Nations Unies CTOC/COP/WG.7/2020/3

Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée

Distr. générale
15 juin 2020
Français
Original : anglais

Groupe de travail sur le trafic illicite de migrants
Vienne, 8 et 9 septembre 2020
Point 3 de l'ordre du jour provisoire*
Stratégies gagnantes concernant l'utilisation de la technologie, notamment des technologies de l'information et des communications, pour prévenir le trafic illicite de migrants, mener des enquêtes à ce sujet et adopter des mesures énergiques face à l'utilisation croissante du cyberespace par des groupes criminels

Stratégies gagnantes concernant l'utilisation de la technologie, notamment des technologies de l'information et des communications, pour prévenir le trafic illicite de migrants, mener des enquêtes à ce sujet et adopter des mesures énergiques face à l'utilisation croissante du cyberespace par des groupes criminels

Note d'information établie par le Secrétariat

I. Introduction

1. Le présent document d'information a été établi par le Secrétariat pour faciliter les débats du Groupe de travail sur le trafic illicite de migrants à sa septième réunion. Il présente une série de questions relatives au lien qui existe actuellement entre la technologie, notamment la technologie de l'information, et le trafic illicite de migrants, que le Groupe de travail voudra peut-être examiner au cours de ses délibérations. Il fournit des informations utiles sur un certain nombre de sujets, notamment le recours aux applications modernes aussi bien pour se livrer au trafic illicite de migrants que pour détecter ce trafic, enquêter à son sujet, en poursuivre les auteurs et le neutraliser, y compris dans le cyberespace, ainsi que les difficultés et les pratiques prometteuses liées à l'exploitation de la technologie, compte dûment tenu des garanties en matière de vie privée et de droits humains et des politiques de protection des données. Il répertorie également des références, ressources et outils que les États voudront peut-être examiner pour approfondir la mise au point de stratégies de lutte contre le trafic illicite de migrants.

* CTOC/COP/WG.7/2020/1.

V.20-03096 (F) 220720 230720

II. Questions à examiner

2. Les délégations voudront peut-être examiner les réponses apportées par leurs États aux questions suivantes lorsqu'elles prépareront les délibérations du Groupe de travail :

a) Quelles utilisations de la technologie moderne, notamment des technologies de l'information et des communications, entravent le plus les mesures de prévention de la criminalité et de justice pénale prises pour lutter contre les opérations de trafic illicite de migrants ?

b) Quelles mesures pratiques les États parties ont-ils prises pour s'adapter et parer à l'augmentation et à l'évolution de l'utilisation de la technologie par les trafiquants ?

c) En luttant contre une utilisation abusive de la technologie, notamment dans le cyberespace, quelles bonnes pratiques en matière de coopération multipartite et internationale les services de détection et de répression ont-ils définies ? Comment la coopération en matière de détection et de répression et de justice pénale pourrait-elle être améliorée pour relever ces défis ?

d) Quels moyens techniques ont été les plus efficaces et les plus abordables pour améliorer l'action menée contre le trafic illicite de migrants ? Quelles campagnes menées dans les médias sociaux ont été les plus efficaces et les plus adaptées pour sensibiliser aux risques du trafic illicite de migrants en déconstruisant la propagande ?

e) Comment l'Organisation des Nations Unies (ONU) peut-elle aider au mieux les États parties à chercher, recenser et diffuser de bonnes pratiques et des stratégies efficaces en matière d'utilisation de la technologie pour lutter contre le trafic illicite de migrants en temps de crise ?

f) Quels sont les enseignements les plus utiles qui ont été tirés du partenariat établi avec le secteur privé et la société civile en matière d'élaboration et de déploiement de moyens techniques efficaces de lutte contre le trafic illicite de migrants ?

g) Quels types de garanties en matière de vie privée et de droits humains les États parties ont-ils adoptées pour encadrer l'utilisation de la technologie dans le cadre de leurs mesures de prévention de la criminalité et de justice pénale, notamment face au trafic illicite de migrants ?

h) Comment les États parties garantissent-ils le respect de la vie privée et des droits humains des migrants lorsqu'ils enquêtent sur l'utilisation abusive des technologies de l'information et des communications et du cyberespace par des groupes criminels qui se livrent au trafic illicite de migrants ?

3. Le Groupe de travail voudra peut-être considérer les idées de mesures suivantes que pourraient prendre les États parties lorsqu'ils réfléchiront à des stratégies gagnantes de lutte contre le trafic illicite de migrants par l'utilisation de la technologie et qu'ils élaboreront des mesures viables pour lutter contre l'essor de l'utilisation abusive de la technologie par les groupes criminels, notamment dans le cyberespace :

- Développer considérablement la collecte et la recherche de données sur la portée, l'ampleur et la nature de l'utilisation abusive de la technologie qui facilite le trafic illicite de migrants, en particulier sur l'usage impropre d'Internet, des applications des médias sociaux et des opérations financières exécutées dans le cyberespace ;
- Déceler les lacunes des systèmes juridiques et y remédier afin de garantir l'efficacité des enquêtes et des poursuites dans les affaires de trafic illicite de migrants facilité par la technologie, en particulier en harmonisant les lois et en améliorant la coopération internationale et transfrontières ;

- Aider l'ONU à recenser, analyser et diffuser plus largement des stratégies et des pratiques prometteuses liées à l'utilisation des technologies modernes pour lutter contre cette forme de criminalité ;
- Soutenir les stratégies, politiques et moyens techniques axés sur la dimension mondiale du trafic illicite de migrants, par exemple les outils modulables d'élaboration de programmes de prévention ou d'agrégation de données en ligne qui facilitent une analyse automatisée de l'information et étayent les mesures de prévention et les enquêtes destinées à lutter contre ce trafic ;
- Contribuer à la normalisation et à la généralisation de l'exploitation de l'infrastructure technologique en mettant à profit les innovations technologiques existantes et veiller à ce que les nouvelles initiatives et les nouveaux cadres stratégiques ne fassent pas double emploi avec les mesures déjà prises dans le domaine de la technologie ;
- Renforcer les compétences techniques et les capacités des praticiens dans tous les secteurs afin de permettre une utilisation optimale de la technologie pour prévenir et combattre le trafic illicite de migrants ;
- Aider les services de détection et de répression à affermir leur présence dans le cyberespace, à mener des opérations de prévention, à saisir des preuves électroniques et à utiliser les outils technologiques disponibles ;
- Encourager et développer, s'il y a lieu, les partenariats et les ententes entre les différents secteurs et parties prenantes, notamment les organisations internationales et régionales, le secteur public, la société civile, le secteur privé et le milieu universitaire, afin d'améliorer la recherche, l'innovation, et la mise au point et l'utilisation de la technologie ;
- Tenir compte des questions de genre lors de l'élaboration de stratégies axées sur le lien entre technologie et criminalité ;
- Veiller à ce que l'utilisation de la technologie par les services de détection et de répression soit respectueuse des normes en matière de droits humains, d'équité, de responsabilité et de transparence ;
- Veiller à ce que les facteurs éthiques soient pleinement pris en compte lors du déploiement stratégique de la technologie, notamment de systèmes de surveillance à grande échelle, et à ce que, dans le cadre d'une utilisation croissante de l'apprentissage automatique et de l'intelligence artificielle pour amplifier l'action des services de détection et de répression, tout biais soit évité pendant les phases de programmation et de déploiement des logiciels d'intelligence artificielle.

