Nations Unies A/CONF.234/11

Quatorzième Congrès des Nations Unies pour la prévention du crime et la justice pénale

Distr. générale
23 janvier 2020
Français
Original : anglais

Kyoto (Japon), 20-27 avril 2020

Point 6 de l'ordre du jour provisoire*
Coopération internationale et assistance technique visant à prévenir et combattre toutes les formes de criminalité

Atelier 4. Les tendances actuelles de la criminalité, les évolutions récentes et les solutions nouvellement apparues, en particulier le recours aux nouvelles technologies pour commettre des actes criminels et lutter contre la criminalité**

Document d'information établi par le Secrétariat

Résumé

Le présent document d'information examine l'impact de la technologie, qui est une arme à double tranchant : elle facilite la criminalité, mais elle contribue aussi à sa prévention, à sa détection et à sa répression. En conséquence, le document adopte une double approche pour expliquer le dualisme fondamental émergent : le rôle de la technologie pour trouver des solutions dans le maintien de l'ordre, les poursuites et les résultats positifs de la justice pénale, d'une part ; et, d'autre part, le rôle plus sombre de la technologie dans l'amélioration des modes opératoires des criminels et des groupes criminels organisés. L'analyse tient compte des développements dans des domaines spécifiques et couvre deux aspects de nature transversale : l'importance de la formation, des approches interdisciplinaires et des synergies de collaboration entre les parties prenantes concernées pour comprendre les avantages actuels des technologies et leur potentiel dans la lutte contre les menaces futures de la criminalité, et la nécessité de prendre dûment en considération les questions éthiques et les garanties de respect des droits de l'homme dans l'utilisation des technologies pour lutter contre la criminalité.

* A/CONF.234/1.

** Le Secrétariat tient à exprimer sa reconnaissance aux instituts du réseau du Programme des Nations Unies pour la prévention du crime et la justice pénale, en particulier l'Institut coréen de criminologie et l'Institut national pour la justice du Ministère de la justice des États-Unis, pour leur aide à la préparation et à l'organisation de l'atelier.

V.20-00549 (F) 180220 190220

I. Introduction

1. En 1997, lorsque le Programme des Nations Unies pour le contrôle international des drogues et le Centre pour la prévention internationale du crime ont fusionné pour former l'Office pour le contrôle des drogues et la prévention du crime, rebaptisé Office des Nations Unies contre la drogue et le crime (ONUDC) en 2002, une version améliorée d'un ordinateur de jeu d'échecs appelé « Deep Blue » est devenue le premier système informatique à battre un champion du monde en titre dans une partie avec contrôles de temps standard d'un tournoi d'échecs. À cette époque, malgré la progression constante de la technologie, la criminalité était encore à relativement « faible technicité » et Internet commençait tout juste à avoir un impact sur la société en tant que technologie essentielle de l'« ère de l'information ».

2. En un peu plus de deux décennies, le développement rapide d'Internet et des technologies de l'information et de la communication a permis la croissance économique et un large accès à des services vitaux, mais a aussi créé de nouvelles opportunités pour les activités criminelles. Les criminels sont devenus les bénéficiaires imprévus des nouvelles technologies et de la mondialisation, car ces évolutions leur ont permis de commettre des crimes et d'en tirer profit en exploitant les activités transnationales et d'étendre leurs activités et commerces illicites sur les plateformes numériques d'une manière qui a réduit les risques, en particulier le risque de détection[1].

3. Par contre, des technologies nouvelles et existantes ouvrent de nouvelles possibilités pour les actions répressives, les enquêtes et les poursuites pénales. L'amélioration de la sûreté publique et l'habilitation des services de détection et de répression et des autorités de justice pénale afin de prévenir et combattre la criminalité grâce aux progrès technologiques peuvent avoir un impact positif sur la réalisation des objectifs du Programme de développement durable à l'horizon 2030, en particulier de l'objectif 16.

4. Dans son rapport intitulé « L'ère de l'interdépendance numérique », le Groupe de haut niveau sur la coopération numérique, créé par le Secrétaire général en 2018 pour renforcer la coopération internationale et multipartite et contribuer au débat public sur un avenir numérique sûr et inclusif pour tous, a aussi mis en évidence les « deux visages de Janus ». Comme indiqué, les technologies numériques ont prouvé qu'elles pouvaient relier les individus par-delà les barrières culturelles et géographiques, favorisant la compréhension et aidant potentiellement les sociétés à devenir plus pacifiques et unies. Cependant, il existe aussi des exemples d'utilisation des technologies numériques pour violer des droits, porter atteinte à la vie privée, polariser les sociétés et inciter à la violence[2].

