) 'Networked trafficking: Reflections on technology and the anti-trafficking movement'. *Dialectical Anthropology*, vol. 37, pp. 277-290
- Office des Nations Unies contre la drogue et le crime (2008). Forum de Vienne sur la lutte contre la traite des personnes 13-15 Février 2008, Austria Center Vienna, document d'information, atelier 017 la technologie et la traite des personnes. Vienne: ONUDC
- Zijlstra, J. et I. van Liempt (2017). (Déplacements intelligents (par téléphone): comprendre l'utilisation et l'impact de la technologie mobile sur les trajets de migration irrégulière) 'Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys', *Int. J. Migration and Border Studies*, vol. 2, pp. 174-191

Lectures avancées

- Foot, K. A., A. Toft et N. Cesare (2015). (progression dans les efforts de lutte contre la traite) 'Developments in Anti-Trafficking Efforts': 2008–2011, *Journal of Human Trafficking*, vol. 1, pp. 136-155
- Gacinya, John (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) 'Analyzing the influence of Information and Communication Technology on the scourge of human trafficking in Rwanda', *Academy of Social Science Journal*, vol. 3, pp. 1095-1102
- Gerry F., J. Muraszkiewicz et N. Vavoula (2016). (Le rôle de la technologie dans la lutte contre la traite des êtres humains: réflexions sur la protection de la vie privée et la protection des données) 'The role of technology in the fight against human trafficking: reflections on privacy and data protection concerns', *Computer Law & Security Review*, vol. 32, pp. 205-217
- Khorshed, Adam et Sophia Imran (2015). (La fracture numérique et l'inclusion sociale parmi les migrants réfugiés: un cas en Australie régionale) 'The Digital Divide and Social Inclusion among Refugee Migrants: A Case in Regional Australia', *Information Technology and People*, vol. 28, pp. 344-365
- Maras, Marie-Helen (2016). (La cybercriminologie*) 'Cybercriminology'*. Oxford University Press.
- Maras, Marie-Helen (2017). (Sites d'annonces classées en ligne: souteneurs et facilitateurs de la prostitution et de la traite à des fins d'exploitation sexuelle ?) 'Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking?', *Journal of Internet Law*, vol. 21, pp. 17-21
- Stalans, Loretta J. et Mary A. Finn (2016). (Comprendre comment Internet facilite la criminalité et la déviance) 'Understanding How the Internet Facilitates Crime and Deviance', *Victims & Offenders*, vol. 11, pp. 501-508

Autres sources

- Brunwasser, Mathew (2015). (Les fondamentaux des migrants du 21ème siècle: nourriture, hébergement, smartphone) A 21st Century Migrant's Essentials: Food, Shelter, Smartphone. *The New York Times*, 25 Août.
- Conrad, Scott, Greg Dorn et Philip Craiger (2010). (Analyse criminalistique d'une console Playstation 3) 'Forensic Analysis of a Playstation 3 Console'. Dans (Avancées en criminalistique numérique VI. criminalistique numérique) *'Advances in Digital Forensics VI. DigitalForensics' 2010. « IFIP Advances in Information and Communication*

*Technology (*Progrès de l'IFIP dans les technologies de l'information et de la communication) », K. Chow et S. Shenoi, eds. Springer

- Davies, Caroline (2016). (Un pédophile britannique prévoyait d'épouser une victime, de devenir famille d'accueil et d'abuser des enfants) British paedophile 'planned to marry victim and abuse foster children'. *The Guardian*, 3 Juin.
- De La Mare, Tess (2017). Online paedophile approached 500 girls on tween Movie Star Planet site - misspelled sex words to avoid moderators (Un pédophile en ligne a approché 500 filles sur le site de Movie Star Planet - des termes sexuels mal orthographiés pour éviter les modérateurs). *The Irish News*, 2 Septembre.
- Commission européenne (2016). L'utilisation des réseaux sociaux dans la lutte contre le trafic illicite de migrants. Réseau européen des migrations (REM).
- Réseau européen des migrations. Questions ad-hoc pour prévenir et lutter contre l'utilisation des réseaux sociaux dans le trafic de migrants
- Europol (2018). Évaluation de la menace que représente la criminalité organisée sur Internet, 2018. La Haye: Europol
- Europol (2017). Europol et le FBI arrêtent près de 900 personnes dans le cadre de la répression contre un réseau mondial de pédophiles, 5 Mai.
- Europol et Interpol (2016). Rapport sur les réseaux de trafic de migrants, résumé. La Haye: Europol
- FBI (2017). Opération Cross Country XI: recherche des mineurs victimes de la traite à des fins d'exploitation sexuelle et de prostitution.
- Internet Watch Foundation (2018). Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse (Tendances de l'exploitation sexuelle des enfants en ligne: examen de la distribution des abus sexuels sur des enfants transmis en direct).
- Interpol (non daté). Cybercriminalité.
- Jackman, Tom (2018). Backpage CEO Carl Ferrer pleads guilty in three states, agrees to testify against other website officials (Le PDG de Backpage, Carl Ferrer, plaide coupable dans trois États et accepte de témoigner contre d'autres responsables du site). *Washington Post*, 13 Avril.
- Karaman, Svebor, Tao Chen et Shih-Fu Chang (non daté). projet MEMEX de la DARPA. New York: Vidéo numérique et multimédias (DVMM) Laboratoire de l'université Columbia.
- Latonero, Mark (2011). The Role of Social Networking Sites and Online Classifieds (Le rôle des sites de réseautage social et des petites annonces en ligne). Californie: Université de Californie du sud, centre Annenberg sur les séries de recherche sur le leadership et les politiques de communication.
- Latonero, Mark (2012). The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking (L'essor du mobile et la diffusion de la traite facilitée par la technologie). Californie: Université de Californie du sud, centre Annenberg sur le leadership et les politiques de communication.