III. Vue d'ensemble des questions et des sujets connexes

4. Le trafic illicite de migrants est une activité extrêmement lucrative, les réseaux criminels prospérant grâce à la forte demande de tels services et au faible risque de détection et de sanction. L'Office des Nations Unies contre la drogue et le crime (ONUDC) a rendu compte des activités de trafic illicite connues, qui ont généré entre 5,5 milliards et 7 milliards de dollars en 2016[1]. En 2017, l'Organisation internationale pour les migrations (OIM) a estimé que le trafic illicite rapportait environ 10 milliards de dollars par an dans le monde[2]. Ces profits dépendent fortement de la capacité qu'ont les États d'origine, de transit et de destination de prévenir cette forme de criminalité, de la détecter et d'enquêter à son sujet.

[1] *Global Study on Smuggling of Migrants 2018* (publication des Nations Unies, numéro de vente : E.18.IV.9).

[2] Source des données : Portail sur les données migratoires de l'OIM.

5. Dans ce contexte, compte tenu de leur ampleur, de leur étendue et de leur rythme, les changements amenés par la technologie numérique, notamment par les technologies de l'information et des communications, sont autant de possibilités à exploiter pour freiner la criminalité organisée tout en accélérant la réalisation du Programme de développement durable à l'horizon 2030[3]. Dans le même temps, le fait que la technologie soit plus accessible a des conséquences imprévues, comme son détournement par des groupes criminels[4].

6. Bien que la communauté internationale s'attache de plus en plus à lutter contre l'utilisation abusive d'Internet et de l'informatique à des fins criminelles et à intensifier l'utilisation constructive qui en est faite pour lutter contre la criminalité, notamment en contribuant aux enquêtes, en améliorant les poursuites, en sensibilisant les victimes et en leur fournissant des services, il n'y a pas assez de données sur l'ampleur des conséquences de l'utilisation de la technologie sur l'infraction de trafic illicite de migrants. Le recensement et la diffusion de pratiques et de stratégies prometteuses de lutte contre le trafic illicite de migrants par l'utilisation de la technologie semblent limités, et les systèmes reposant sur la technologie ne sont pas déployés de manière homogène d'un pays à l'autre, faute d'infrastructures adaptées, entre autres. En conséquence, le Groupe de travail voudra peut-être envisager ce qui a échoué et ce qui a fonctionné dans l'utilisation de la technologie, et comment appliquer uniformément les enseignements tirés, notamment par une coopération internationale accrue.

1. L'utilisation de la technologie pour faciliter le trafic illicite de migrants

7. Les technologies de l'information et de la communication sont devenues des outils importants et largement utilisés par les passeurs pour transmettre des informations sur les itinéraires, les services et les prix. La technologie est utilisée par les délinquants de manière abusive pour faciliter les paiements, ainsi que pour produire et diffuser des documents de manière frauduleuse, ce qui pose des difficultés supplémentaires aux systèmes de justice pénale qui, face à l'adaptation rapide des modes opératoires des délinquants et à la mutation constante du marché illicite, ont du mal à prévenir le phénomène et à y trouver des parades (A/CONF.234/11, par. 41 à 48). En ce qui concerne l'utilisation de la technologie par ceux qui ont recours aux services des passeurs, les plateformes des médias sociaux sont utilisées par les migrants pour communiquer et échanger leurs expériences au cours de leur voyage.

Publicité

8. Dernièrement, l'utilisation des plateformes des médias sociaux par les passeurs a augmenté de manière exponentielle. Les passeurs utilisent souvent les pages des médias sociaux que les migrants utilisent pour leurs échanges de vues et d'expériences pour publier des informations et des annonces destinées à faire connaître leurs itinéraires, leurs services et leurs tarifs. Il peut notamment s'agir d'images publicitaires, de descriptions précises des services offerts ou de modalités de paiement, par exemple le règlement après livraison du visa requis. La communication avec les clients potentiels est prise en charge par différentes applications de messagerie, dont certaines peuvent présenter l'avantage de l'anonymat et du chiffrement de bout en bout[5].

9. Parmi les informations fournies, les passeurs peuvent, par exemple, vendre différentes « formules de voyage » proposant des modes de transport allant du transport aérien au transport maritime. Pour vendre leurs services, les passeurs abusent souvent les migrants en éloignant ou en rapprochant les itinéraires de

[3] Voir le rapport du Groupe de haut niveau sur la coopération numérique du Secrétaire général de l'ONU sur la suite donnée aux recommandations (17 mars 2020).

[4] Rapport annuel 2019 des laboratoires d'innovation technologique des Nations Unies (New York, 2018).

[5] Réseau européen des migrations, « The use of social media in the fight against migrant smuggling » (octobre 2016).

migration clandestine de certains pays de transit et de destination, par exemple, en comptant sur leur méconnaissance des pays qui sont membres de l'Union européenne. Il a été rapporté que dans certains cas, les pages des médias sociaux avaient été utilisées par des passeurs qui prétendaient travailler pour des organisations non gouvernementales ou des institutions de l'Union européenne chargées d'organiser en toute sécurité l'acheminement de migrants en Europe par la mer. D'autres passeurs se seraient fait passer, dans les médias sociaux, pour des « conseillers juridiques » chargés d'aider les migrants afghans à déposer des demandes d'asile[6].

10. Les services de détection et de répression de l'Union européenne ont signalé des difficultés découlant de l'utilisation, par les délinquants, d'applications leur permettant d'utiliser des numéros de téléphone difficiles à repérer lorsqu'ils font la publicité de leurs services sur les réseaux sociaux ou qu'ils communiquent avec des migrants clandestins ou avec d'autres membres des réseaux criminels, ce qui complique les enquêtes menées sur les suspects[7].