5. Le présent document d'information s'appuie sur le cadre thématique de l'atelier 4, évoqué dans le guide de discussion du quatorzième Congrès, et l'élargit[3]. Il est structuré en sections distinctes, chacune d'entre elles reflétant les différentes facettes d'une même question centrale : les services de détection et de répression et les autorités de justice pénale sont à la croisée des chemins, en raison d'innovations technologiques rapides qui peuvent non seulement favoriser l'efficacité des services de police et contribuer à remédier aux lacunes traditionnelles des efforts visant à faire respecter pleinement l'état de droit, mais aussi être exploitées à des fins criminelles dans différents domaines[4].

---

[1] Yury Fedotov, « In just two decades, technology has become a cornerstone of criminality », *Huffington Post UK*, 23 octobre 2017.

[2] Voir Nations Unies, « L'ère de l'interdépendance numérique », juin 2019.

[3] A/CONF.234/PM.1, par. 161 à 189.

[4] L'utilisation d'Internet et des technologies numériques à des fins terroristes, ainsi que les questions liées à la cybercriminalité, sont traitées dans le document de travail préparé par le Secrétariat sur le point 6 de l'ordre du jour (A/CONF.234/7).

II La technologie comme outil pour et contre la criminalité

A. Cybermonnaies et actifs virtuels

6. Ces dernières années sont apparus les cybermonnaies et les actifs virtuels, qui ont attiré des investissements dans les infrastructures de paiement basées sur leurs protocoles logiciels[5]. Les utilisateurs de cybermonnaies peuvent les trouver utiles pour diverses raisons, et peuvent aussi détenir de tels actifs en tant qu'investissements spéculatifs. Certains utilisateurs recherchent la confidentialité associée à un niveau d'anonymat plus élevé des transactions, tandis que d'autres veulent simplement éviter la surveillance et/ou le contrôle de l'État ou des banques en ce qui concerne leurs transactions légales[6]. Les partisans des cybermonnaies soulignent que les frais de transaction sont inférieurs à ceux facturés par les banques traditionnelles pour les monnaies nationales, bien que les pertes de change et les frais prélevés par les fournisseurs de services de cybermonnaies puissent diminuer les économies réalisées[7]. Là où les banques traditionnelles ne sont pas disponibles, les cybermonnaies peuvent offrir la fonctionnalité associée aux services de paiement traditionnels[8]. Enfin, comme une cybermonnaie n'est généralement pas une monnaie d'État, elle peut faciliter les transactions transfrontalières[9].

7. Néanmoins, de nombreux pays qui autorisent le fonctionnement de marchés des cybermonnaies ont promulgué des lois pour empêcher le blanchiment d'argent, la criminalité organisée et le financement du terrorisme[10], bien qu'à ce jour, il ne semble pas y avoir d'utilisation à grande échelle des cybermonnaies par les terroristes[11]. Cette tendance à la réglementation est apparue en réaction à l'utilisation fréquente de cybermonnaies pour effectuer des achats illégaux et sur le marché noir en ligne[12] et comme méthode de paiement dans les cas de blanchiment d'argent, de combines à la Ponzi, d'extorsion, de chantage [menace d'attaques par dénis de service distribués (DDOS)] et de fraude.

8. Les mêmes concepts qui s'appliquent au blanchiment d'argent en espèces peuvent s'appliquer au blanchiment d'argent en cybermonnaies[13]. Le blanchiment d'argent impliquant une cybermonnaie se fait selon un processus similaire à celui du blanchiment d'argent traditionnel, mais avec un recours à la technologie pour blanchir

---

[5] Sesha Kethineni et Yin Cao, « The rise in popularity of cryptocurrency and associated criminal activity », *International Criminal Justice Review*, 6 février 2019 ; Stearns Broadhead, « The contemporary cybercrime ecosystem: a multi-disciplinary overview of the state of affairs and developments », *Computer Law and Security Review*, vol. 34, nº 6 (décembre 2018), p. 1180 à 1196.