- Legorano, Giovanni et Joe Parkinson (2015). Following the Migrant Money Trail (suivre la piste de l'argent des migrants). *Washington Post*, 30 Décembre.
- Kunz, Ryan et al (non daté). Social Media and Sex Trafficking Process: From connection and recruitment, to sales (les réseaux sociaux et le processus de la traite à des fins d'exploitation sexuelle : de la connexion au recrutement jusqu'à la vente). Ohio: Université de Toledo.
- McGoogan, Cara et Muktadir Rashid (2016). Satellites reveal 'child slave camps' in Unesco-protected park in Bangladesh (Des satellites révèlent des "camps d'enfants esclaves" dans un parc protégé par l'Unesco au Bangladesh). *The Telegraph*, 23 Octobre.
- Pellerin, Cheryl. (2017). DARPA Program Helps to Fight Human Trafficking. DOD Combating Trafficking in Persons (Le programme de la DARPA aide à lutter contre la traite des personnes. Le DOD Lutte contre la traite des personnes), 4 Janvier.
- Slater, Chris (2018). Paedophile used computer games to groom young boy he raped and sexually abused (Un pédophile a utilisé des jeux informatiques pour violer et abuser sexuellement d'un jeune garçon). *Manchester Evening News*, 3 Août.
- Thorn (non daté). Spotlight (sous les projecteurs).
- Sénat des Etats Unis (2017). Backpage.com's Knowing Facilitation of Online Sex Trafficking. Staff Report Permanent Subcommittee on Investigations (Backpage.com savait qu'il facilitait la traite en ligne à des fins d'exploitation sexuelle. Rapport du sous -comité permanent en charge des enquêtes)
- Haut-Commissariat des Nations Unies pour les réfugiés. (2017). Du point de vue des réfugiés, discours des réfugiés et des migrants arabes et afghans sur les médias sociaux de mars à décembre 2016. Genève: HCRNU
- Projet interinstitutions des Nations Unies sur la traite des êtres humains (2008). Guide sur l'éthique et les droits de l'homme dans la lutte contre la traite. Bangkok: NU
- ONUDC (2008). Référentiel de lutte contre la traite des personnes. Vienne: ONUDC

Evaluation des étudiants

Rapport de recherche sur le rôle des technologies spécifiques dans le contexte de la traite des personnes/ du trafic illicite de migrants. Il est recommandé que l'essai soit de 3000 mots. Les questions possibles sont:

- Comment la technologie est-elle utilisée pour faciliter la traite et le trafic?
- Comment la technologie peut-elle aider à identifier et à protéger les victimes de la traite sans compromettre leurs données et leur droit à la vie privée?
- Comment la délinquance en ligne est-elle utilisée pour exploiter les victimes de la traite?

- L'exploitation humaine sera-t-elle réduite au fur et à mesure que les méthodes technologiques de délinquance sont identifiées?
- Dans quelle mesure les tribunaux virtuels seraient-ils utiles dans ce contexte?
- Toute autre question pertinente basée sur ces problèmes clés.

Outils additionnels d'apprentissage

Matériel vidéo

- (Pas ma vie) *Not My Life* (app. 1h 20 minutes), par Robert Bilheimer. Dans le but d'éduquer les téléspectateurs, ce film décrit les pratiques épouvantables de la traite des êtres humains dans le monde entier, notamment l'exploitation d'enfants aux fins de travail forcé, le tourisme sexuel, l'exploitation sexuelle et les enfants soldats..
- (Comment les banques peuvent-elles être utilisées pour mettre fin au trafic illicite des personnes) *How can banks be used to stop human trafficking?* (app. 29 minutes) par The Economist. La vidéo de 2018 montre comment les services répressifs allemands se sont associés à des banques pour identifier les flux financiers provenant de la traite des personnes afin de perturber cette activité criminelle.
- (Le rôle de la technologie dans la traite des personnes) *The Role of Technology in Human Trafficking* (app. 1h 30 minutes), par Microsoft Research (2012). La conférence présente plusieurs projets de recherche Microsoft qui mettent en lumière le rôle de plus en plus important de la technologie dans la traite des personnes, en mettant l'accent sur la prostitution des enfants. Les différents intervenants de la vidéo traitent de différents problèmes dans ce sens, notamment l'utilisation des traces de données pour aider à lutter contre la traite des personnes en identifiant les auteurs ou les victimes, en responsabilisant les forces de l'ordre et en perturbant la criminalité organisée.
- La technologie et la traite à des fins d'exploitation du travail dans une société en réseau (3:40 minutes), par le centre Annenberg sur le leadership et les politiques de communication (2015). La courte vidéo présente un projet de recherche sur le rôle de la technologie dans la traite des personnes à des fins de travail forcé, avec une étude de cas sur les Philippines.
- *I Am Jane Doe* (app. 1h 40 minutes), par Mary Mazzio (Netflix production). Ce documentaire de 2017 présente des cas réels de filles américaines impliquées dans le commerce sexuel d'enfants par le biais d'annonces dans la section des annonces classées en ligne d'un journal.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-3389, www.unodc.org