Communication

11. Il a été rapporté que les migrants utilisaient de plus en plus les médias sociaux, à la fois avant leur départ, pour entrer en contact avec des passeurs, par exemple, et au cours de leur voyage, pour communiquer et recevoir des informations sur les itinéraires de migration des passeurs. On leur aurait aussi fourni des téléphones satellitaires à bord des bateaux ou sur les itinéraires empruntés pour leur permettre de communiquer avec les passeurs. La technologie mobile et son développement peuvent aussi avoir des incidences sur la relation entre passeurs et migrants. Dans quelques groupes de médias sociaux, par exemple, les migrants peuvent vérifier la fiabilité de certains services de passeurs, notamment en ce qui concerne la sécurité, les itinéraires et les tarifs, et partager des informations à ce sujet. Une fonction commune aux médias sociaux est donc qu'ils servent de tribunes à l'usage des consommateurs (voir A/CONF.234/11).

12. L'utilisation des médias sociaux par les migrants varie en fonction de leur nationalité, de leur appartenance ethnique et de leur région d'origine, et dépend aussi de leur accès à Internet ou à des smartphones, ainsi que de leur niveau d'instruction[5]. Il a été rapporté que les Syriens déplacés, par exemple, utilisaient beaucoup les applications de messagerie et les réseaux sociaux pour communiquer et partager des observations sur leur voyage. L'utilisation de ces outils a également été relevée en Asie du Sud, pour la sélection des passeurs, et en Afrique. Dans les pays de destination, les migrants ayant fait l'objet d'un trafic illicite publient des commentaires sur les passeurs et leurs services et dénoncent des situations dans lesquelles les passeurs ont délaissé, trompé ou maltraité des migrants. Les migrants et les réfugiés font également des observations sur ce qu'ils vivent dans les pays d'accueil et donnent notamment des informations sur les procédures administratives à accomplir pour séjourner dans le pays d'arrivée[8].

13. Dans l'ensemble, d'après la description qui a en été faite, l'utilisation des médias sociaux dans le cadre du trafic illicite de migrants aurait donc fortement contribué non seulement à la multiplication des opérations d'acheminement illégal, mais aussi à l'amélioration de leur efficacité. En conséquence, s'il est plus difficile d'enquêter sur cette infraction et d'en poursuivre les auteurs, l'entreprise pourrait aussi être plus sûre pour les migrants. Ces dernières années, un certain nombre de campagnes d'information et de sensibilisation ont été menées dans les médias sociaux pour empêcher, en déconstruisant la propagande, les candidats à la migration de

[6] Haut-Commissariat des Nations Unies pour les réfugiés, « From a refugee perspective: discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016 » (avril 2017).

[7] Agence de l'Union européenne pour la coopération des services répressifs (Europol), Centre européen pour la lutte contre le trafic de migrants, « 4th annual report 2019 » (mai 2020).

[8] Voir *Global Study on Smuggling of Migrants 2018*, p. 44.

s'embarquer dans des expéditions dangereuses. Toutefois, ces campagnes ont souvent donné des résultats mitigés[5].

Financement

14. Les technologies sont utilisées de manière abusive pour recevoir des paiements effectués dans des systèmes de paiement en ligne. Des virements peuvent être faits à des passeurs à partir des pays de destination par l'intermédiaire d'organismes commerciaux de transfert de fonds ou à l'aide d'applications de transfert de fonds. Dans certains cas, les fonds sont déposés auprès d'un organisme et protégés par un code de sécurité. Une fois que la personne migrante a confirmé qu'elle était arrivée sain et sauve dans le pays qui constitue sa destination intermédiaire ou finale, le code de sécurité est divulgué au passeur et les fonds sont débloqués.

15. Les paiements aux passeurs peuvent être échelonnés, y compris s'ils sont effectués par des membres de la famille qui se sont portés caution. L'utilisation de cybermonnaies peut aider les passeurs à recevoir, dissimuler et transférer de l'argent plus aisément. Elle peut faciliter le blanchiment d'argent et éviter aux passeurs d'être visés par une enquête et arrêtés, en leur garantissant l'anonymat et en leur permettant de ne pas avoir à transporter de grandes quantités d'espèces (voir A/CONF.234/11).

Faux documents

16. Divers équipements sont utilisés pour produire, modifier ou copier des passeports de manière frauduleuse. La technologie joue également un rôle majeur dans la mise à disposition de faux documents de voyage ou d'identité pour faciliter le trafic de migrants[9].

17. Parce qu'ils garantissent aux utilisateurs l'anonymat et la possibilité de communiquer des informations en temps réel, les services de messagerie sont utilisés pour promouvoir à grande échelle les faux documents destinés à faire entrer des personnes illégalement, sous une fausse identité. D'après Europol, le commerce en ligne de faux documents qui facilitent la criminalité gagnera de l'importance pour l'organisation des migrations irrégulières[7].

18. Les délinquants peuvent recourir à des services de messagerie pour envoyer de faux documents d'identité à des intermédiaires ou directement aux migrants. Ainsi, Europol a détecté, dans les médias sociaux, des dizaines de comptes de groupes contenant des photos de milliers de documents. Certains de ces groupes avaient des dizaines de milliers d'abonnés. Un grand nombre de ces documents auraient été volés par des groupes organisés de pickpockets dans divers sites touristiques européens[7].

2. Utilisation de la technologie moderne pour prévenir et combattre le trafic illicite de migrants

19. Dans son article 10, le Protocole contre le trafic illicite de migrants par terre, air et mer, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée, qui est entré en vigueur le 28 janvier 2004, dispose que les États parties échangent, conformément à leurs systèmes juridiques et administratifs respectifs, des informations pertinentes concernant notamment des questions techniques présentant une utilité pour la détection et la répression, afin de renforcer mutuellement leur capacité à prévenir et détecter le trafic illicite de migrants, à mener des enquêtes sur ces actes et à en poursuivre les auteurs. De plus, il est essentiel de prévoir des garanties suffisantes en matière de droits humains lorsque la technologie est utilisée à toutes les étapes des enquêtes, notamment lors d'opérations de recherche et de saisie (voir section IV ci-dessous).

[9] Pour plus d'informations sur l'utilisation de documents à des fins abusives et les faux documents dans le cadre du trafic illicite, voir CTOC/COP/WG.7/2019/3.

20. La lutte contre le trafic illicite de migrants restant une priorité politique des États Membres, ceux-ci ont de plus en plus à cœur de trouver des moyens efficaces d'exploiter et d'appliquer la technologie, de mettre à mal les réseaux du trafic illicite de migrants et d'adopter des mesures énergiques contre cette forme de criminalité. De fait, au-delà de leur utilisation délictueuse, comme dans le cas de la traite des personnes[10], les technologies peuvent être exploitées de manière constructive pour prévenir, détecter, combattre et contrecarrer la criminalité organisée.