[6] Geoff Goodell et Tomaso Aste, « Can cryptocurrencies preserve privacy and comply with regulations? », *Frontiers in Blockchain*, vol. 2, art. 4 (mai 2019), p. 1 à 20.

[7] Angela S. M. Irwin et Adam B. Turner, « Illicit Bitcoin transactions: challenges in getting to the who, what, when and where », *Journal of Money Laundering Control*, vol. 21, nº 3 (juillet 2018), p. 297 à 313.

[8] Ibid.

[9] Perri Reynolds et Angela S. M. Irwin, « Tracking digital footprints: anonymity within the bitcoin system » , *Journal of Money Laundering Control*, vol. 20, nº 2 (mai 2017), p. 172 à 189.

[10] États-Unis, Law Library of Congress, Global Legal Research Center, *Regulation of Cryptocurrency around the World* (Washington, D.C., 2018), juin 2018.

[11] Cynthia Dion-Schwarz, David Manheim et Patrick B. Johnson, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Monica, Californie, RAND Corporation, 2019).

[12] Reynolds et Irwin, « Tracking digital footprints »; Monica J. Barratt, Jason A. Ferris et Adam R. Winstock, « Safer scoring? Cryptomarkets, social supply and drug market violence », *International Journal of Drug Policy*, vol. 35 (septembre 2016) p. 24 à 31.

[13] Chad Albrecht *et al.*, « The use of cryptocurrencies in the money laundering process », *Journal of Money Laundering Control*, vol. 22, nº 2 (mai 2019), p. 210 à 216; Rolf van Wegberg, Jan-Jaap Oerlemans et Oskar van Deventer, « Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin », *Journal of Financial Crime*, vol. 25, nº 2 (juin 2018), p. 419 à 435.

l'argent[14]. En outre, les cybermonnaies pourraient être utilisées pour faciliter la fraude fiscale[15].

9. Le vol de cybermonnaies est aussi une préoccupation croissante[16]. Les utilisateurs de cybermonnaies peuvent être la proie d'escroqueries visant à les leur voler[17]. De plus, les attaques par logiciel rançonneur contre des particuliers, des entreprises ou des gouvernements sont souvent assorties d'extorsions de fonds à payer en cybermonnaie.

10. La criminalité impliquant des cybermonnaies est facilitée dans les environnements où les réglementations sont insuffisantes pour permettre l'identification des utilisateurs ou imposer des sanctions, et où des lacunes réglementaires peuvent être exploitées. Les différences entre les réglementations sur les cybermonnaies dans les différents pays permettent aux utilisateurs de mener dans un pays une activité qui est illégale ailleurs[18].

11. Un certain nombre d'actions doivent être envisagées et menées pour empêcher l'utilisation des cybermonnaies à des fins criminelles. Les approches visant à lever l'anonymat sur les transactions peuvent étayer les fonctions de dissuasion et d'enquête. Il peut s'agir de réglementations exigeant des informations d'identification (règles de « connaissance du client »)[19] ou l'analyse des transactions à l'aide de l'apprentissage automatique ou d'autres techniques de surveillance pour identifier les transactions illégales[20].

12. Les connaissances et les compétences limitées pour identifier les systèmes de cybermonnaies ou enquêter efficacement sur eux ouvrent la voie à des possibilités élargies d'utilisation de ces monnaies pour des activités illicites[21]. Des efforts tels que ceux entrepris par l'Organisation des Nations Unies pour former les enquêteurs à la criminalité liée aux cybermonnaies contribuent à la prévention et à l'identification de ces activités[22].

13. Les émetteurs de cybermonnaies, les régulateurs et les services de détection et de répression sont des acteurs clefs pour ce qui est d'empêcher l'utilisation des cybermonnaies au service de la criminalité. Il est important d'élaborer un ensemble solide de techniques de prévention et d'enquête pouvant être adaptées à l'évolution de la technologie et aux diverses applications des cybermonnaies afin de réduire le plus possible les menaces liées à leur utilisation criminelle.

---

[14] Denis B. Desmond, David Lacey et Paul Salmon, « Evaluating cryptocurrency laundering as a complex socio-technical system: a systematic literature review », *Journal of Money Laundering Control*, vol. 22, nº 3 (juillet 2019), p. 480 à 497.

[15] Albrecht *et al.*, « The use of cryptocurrencies in the money laundering process »; Saman Jafari *et al.*, « Cryptocurrency: a challenge to legal system », 10 mai 2018.

[16] Garrick Hileman et Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (Cambridge, United Kingdom of Great Britain and Northern Ireland, Cambridge Centre for Alternative Finance, 2017).

[17] Desmond *et al.*, « Evaluating cryptocurrency laundering as a complex socio-technical system ».

[18] Angela S. M. Irwin et Caitlin Dawson, « Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help », *Journal of Money Laundering Control*, vol. 22, nº 1 (janvier 2019) p. 110 à 131.

[19] Groupe d'action financière, *Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération : Les recommandations du GAFI* (Paris, 2016).

[20] Irwin et Turner, « Illicit Bitcoin transactions »; Goodell et Aste, « Can cryptocurrencies preserve privacy and comply with regulations? ».

[21] Sesha Kethineni, Yin Cao et Cassandra Dodge, « Use of Bitcoin in darknet markets: examining facilitative factors on Bitcoin-related crimes », *American Journal of Criminal Justice*, vol. 43, nº 2 (juin 2018) p. 141 à 157.

[22] Office des Nations Unies contre la drogue et le crime (ONUDC), « UNODC launches training to tackle cryptocurrency-enabled organized crime », 8 mai 2017.

B. La technologie et les marchés du darknet, y compris les marchés de la drogue

14. Internet ouvre de nouvelles possibilités de vente et d'achat illicites de marchandises, tant par le biais de l'Internet classique que de l'Internet sombre. Contrairement à l'Internet classique (aussi appelé « Internet surfacique »), qui contient des informations accessibles par le public et indexées par les moteurs de recherche courants, l'Internet sombre (ou darknet, les termes sont utilisés de manière interchangeable ci-après) est constitué de réseaux cryptés, ce qui permet aux propriétaires et aux utilisateurs des sites de rester relativement anonymes et intraçables[23].

15. Les marchés du darknet (aussi appelés « cryptomarchés »)[24] assurent l'anonymat des acheteurs et des vendeurs, et ce sont surtout les cybermonnaies qui sont utilisées pour le paiement sur ces marchés afin de faciliter le commerce de biens tels que les armes et les drogues illicites.

16. Selon l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), les données personnelles, médicales et financières compromises sont une denrée essentielle sur les marchés du darknet et jouent un rôle crucial dans des activités telles que les fraudes, le hameçonnage, l'usurpation d'identité et la prise de contrôle de comptes. Toutefois, si les marchés du darknet proposent à la vente toute une série de produits contrefaits et piratés, la majeure partie du commerce illicite se fait encore sur le web surfacique[25]. Les matchs truqués et les jeux d'argent sont de plus en plus utilisés sur l'Internet sombre pour soutenir les circuits de blanchiment d'argent, en particulier par les groupes criminels transnationaux organisés[26]. La Réunion régionale pour l'Europe préparatoire au quatorzième Congrès a aussi souligné la nécessité de s'attaquer à l'utilisation du darknet pour la commission de crimes de haine[27].

17. Dans le domaine des drogues, le *Rapport mondial sur les drogues 2019* indique que les achats de drogues sur le darknet augmentent à long terme, bien qu'ils aient pu diminuer de 2018 à 2019. Les données de l'enquête mondiale sur les drogues de 2019 suggèrent que l'achat de drogues via le darknet est encore un phénomène très récent, 48 % des personnes ayant déclaré avoir acheté des drogues via le darknet en 2019 ayant commencé à utiliser le darknet à cette fin au cours des deux dernières années, et 29 % de plus au cours des deux années précédentes[28].

18. Les marchés de la drogue du darknet pourraient déclencher des changements dans les schémas et la prévalence de la consommation de drogues[29] car ils peuvent réduire certains risques pour les acheteurs et les vendeurs, comme les rencontres violentes dans les quartiers où se déroulent les ventes de drogues[30], la coercition et

---

[23] Darren Guccione, « What is the dark web? How to access it and what you'll find », *The State of Cybersecurity*, 4 juillet 2019.

[24] Julian Broseus *et al.*, « Studying illicit drug trafficking on Darknet markets: structure and organization from a Canadian perspective », *Forensic Science International*, vol. 264, 5 mars 2016, p. 7.