21. Par exemple, la technologie est de plus en plus souvent déployée aux frontières, où elle permet de lutter contre le trafic illicite, pourvu que les agents qui y opèrent soient suffisamment entraînés et formés pour repérer les indices de ce trafic. La technologie peut aussi être utilisée par les services de détection et de répression pour repérer des passeurs (systèmes d'apprentissage automatique, d'intelligence artificielle et de reconnaissance faciale) et des opérations suspectes (applications d'exploration de données).

22. En outre, la technologie peut faciliter l'enregistrement, le stockage, l'analyse et l'échange d'informations relatives au trafic illicite de migrants. Les preuves électroniques – réservations de billets d'avion et relevés bancaires de retraits d'espèces à l'étranger – aident à prouver qu'un acte de criminalité transnationale a été commis. Les éléments qui prouvent que des suspects ont utilisé de faux identifiants d'appelants ou des logiciels espions peuvent être utilisés pour rejeter des affirmations d'association innocente et prouver une intention délictueuse.

Gestion du contrôle aux frontières

23. L'utilisation de la technologie moderne pour détecter le franchissement illégal de frontières a eu des avantages sensibles pour les services de surveillance des frontières chargés de prévenir et de combattre le trafic illicite de migrants conformément à l'article 11 du Protocole relatif au trafic illicite de migrants, et elle est souvent présentée comme une mesure efficace et concrète qui facilite le contrôle des passagers dans les aéroports. Il a été rapporté que plusieurs technologies différentes étaient utilisées, par exemple l'imagerie thermique et d'autres types de détecteurs de présence humaine. Comme c'est le cas pour toutes les mesures prises pour faire appliquer la loi, leur conception et leur mise en œuvre doivent s'inscrire dans le respect du droit international et du droit interne, notamment de leurs dispositions relatives aux droits humains.

Matériel de détection automatique

24. Parmi les technologies évoluées qui sont utilisées, on trouve les scanneurs à rayons X, les scanneurs d'empreintes digitales, les scanneurs de passeports électroniques et leurs interfaces utilisateur, les portes électroniques automatisées et les visas biométriques. Les pays ont mis en évidence un large éventail de dispositifs, notamment des microscopes, des lentilles permettant de décoder les éléments invisibles de sécurité des photos et des appareils permettant de vérifier les documents, par exemple des appareils de contrôle de l'authenticité et des lecteurs de documents. D'autres ont noté l'avantage des contrôles d'identité automatisés, qui autorisent l'entrée des passagers sur la base de la reconnaissance de leurs informations biométriques, comme la reconnaissance faciale et la reconnaissance de l'iris, de sorte que les erreurs d'origine humaine qui pourraient être causées par la fatigue ou la distraction du personnel de contrôle aux frontières peuvent être évitées. Ces contrôles peuvent aussi se révéler rentables, car ils nécessitent moins de personnel.

25. Dans l'espace Schengen, par exemple, les États Membres ont noté que le Système d'information Schengen et le Système européen d'identification des visas mis en œuvre étaient des outils pratiques et permettaient de détecter le trafic illicite de migrants aux frontières. D'autres exemples ont été fournis sur la question du

[10] Voir Groupe interinstitutions de coordination contre la traite des personnes, « Human trafficking and technology: trends, challenges and opportunities », Issue brief, n° 7 (2017).

contrôle des documents aux points d'entrée. Les bases de données et d'autres systèmes d'archivage d'images de l'Organisation internationale de police criminelle (INTERPOL), comme les systèmes de renseignements préalables concernant les voyageurs, sont aussi utilisés pour vérifier les informations aux points d'entrée. Tous ces systèmes sont des moyens de partager et de télécharger des éléments de données communs relatifs aux voyageurs. Les informations recueillies sont souvent utilisées pour démanteler des réseaux de trafic illicite[11].

26. On rapporte que des moyens techniques d'un nouveau type, tels que les scanneurs d'empreintes digitales et les scanneurs faciaux sans contact, sont en cours de mise au point et qu'ils permettront une automatisation plus poussée des contrôles aux frontières et une sécurité accrue. On s'attend à ce qu'ils ouvrent la voie à la « biométrie en mouvement », qui bénéficiera aux aéroports et aux compagnies aériennes mais contribuera aussi à réduire le temps d'attente des voyageurs[12].

Intelligence artificielle

27. À l'échelle mondiale, comme c'est le cas pour d'autres applications professionnelles, la puissance de calcul de l'intelligence artificielle et de l'apprentissage automatique est de plus en plus étudiée pour donner plus d'efficacité aux mesures prises contre le trafic illicite de migrants. L'intelligence artificielle peut aider à établir des prévisions, formuler des recommandations ou prendre des décisions en toute indépendance, à une grande échelle et sans intervention humaine, en combinant et analysant les renseignements obtenus de multiples sources à l'aide d'algorithmes programmés.

28. Dans le contexte du trafic illicite de migrants, par exemple, on déploie des systèmes fonctionnant à l'aide de l'intelligence artificielle pour évaluer les voyageurs aux points de passage de la frontière. L'intelligence artificielle permet d'amplifier la capacité de traitement et d'échange d'une grande quantité de données dans un bref laps de temps pour produire et partager rapidement une évaluation complète de la menace. Pour illustrer son application récente au contrôle aux frontières, on peut citer : l'utilisation d'algorithmes conçus pour reconnaître des schémas ou des comportements à partir de données anciennes sur les voyageurs obtenues auprès de différents organismes publics et d'autres sources, qui permet d'établir en temps réel des évaluations mathématiques des risques ; et le déploiement de caméras et de radars à haute résolution fonctionnant à l'aide de l'intelligence artificielle et utilisant un logiciel spécifique qui peut faire la distinction entre des déplacements anormaux de bateaux et le trafic maritime dense habituel[13].

Données d'imagerie et du Système mondial de localisation

29. Les systèmes de poursuite à l'aide d'images satellites et le Système mondial de localisation permettent la détection et la reconnaissance de mouvements suspects aux frontières. Parmi le matériel technique recensé, fourni et déployé, on peut citer les scanneurs de véhicules à rayons X, les scanneurs thermiques et les caméras de surveillance utilisés pour détecter les migrants faisant l'objet d'un trafic illicite, y compris lorsqu'ils sont enfermés dans des véhicules ou des caches pendant leur transit. Cette technologie et ses améliorations progressives, si elles sont prises en

[11] Commission européenne, Réseau européen des migrations, *Practical Measures to Reduce Irregular Migration* (octobre 2012).

[12] Frontex, « 2019 in brief » (janvier 2020). Frontex, l'Agence européenne de garde-frontières et de garde-côtes, recueille et partage avec les autorités nationales et Europol des informations relatives à la criminalité aux frontières. Elle a annoncé qu'elle mettait en place le service central du système européen d'information et d'autorisation concernant les voyages, un nouveau système conçu pour délivrer des autorisations de voyager dans l'Union européenne aux ressortissants de pays tiers exemptés de visa, qui sera utilisé pour vérifier les demandes de visa.

[13] Paul Koscak, « Artificial intelligence turns the tide on securing northern border waterways », Bureau des douanes et de la protection des frontières des États-Unis (mai 2020).

charge par des professionnels bien formés, peuvent faciliter et encourager une meilleure gestion des frontières et des migrations[14].

30. Parmi les pratiques adoptées au niveau national et transnational, on peut citer l'utilisation de systèmes de surveillance intégrés à longue portée capables d'intercepter et de surveiller des bateaux en mer et de déterminer le nombre de personnes présentes à leur bord. Ces mesures peuvent aussi faciliter l'identification des passeurs, qui pourraient, au moment de leur interception, essayer de se cacher parmi les migrants qu'ils acheminent illégalement. Des systèmes de drones aériens sont de plus en plus utilisés comme des plateformes aériennes pour capteurs – des caméras optiques fonctionnant dans les spectres visible et infrarouge, par exemple – pour assurer des fonctions de détection, de reconnaissance et d'identification à longue portée. Ils peuvent en outre enregistrer une image complète des déplacements des bateaux. À mesure que le secteur des drones évoluera, le coût de cette technologie diminuera et il sera possible de la déployer plus largement.

Stratégies et techniques d'enquête

31. Il est très intéressant de chercher des moyens permettant aux services de détection et de répression d'utiliser la technologie moderne de manière intégrée pour mettre à mal les réseaux du trafic illicite et de tirer pleinement parti de technologies en plein essor telles que l'intelligence artificielle, l'apprentissage automatique et la criminalistique informatique pour améliorer la prévention et le contrôle de la criminalité et les enquêtes pénales dans les affaires de trafic illicite.

Intelligence artificielle

32. En ce qui concerne la lutte contre la criminalité organisée, des débats sont actuellement menés au niveau national sur l'utilisation de l'intelligence artificielle pour contribuer à l'optimisation des ressources de la police consacrées à la collecte de preuves numériques. Encouragés par les avancées de l'intelligence artificielle qui ont rendu la robotique plus « intelligente » et en mesure de remplacer les êtres humains dans de nombreuses fonctions et tâches, un nombre croissant de services de détection et de répression ont adopté ces technologies dans plusieurs opérations.

33. Parmi les utilisations prometteuses de l'intelligence artificielle et de la robotique qui pourraient être appliquées aux enquêtes et aux opérations de détection et de répression pour lutter contre le trafic illicite de migrants, on peut citer les pratiques prédictives modernes de police et l'analyse des zones de tension, qui permettent d'optimiser les outils de détection des comportements dont disposent les forces de l'ordre et de prévoir où et quels types d'infractions risquent de se produire[15].

34. Par ailleurs, on rapporte que l'intelligence artificielle et l'apprentissage automatique constituent des outils de plus en plus efficaces pour prévenir le blanchiment du produit d'opérations de trafic illicite et remonter à son origine. À l'instar des algorithmes qui aident les commerçants en ligne à cibler leurs clients, l'intelligence artificielle et l'apprentissage automatique peuvent contribuer à l'application de mesures de diligence raisonnable plus pertinentes et plus précises, en interprétant les signaux caractéristiques d'une activité criminelle et en analysant de plus grandes quantités de données de manière plus fiable (A/CONF.234/11, par. 41 à 48).

[14] OIM, Immigration and Border Management. Disponible à l'adresse https://www.iom.int/fr/immigration-and-border-management-2.

[15] Institut interrégional de recherche des Nations Unies sur la criminalité et la justice et Organisation internationale de police criminelle, « Artificial intelligence and robotics for law enforcement » (2019).

Technologie mobile et criminalistique informatique

35. Puisque les passeurs dépendent de la technologie mobile, notamment des smartphones, ces appareils pourraient constituer une source abondante de preuves. Les publications – images, vidéos et informations sur les contacts, les contacts associés et les lieux – peuvent être collectées à partir des comptes des médias sociaux, et les traces numériques, notamment l'historique de navigation stocké sur les ordinateurs personnels et les adresses IP, peuvent être enregistrées[5].

36. Les données stockées sur des appareils numériques (ordinateurs, smartphones, tablettes, téléphones et autres appareils dotés d'une mémoire numérique), sur des dispositifs de stockage externe (disques durs externes et clés USB) et sur des composants et appareils de réseau (routeurs et serveurs) pourraient être prélevées pour en extraire des informations ou des métadonnées concernant notamment l'identité et l'emplacement des utilisateurs, des transactions ou les expéditeurs et destinataires de télécommunications et de communications électroniques. Les métadonnées peuvent aider les services de détection et de répression à déterminer les dates auxquelles les images ont été prises et les infractions commises. Les données relatives aux images et à la localisation géographique peuvent aussi être utilisées pour déterminer l'emplacement où s'est déroulé un événement concret[16].

La technologie au tribunal

37. L'article 24 de la Convention contre la criminalité organisée oblige les États parties à protéger activement les témoins dans le cadre d'affaires pénales, précisément en prévoyant des règles de preuve qui leur permettent de déposer d'une manière qui garantisse leur sécurité, par exemple en les autorisant à déposer en recourant à des techniques de communication telles que les liaisons vidéo ou à d'autres moyens adéquats. Il existe plusieurs pratiques qui permettent aux témoins de déposer un témoignage à distance par liaison vidéo ou en audioconférence. Elles permettent par exemple aux migrants victimes de trafic qui sont retournés dans leur pays d'origine, ou aux témoins qui se trouvent dans d'autres juridictions, de fournir des preuves sans avoir à être présents dans le pays où se déroulent les poursuites.

38. Dans ces cas, les témoins apparaissent sur l'écran installé dans la salle d'audience, et une caméra placée dans la salle d'audience leur permet de suivre les débats à distance. De telles procédures, lorsqu'elles sont rendues possibles par le droit pénal interne, sont particulièrement utiles pour recueillir les témoignages de personnes résidant à l'étranger, notamment celles qui ont une connaissance du trafic illicite de migrants. Elles peuvent aussi être appliquées à différents stades du procès pénal, notamment au stade de l'audience relative à la détention, de la première comparution, de l'audience préliminaire et du prononcé de la peine. L'efficacité de ces pratiques dépend de la possibilité d'accéder à Internet et à des moyens techniques à distance.