[25] European Union Agency for Law Enforcement Cooperation (Europol), European Cybercrime Centre, *Internet Organised Crime Threat Assessment (IOCTA) 2018* (La Haye, 2018), p. 49.

[26] Robin Cartwright et France Cleland Bones, *Transnational Organized Crime and the Impact on the Private Sector: The Hidden Battalions* (Genève, Global Initiative against Transnational Organized Crime, 2017), p. 29.

[27] Voir A/CONF.234/RPM.5/1, par. 36 g).

[28] *Rapport mondial sur les drogues 2019* : *Tableau général de la demande et de l'offre de drogues [publication des Nations Unies*, numéro de vente : E.19.XI.8 (Fascicule 2)].

[29] Judith Aldridge et David Décary-Hétu, « Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets », *International Journal of Drug Policy*, vol. 35, septembre 2016, p. 12.

[30] Julia Buxton et Tim Bingham, *The Rise and Challenge of Dark Net Drug Markets*, Policy brief, nº 7 (Swansea, United Kingdom, Global Drug Policy Observatory, janvier 2015) p. 1 à 24.

l'arrestation[31]. Cependant, la vente de drogues par Internet comporte ses propres risques. Les risques les plus importants sont susceptibles de se produire lors des activités « hors ligne » connexes[32]. Les ventes de drogues par Internet peuvent aussi être liées à l'augmentation des surdoses dans la mesure où elles facilitent l'expérimentation et la disponibilité de drogues plus puissantes[33].

19. Des succès notables ont été enregistrés dans le démantèlement de grands marchés du darknet. Selon Europol, cependant, les criminels explorent d'autres moyens de contourner les mesures répressives. Une nouvelle tendance est l'émergence de modèles commerciaux dans lesquels les criminels utilisent des identités multiples, en recourant à des profils multiples sur différentes plateformes en ligne, ce qui facilite l'intervention de plusieurs personnes plutôt que d'une seule[34].

20. La conduite d'enquêtes sur le darknet présente un certain nombre de difficultés. Un problème majeur est que les informations du darknet n'étant pas indexées, les enquêteurs ne peuvent pas facilement les localiser à l'aide de moteurs de recherche ou de mots-clefs. En outre, les criminels utilisent des plateformes décentralisées pour l'hébergement de leurs serveurs web, ce qui permet une prolifération de services qui peuvent être plus difficiles à détecter[35].

21. Par contre, les services de détection et de répression ont des possibilités de surveiller les marchés du darknet et de mener des enquêtes en ligne[36]. Dans ce contexte, un ensemble d'outils peut fournir des solutions, notamment des robots Web qui peuvent servir à automatiser l'indexation des données en ligne de manière récurrente, des outils d'exploration de données pour l'analyse d'énormes ensembles de données, des outils d'analyse cybermonétaire pour suivre le flux des paiements et des logiciels de chaîne de blocs utilisés pour le suivi des preuves[37]. L'assistance technique est importante et l'ONUDC a participé activement à des activités de formation axées sur les techniques d'enquête pour le darknet.

C. Armes à feu : menaces pour la sécurité liées à la technologie

1. Les technopolymères dans la fabrication des armes à feu

22. Les polymères industriels sont appelés à jouer un rôle de plus en plus dominant dans l'industrie de l'armement, ce qui pose des problèmes pour la mise en œuvre effective des dispositions relatives au traçage et à l'enregistrement des armes à feu contenues dans le Protocole contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée. Cette apparition de polymères industriels compromet la capacité des autorités compétentes de détecter, d'enquêter et de poursuivre de manière adéquate en ce qui concerne les délits connexes.

---

[31] Buxton et Bingham, *The Rise and Challenge of Dark Net Drug Markets*. Voir aussi David Décary-Hétu, Masarah Paquet-Clouston et Judith Aldridge, « Going international? Risk taking by cryptomarket drug vendors », *International Journal of Drug Policy*, vol. 35, septembre 2016, p. 71.

[32] Judith Aldridge et Rebecca Askew, « Delivery dilemmas: how drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement », *International Journal of Drug Policy*, vol. 41, mars 2017 p. 101 à 109.

[33] Nathaniel Popper, « Opioid dealers embrace the dark web to send deadly drugs by mail », *New York Times*, 10 juin 2017.

[34] Europol, European Cybercrime Centre, *Internet Organised Crime Threat Assessment* (IOCTA) 2019 (La Haye, 2019), p. 45.

[35] International Criminal Police Organization (INTERPOL) « Innovation report: anonymous networks and darknet » (septembre 2018) p. 12 à 13.

[36] European Monitoring Centre for Drugs and Drug Addiction and Europol, *Drugs and the Darknet: Perspectives for Enforcement, Research and Policy* (Luxembourg, 2017), p. 60 et suiv.

[37] INTERPOL, « Innovation report », p. 14. Voir aussi Shira Stein, « Law enforcement adapts to using cryptocurrency to catch criminals », *Securities Regulation and Law Report*, 49 SRLR 1029 (Arlington, Virginie, Bureau of National Affairs, 2017).

23. Le Recueil de modules concernant la maîtrise des armes légères (MOSAIC) – recueil de bonnes pratiques non contraignantes en matière de maîtrise des armes légères qui s'appuie sur l'acquis des instruments internationaux pertinents : Protocole relatif aux armes à feu, Programme d'action sur les armes légères et Instrument international de traçage connexe, et Traité sur le commerce des armes – peut aider les pays à relever les défis posés par les boîtiers de culasse en polymère.

2. Armes modulaires

24. Les nouvelles technologies et les lacunes législatives existantes ont eu pour effet d'inonder les marchés licites et illicites de trousses de modification, de conversion et de fabrication qui permettent aux propriétaires d'armes à feu, avec un minimum de connaissances techniques, de transformer leurs armes ou même de produire des armes complètement fonctionnelles.

25. Le Protocole relatif aux armes à feu s'applique aux « pièces et éléments », mais ses dispositions en matière de marquage (art. 8) ne s'appliquent qu'aux « armes à feu ». Cela peut être particulièrement problématique en ce qui concerne les armes modulaires[38]. Pour résoudre ce problème, il peut être nécessaire de prendre des mesures telles que l'identification d'un élément de contrôle pour toutes les armes à feu, qu'elles soient standard ou modulaires, à des fins de marquage, d'enregistrement et de traçage ; la détermination des informations qui doivent être marquées sur l'élément de contrôle pour éviter la duplication des numéros de série ; et la fourniture d'orientations sur l'identification unique à des fins de traçage, en particulier pour les armes modulaires[39].

3. Fabrication additive (impression 3D)

26. La fabrication additive – familièrement appelée impression tridimensionnelle, ou impression 3D – est une technologie émergente qui peut avoir des incidences locales, nationales et internationales sur la sécurité à court et à long terme. Le développement et la diffusion de la fabrication additive pourraient accélérer considérablement la prolifération des armes et avoir des conséquences dramatiques sur la criminalité quotidienne. En outre, les armes à feu imprimées en 3D peuvent avoir un impact négatif sur l'efficacité des systèmes d'enregistrement et de licence des armes à feu et sur celle des bases de données balistiques utilisées pour les enquêtes de police.

27. L'article 3 d) et l'alinéa 1 a) de l'article 5 du Protocole relatif aux armes à feu, concernant la fabrication illicite d'armes à feu, s'appliqueraient aux armes à feu produites par impression 3D de la même manière qu'ils s'appliquent aux armes à feu fabriquées de façon traditionnelle. Toutefois, le téléchargement de fichiers numériques pour l'impression 3D des armes à feu semble sortir du champ d'application du Protocole, situation qui exige des réponses législatives urgentes.

28. De nombreuses lois et infractions existantes concernant la fabrication, la création et la possession d'armes à feu sans licence couvrent les armes à feu imprimées en 3D, mais pas nécessairement la possession ou la distribution des fichiers de conception[40]. Il se peut que les lois relatives à la fabrication illicite d'armes à feu doivent contenir des dispositions sur la culpabilité de tiers dans les cas où des outils

---

[38] Giacomo Persi Paoli, « From firearms to weapon systems: challenges and implications of modular design for marking, record-keeping, and tracing », in *Behind the Curve: New Technologies, New Control Challenges*, Occasional paper of the Small Arms Survey, n° 32, Benjamin King et Glenn McDonald, éd. (Genève, Small Arms Survey, 2015), p. 23.

[39] Ibid., p. 40.