39. L'utilisation et l'admissibilité de la technique de la liaison vidéo dépendent généralement de plusieurs facteurs : incapacité ou refus du témoin de se déplacer, coût relatif de la technique, sécurité et fiabilité de cette technique en ligne, importance de la preuve proposée et existence d'autres moyens pour admettre la preuve.

40. À bien des égards, la pandémie mondiale de maladie à coronavirus (COVID-19) a entraîné une intensification ou une accélération de l'application des technologies et la mise au point de stratégies de justice pénale fondées sur l'utilisation de la technologie. Ainsi, en raison de la pandémie et des mesures de confinement auxquelles elle a donné lieu, qui ont entravé la mobilité à l'échelle mondiale, une nouvelle technologie a été déployée pour continuer à faire fonctionner le système de justice pénale, notamment des plateformes vidéo permettant aux parties à une audience pénale d'y participer à distance et aux magistrats de tenir des audiences en

[16] Initiative Éducation pour la justice de l'ONUDC, Série de modules universitaires, « Module 4 : Introduction à la criminalistique informatique » et « Module 6 : Aspects pratiques des enquêtes sur la cybercriminalité et de la criminalistique numérique ».

toute sécurité, ce qui a permis d'assurer plus facilement la continuité des mesures de justice pénale[17].

41. En outre, le recours à des éléments de preuve obtenus dans les médias sociaux ou à l'aide de la technologie peut étayer les témoignages des migrants victimes de trafic recueillis dans le cadre de procédures pénales. Des conditions juridiques et techniques doivent être remplies pour assurer l'admissibilité des preuves numériques dans un tribunal de justice et, dans la pratique, ces conditions varient considérablement au niveau national.

42. Les enquêteurs spécialisés dans la cybercriminalité et les experts de la criminalistique informatique qui manipulent ou traitent de quelque manière que ce soit des preuves numériques doivent adhérer aux politiques nationales et aux lignes directrices relatives aux pratiques exemplaires pour garantir l'admissibilité des preuves numériques dans les tribunaux. Ces politiques énoncent les conditions techniques et juridiques nécessaires à l'admissibilité des preuves. Outre ces conditions, l'harmonisation des pratiques en matière d'enquêtes sur la cybercriminalité et de criminalistique informatique entre les pays est essentielle pour les enquêtes, qui font souvent intervenir plusieurs juridictions[18].

43. Pour déterminer l'admissibilité des preuves issues de la criminalistique informatique, il faut donc bien connaître le droit pénal, la loi relative à la protection de la vie privée, les droits de la personne, les politiques de protection des données et les voies de l'entraide judiciaire[19]. Pour demander des preuves électroniques du trafic illicite de migrants transfrontière, il faut qu'il existe des lignes directrices sur la marche à suivre au niveau national pour recueillir, conserver et partager les preuves électroniques, l'objectif global étant de permettre le bon déroulement de l'entraide judiciaire. Cela peut nécessiter, entre autres, d'associer les procédures adoptées par les grands prestataires de services de communication et les modalités pratiques de la coopération en matière de détection et de répression et de l'entraide judiciaire adoptées par les points de contact et définies dans les cadres juridiques[20].

IV. Stratégies visant à prévenir et combattre le trafic illicite de migrants à l'aide de la technologie : difficultés liées à leur conception et autres considérations

44. Dans le cadre du trafic illicite de migrants facilité par les technologies de l'information et des communications, il se peut que les responsables du trafic illicite, les migrants qui en sont victimes et les plateformes technologiques se trouvent tous dans des pays différents, ce qui pose de grandes difficultés pour la détermination de la juridiction, la collecte de preuves, l'extradition et l'entraide judiciaire.

45. L'absence ou le manque de coopération entre les institutions nationales, ainsi que d'autres obstacles pratiques et juridiques à la coopération internationale, entravent l'élaboration et l'application de stratégies efficaces de lutte contre l'utilisation abusive de la technologie par des réseaux criminels.

46. Pour tirer parti de toutes les possibilités qu'offre la technologie, y compris l'informatique, afin de réagir rapidement face aux innovations adoptées par les délinquants, il faut savoir exploiter toutes les ressources et les compétences techniques de secteurs très variés.

---

[17] Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, « New tech will help keep the criminal justice system moving during COVID-19 pandemic » (30 avril 2020).

[18] Voir ONUDC, initiative Éducation pour la justice, « Module 6 : Aspects pratiques des enquêtes sur la cybercriminalité et de la criminalistique numérique ».

[19] Voir Convention des Nations Unies contre la criminalité transnationale organisée, art. 18, par. 1.

[20] Voir ONUDC, Direction exécutive du Comité contre le terrorisme et Association internationale des procureurs et poursuivants, *Guide pratique sur la demande de preuves électroniques à l'étranger* (Vienne, 2019).

47. Le manque de capacités, d'informations et de compétences techniques des services de détection et de répression, des procureurs et de l'appareil judiciaire, qui s'expliquent, entre autres, par le manque de ressources et par la complexité et l'évolution rapide des technologies de l'information et des communications, empêche les services de prévention de la criminalité et les systèmes de justice pénale de s'adapter rapidement aux modes opératoires des passeurs et de tirer parti des possibilités offertes par l'utilisation de la technologie moderne pour prévenir et combattre la criminalité.

48. Le secteur de l'intelligence artificielle et de l'apprentissage automatique se développant rapidement, il est difficile d'éviter les biais dans la programmation des algorithmes complexes qui pourraient renforcer les stéréotypes ethniques ou de genre. Ces biais concernent par exemple l'intelligence artificielle appliquée aux technologies de l'analyse faciale, qui risque non seulement d'introduire des discriminations à l'égard de groupes caractérisés par l'appartenance à une ethnie ou à un genre, mais aussi de donner lieu à des données faussées et à des erreurs[21].

49. La recherche, le recensement et la diffusion de solutions techniques et de stratégies prometteuses et efficaces de lutte contre le trafic illicite de migrants sont actuellement insuffisants et pourraient être utilement intensifiés pour porter davantage sur l'adaptabilité et l'utilisation plus large des pratiques qui ont fait leurs preuves.

50. La disponibilité limitée des outils technologiques et les difficultés qu'il y a à accéder à des infrastructures technologiques souvent coûteuses font que l'obtention, l'utilisation et le déploiement de moyens techniques sont fragmentés et inégaux d'un pays à l'autre et d'une région à l'autre.

51. Une utilisation appropriée de la technologie aide les pouvoirs publics, le secteur privé et les organisations non gouvernementales à prévenir le trafic illicite de migrants dans leurs domaines de compétence respectifs et à porter assistance aux migrants. Il est donc primordial de renforcer l'efficacité des mesures de justice pénale, de mettre en place des mesures incitatives à l'intention des prestataires de services en ligne et d'établir des partenariats avec eux pour améliorer la surveillance, la détection et le signalement des cas de trafic illicite.