[40] INTERPOL Innovation Paper, « 3D and 4D printing », INTERPOL Global Complex for Innovation, 2018, p. 6.

sont mis à la disposition de personnes qui peuvent souhaiter produire des armes à feu en utilisant des techniques de fabrication additive[41].

29. Une approche réglementaire globale devrait inclure les acteurs nationaux et internationaux, ainsi que les secteurs public et privé. Le double usage potentiel de la fabrication additive fait qu'il est impossible de limiter la diffusion de cette technologie sans en réduire également les nombreux avantages[42]. Comme pour toute technologie émergente, il sera important de prévoir la formation théorique et pratique du personnel des services de détection et de répression.

4. Le trafic des armes à feu sur l'Internet sombre

30. L'Internet sombre a le potentiel de devenir une plateforme de choix pour les groupes criminels organisés et les individus qui veulent acheter des armes à feu de manière anonyme ou à des fins illégales[43]. En réponse à une étude présentée par le Bureau des affaires de désarmement de l'Organisation des Nations Unies à la Première Commission de l'Assemblée générale en 2018, préparée sur la base d'un projet de recherche plus vaste mené par RAND Europe en 2017[44], il a été constaté qu'il y avait un besoin urgent d'une nouvelle coopération internationale pour lutter contre les ventes d'armes illicites rendues possibles par l'anonymat de l'Internet sombre[45].

31. La proportion des ventes d'armes qui ont lieu sur l'Internet sombre semble être plus faible que celle des autres articles illicites[46]. Une étude récente portant uniquement sur les listes relatives aux armes sur l'Internet sombre a révélé que les listes d'armes à feu étaient les plus courantes, représentant 42 % de toutes les listes sur l'Internet sombre, suivies par les produits numériques liés aux armes à 27 %, et par d'autres produits tels que les munitions à 22 %[47].

32. Il est essentiel de comprendre l'ampleur et la portée du commerce illicite d'armes sur l'Internet sombre pour mieux cerner la gravité de la menace et les incidences pour les services de détection et de répression. Au niveau national, les décideurs doivent veiller à ce que les services de détection et de répression soient dotés du personnel, de la formation et de l'équipement dont ils ont besoin pour résoudre les problèmes connexes. Les cadres juridiques internationaux existants, en particulier la Convention contre la criminalité organisée et son Protocole relatif aux armes à feu, peuvent servir de base à des approches globales pour lutter contre ce phénomène. Une analyse approfondie est nécessaire pour déterminer si les réglementations existantes en matière de courtage, prévues par le Protocole relatif aux armes à feu (art. 15) et le Traité sur le commerce des armes (art. 10), seraient applicables[48].

---

[41] N. R. Jenzen-Jones, « Small arms and additive manufacturing: An assessment of 3D-printed firearms, components, and accessories », in *Behind the Curve: New Technologies, New Control Challenges*, Occasional paper of the Small Arms Survey, nº 32, Benjamin King et Glenn McDonald, éd. (Genève, Small Arms Survey, 2015) p. 63 et 64.

[42] Trevor Johnston, Troy D. Smith et J. Luke Irwin, « Additive manufacturing in 2040: powerful enabler, disruptive threat », document nº PE-283-RC (Santa Monica, Californie, RAND Corporation, 2018), p. 17.

[43] RAND Europe, « International arms trade on the dark web » (2019), Findings section, par. 8.

[44] Giacomo Persi Paoli *et al.*, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, Californie, RAND Corporation, 2017).

[45] Giacomo Persi Paoli, *The Trade in Small Arms and Light Weapons on the Dark Web*, United Nations Office for Disarmament Affairs (UNODA) Occasional Papers, nº 32 (United Nations publications, Sales nº E.19.XI.1), p. ix.

[46] Damien Rhumorbarbe *et al.*, « Characterising the online weapons trafficking on cryptomarkets », *Forensic Science International*, vol. 283, décembre 2018, p. 16 et 20

[47] RAND Europe, « International arms trade on the dark web » (2019), Findings section, par. 4.

[48] Simonetta Grassi et Mareike Buettner, « Annex: overview of international legal instruments and their applicability to illicit firearms trafficking on the dark web », in Paoli *et al.*, *Behind the Curtain*, p. 101.