Considérations relatives à la vie privée, aux garanties et à la protection des données

52. Compte tenu de la nature internationale du trafic illicite de migrants, l'action menée par les services de détection et de répression pour lutter contre ce phénomène fait nécessairement intervenir de multiples juridictions. Dans le cadre de cette lutte, il convient de prêter une attention particulière aux questions de vie privée et de protection des données, outre celles, plus larges, des droits humains. Il est d'une importance fondamentale que toutes les technologies de géolocalisation, de collecte de données et de surveillance, notamment celles que met au point le secteur privé, respectent les normes en matière de droits humains, d'équité, de responsabilité et de transparence lorsqu'elles sont utilisées, de quelque manière que ce soit, par les services de détection et de répression[22].

53. L'intelligence artificielle et la robotique améliorant de plus en plus et dans une large mesure les capacités de surveillance des services de détection et de répression, il devient de plus en plus nécessaire de répondre aux préoccupations en matière de vie privée que soulève leur utilisation, notamment pour déterminer quand et où elle est autorisée.

---

[21] Pour plus d'informations sur les biais dans l'intelligence artificielle, voir James Manyika, Jake Silberg et Brittany Presten, « What do we do about the biases in AI? », *Harvard Business Review* (25 octobre 2019).

[22] Voir aussi Haut-Commissariat aux droits de l'homme, *Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies* (Genève, 2011).

54. L'utilisation croissante de la technologie dans d'autres secteurs de la justice pénale a déjà mis en évidence des préoccupations relatives à la vie privée, à l'éthique, à la transparence, au principe de responsabilité et au consentement éclairé, ce dernier devenant de plus en plus pertinent en raison du recours des services de détection et de répression à l'intelligence artificielle[23]. La question des garanties normatives et législatives est souvent débattue lorsqu'il s'agit d'utiliser des informations obtenues par les services de détection et de répression sur des personnes suspectes ou accusées ou des informations sur des tiers, notamment les migrants, acquises dans le cadre d'enquêtes, ainsi que la question de l'admissibilité de ces informations devant les tribunaux.

55. Il y a à cet égard des défis à relever, par exemple : faire en sorte que les données sensibles soient stockées en toute sécurité et que seules les personnes autorisées puissent y accéder ; veiller à ce que le partage de données entre les organismes compétents et entre les pays soit conforme aux cadres juridiques nationaux et internationaux et prenne en compte les normes relatives à la vie privée et à la confidentialité ; élaborer des protocoles de consentement qui prennent en compte le genre et l'âge ; évaluer les risques liés à la diffusion par les services de détection et de répression d'informations susceptibles d'être reliées à l'identité des migrants[24].

56. Une autre préoccupation essentielle est de préserver les garanties en matière de droits humains à tous les stades des enquêtes menées sur des personnes suspectes ou accusées. Cette considération est particulièrement pertinente dans le cas des opérations de recherche et de saisie, par exemple lorsqu'il s'agit de déchiffrer ou d'intercepter des SMS, d'enregistrer des appels audio ou d'analyser des données informatiques. La vie privée en ligne et l'existence de garanties et de normes à l'usage des services de détection et de répression peuvent être des sources de préoccupation lorsqu'il est question de l'obtention de mots de passe de smartphones ou d'ordinateurs ou du déchiffrement d'applications de messagerie du secteur privé[25].

57. Pour conclure, les outils technologiques peuvent être utiles pour intensifier la lutte contre le trafic illicite. Toutefois, la prudence est de mise lorsqu'il s'agit d'y recourir, afin d'en garantir une utilisation responsable et éthique et d'éviter les imprévus. Ce point est particulièrement important dans la mesure où certaines des technologies qui sont mises au point et déployées rapidement sont relativement nouvelles et n'ont pas encore été mises à l'essai, aussi faut-il suivre et évaluer leurs retombées, comme c'est le cas lorsqu'elles sont appliquées dans des domaines similaires.

Coopération internationale

58. La question de l'utilisation de la technologie dans le cadre de la coopération internationale en matière d'affaires pénales continue à être débattue. En 2016, la Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée a encouragé les États parties, dans sa résolution 8/1, à exploiter le plus efficacement possible les technologies disponibles pour faciliter la coopération entre les autorités centrales.

59. Dans le cadre de la Commission pour la prévention du crime et la justice pénale, un groupe intergouvernemental d'experts à composition non limitée a été chargé de faire une étude exhaustive du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, y compris l'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, le but étant

[23] Dunja Mijatović, « Safeguarding human rights in the era of artificial intelligence », Conseil de l'Europe (3 juillet 2018).

[24] Projet interorganisations des Nations Unies sur la traite des êtres humains, *Guide to Ethics and Human Rights in Counter-Trafficking: Ethical Standards for Counter-Trafficking Research and Programming* (Bangkok, 2008).

[25] Voir Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, « Encryption and anonymity follow-up report » (juin 2018).

d'examiner les options envisageables pour renforcer les mesures, juridiques ou autres, prises aux échelons national et international pour faire face à la cybercriminalité et d'en proposer de nouvelles[26]. En décembre 2019, l'Assemblée générale a adopté la résolution 74/247 sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, dans laquelle elle s'est félicitée du travail accompli par le groupe d'experts et a prié celui-ci de le poursuivre. Dans la même résolution, l'Assemblée a décidé d'établir un comité intergouvernemental spécial d'experts à composition non limitée, représentatif de toutes les régions, ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

60. Le renforcement de la coopération internationale, de plus en plus nécessaire, est largement subordonné à la disponibilité des ressources, notamment des ressources technologiques, telles que des réseaux permettant de transmettre des informations en toute sécurité, des outils facilitant la communication et des systèmes de gestion des dossiers assurant le suivi des demandes reçues et envoyées. La mise à disposition de ces ressources devrait permettre, entre autres, un traitement plus efficace des demandes d'entraide judiciaire portant sur des éléments de preuve électroniques, par exemple par la création d'unités spécialisées relevant des autorités centrales[27].

61. D'une manière générale, la coopération internationale contribue à l'application normalisée de stratégies et de solutions techniques efficaces et au partage effectif d'informations qui permet d'harmoniser leur utilisation et leur application.

Recommandations antérieures du Groupe de travail sur le trafic illicite de migrants portant sur des sujets connexes

62. À ce jour, le Groupe de travail sur le trafic illicite de migrants a formulé plus de 170 recommandations adressées aux États parties au sujet de l'application du Protocole relatif au trafic illicite de migrants.

63. Avant la présente session, le Groupe de travail n'a pas examiné ou adopté de recommandations sur l'utilisation de la technologie, notamment des technologies de l'information et des communications, pour prévenir le trafic illicite de migrants et mener des enquêtes à ce sujet.

64. En examinant les mesures concrètes à mettre en œuvre face à l'utilisation de technologies émergentes, le Groupe de travail a mis en évidence, dans ses recommandations antérieures, les points suivants : a) les États parties devraient examiner les moyens de renforcer la coopération à tous les niveaux pour prévenir et combattre les infractions visées par le Protocole relatif au trafic illicite de migrants commises grâce à l'utilisation de nouvelles technologies, en particulier Internet ; b) cette coopération pourrait porter sur l'amélioration de l'échange d'informations et de bonnes pratiques en matière d'incrimination, d'enquêtes et de poursuites ; et c) les États parties devraient organiser des campagnes d'information, qui pourraient faire intervenir les médias et les réseaux sociaux sur Internet, afin de faire prendre davantage conscience des effets préjudiciables du trafic illicite de migrants et de mettre en garde les personnes vulnérables susceptibles d'en faire l'objet, en particulier les jeunes et leurs familles, contre les risques qu'ils encourent.

65. Dans le document d'information établi par le Secrétariat, contenant un index des recommandations adoptées par le Groupe de travail sur le trafic illicite de migrants au cours de ses cinq premières réunions (CTOC/COP/WG.7/2019/4), on trouve des orientations utiles sur les thèmes suivants : contrôle et gestion des frontières ; système de justice pénale et enquêtes ; partage d'information ; partage de renseignement ; coopération internationale et entraide judiciaire ; et intervenants et secteur privé.

[26] Résolution 65/230 de l'Assemblée générale, par. 42.

[27] A/CONF.234/11, par. 64 à 69.

V. Principaux outils et ressources recommandées

Global Study on Smuggling of Migrants 2018

66. La *Global Study on Smuggling of Migrants 2018*, première étude du genre publiée par l'ONUDC, montre que les itinéraires empruntés pour le trafic illicite de migrants passent par toutes les régions du monde. Elle s'appuie sur l'analyse d'une grande quantité de données et de documents et éclaire sur les tendances qui se dégagent, les itinéraires empruntés pour le trafic illicite de migrants et les profils des passeurs et des migrants qui en sont victimes.

Référentiel d'aide à la lutte contre le trafic illicite de migrants

67. Le *Référentiel d'aide à la lutte contre le trafic illicite de migrants* publié par l'ONUDC fournit des orientations, présente des pratiques prometteuses et recommande des ressources dans différents domaines, le but étant d'aider les pays à appliquer le Protocole relatif au trafic illicite de migrants. Parmi les différents outils que compte le *Référentiel*, l'outil 1 présente de façon générale le trafic illicite de migrants, l'outil 5 établit le cadre législatif permettant d'incriminer cette forme de criminalité, et l'outil 7 porte sur la détection, la répression et les poursuites.

Loi type contre le trafic illicite de migrants

68. La *Loi type contre le trafic illicite de migrants* de l'ONUDC a pour objectif d'aider les États à appliquer le Protocole relatif au trafic illicite de migrants en facilitant l'examen et la modification des législations existantes ainsi que l'adoption de nouvelles lois à partir de dispositions types. Ses différents chapitres portent sur l'incrimination du trafic illicite de migrants, les mesures de protection et d'assistance à l'égard des migrants objet d'un trafic, la coordination et la coopération entre les organismes, la coopération concernant le trafic illicite de migrants en mer et les processus relatifs au retour des migrants objet d'un trafic.

Portail d'information sur le trafic illicite de migrants et base de données sur la jurisprudence

69. En octobre 2016, l'ONUDC a lancé le Portail d'information sur le trafic illicite de migrants, qui constitue un élément de son portail de gestion des connaissances pour la mise en commun de ressources électroniques et de lois contre la criminalité (SHERLOC). Il inclut une base de données sur la jurisprudence, une base de données sur les législations et une bibliographie annotée où figurent des informations sur les principaux articles et publications relatifs au trafic illicite de migrants. La base de données sur la jurisprudence a pour objet de permettre aux juges, aux procureurs, aux responsables politiques, aux médias, aux chercheurs et aux autres parties intéressées d'accroître leurs connaissances sur la façon dont différents États utilisent leurs lois pour combattre le trafic illicite de migrants, l'objectif étant, à terme, d'améliorer l'action de la justice pénale au niveau mondial. Elle constitue un outil essentiel pour donner plus de retentissement aux poursuites qui ont abouti, déceler des tendances à l'échelle mondiale et mieux faire connaître les réalités du trafic illicite de migrants. Elle répertorie actuellement plus de 800 affaires de trafic traitées dans 43 pays. Le Portail d'information est accessible en ligne à l'adresse suivante : https://sherloc.unodc.org/cld/en/v3/som/?lng=fr.

Guides législatifs pour l'application de la Convention des Nations Unies contre la criminalité transnationale organisée et des Protocoles s'y rapportant

70. Les *Guides législatifs pour l'application de la Convention des Nations Unies contre la criminalité transnationale organisée et des Protocoles s'y rapportant* ont pour objet d'aider les États à appliquer la Convention et les Protocoles. On trouve cette publication dans la rubrique « Guides législatifs » du portail de gestion des connaissances SHERLOC.

Cadre d'action international pour l'application du Protocole relatif au trafic illicite de migrants

71. Le *Cadre d'action international pour l'application du Protocole relatif au trafic illicite de migrants* est un outil d'assistance technique destiné à aider les États parties et les acteurs non étatiques à déceler et à combler, conformément aux normes internationales, les lacunes de leur dispositif de lutte contre le trafic illicite de migrants. Il s'appuie sur les instruments internationaux, engagements politiques, lignes directrices et meilleures pratiques déjà adoptés pour proposer une approche globale de l'action à mener pour prévenir et combattre le trafic de migrants. La deuxième partie du *Cadre d'action international* présente, sous forme de quatre tableaux, une vue d'ensemble des questions suivantes : les poursuites et les enquêtes, la protection et l'assistance, la prévention, et la coopération et la coordination.

Séries de modules universitaires Traite des personnes et trafic illicite de migrants et Cybercriminalité de l'initiative Éducation pour la justice

72. Dans le cadre de l'initiative Éducation pour la justice, l'ONUDC a élaboré une série de modules pédagogiques et d'autres outils pour aider le milieu universitaire à dispenser aux étudiants un enseignement sur certaines des menaces les plus graves de l'époque actuelle. Des modules sur la traite des personnes et le trafic illicite de migrants et sur la cybercriminalité ont ainsi été élaborés.