5. Armes létales autonomes

33. Bien qu'il n'y ait pas de reconnaissance officielle de l'existence d'armes totalement autonomes, l'idée d'utiliser l'intelligence artificielle pour contrôler de telles armes a suscité de vifs débats. En 2016, la cinquième Conférence des Hautes Parties contractantes chargée de l'examen de la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination a créé le Groupe d'experts gouvernementaux sur les technologies émergentes dans le domaine des systèmes d'armes létaux autonomes. Lors de sa session de 2019, le Groupe a recommandé que les Hautes Parties contractantes approuvent les principes directeurs qu'il avait affirmés[49].

D. Traite des personnes

34. Des recherches menées ces dernières années et des preuves directes montrent que la technologie est utilisée par les trafiquants d'êtres humains à tous les stades du crime, y compris le recrutement, le contrôle et l'exploitation des victimes.

35. L'une des raisons pour lesquelles la technologie est exploitée par les trafiquants est qu'elle leur permet d'opérer de manière anonyme et de dissimuler leur identité. En outre, les cybermonnaies permettent aux trafiquants de réaliser des transactions financières et de faire circuler les produits du crime de manière anonyme. Une autre raison est que la technologie facilite le recrutement et l'exploitation des victimes par les trafiquants. Les petites annonces en ligne et les sites de réseautage social peuvent être utilisés comme « canaux de la traite des êtres humains »[50].

36. En outre, l'utilisation abusive de la technologie peut permettre aux trafiquants d'effectuer plus facilement des transactions avec les utilisateurs, de pénétrer de nouveaux marchés et d'étendre leurs activités criminelles. Les trafiquants peuvent utiliser la diffusion en direct pour atteindre un marché plus large de clients qui n'auront peut-être jamais de contact physique avec la victime[51].

37. En outre, l'utilisation abusive des technologies peut aider les trafiquants à contrôler et à contraindre les victimes. Les trafiquants peuvent tirer parti des dispositifs de localisation pour faciliter l'exploitation des victimes. Même lorsque les victimes ont échappé à l'emprise des trafiquants, elles peuvent encore être suivies si les agresseurs découvrent où elles se trouvent grâce aux systèmes de localisation de leurs téléphones portables.

38. Par contre, les services de détection et de répression utilisent déjà le suivi de localisation pour détecter la position de présumés trafiquants ou d'autres individus participant à la traite. L'utilisation des données de localisation des victimes est l'autre face de la même médaille, étant donné que les victimes peuvent être traitées comme des « bases de preuves ambulantes »[52].

39. L'utilisation d'interventions technologiques dans la lutte contre la traite des êtres humains nécessite une collaboration entre les secteurs. L'industrie des technologies de l'information et de la communication et des organisations internationales se sont associées pour étudier comment les technologies peuvent être exploitées pour prévenir la traite des personnes et soutenir la réhabilitation des victimes. Tech Against Trafficking, coalition de grandes entreprises technologiques,

---

[49] CCW/GGE.1/2019/3, annexe IV.

[50] Mark Latonero, *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*, Centre on Communication Leadership and Policy Research Series (Los Angeles, University of Southern California, septembre 2011), p. 8.

[51] Groupe interinstitutions de coordination contre la traite des personnes, « Human trafficking and technology: trends, challenges and opportunities », Issue brief, n° 7 (2019), p. 1 et 2.

[52] Felicity Gerry, Julia Muraszkiewicz et Niovi Vavoula, « The role of technology in the fight against human trafficking: reflections on privacy and data protection concerns », *Computer Law and Security Review*, vol. 32, n° 2 (avril 2016), p. 210 et 211.

d'établissements universitaires et de l'Organisation internationale pour les migrations, fournit une liste de solutions technologiques utilisées pour lutter contre la traite des êtres humains[53].

40. Le renforcement des capacités de tous les acteurs concernés est essentiel pour relever les défis posés par l'utilisation de la technologie pour la traite des personnes. Il convient de réfléchir attentivement au développement, à l'utilisation, à la maintenance, au suivi et à l'évaluation des technologies utilisées par les praticiens pour lutter contre la traite des personnes[54]. Toutefois, les concepteurs d'outils pertinents doivent anticiper et prendre en compte les différences qui existent entre les utilisateurs qui risquent d'être victimes de la traite[55].

E. Trafic illicite de migrants

41. Les technologies de l'information et de la communication sont devenues des outils importants, largement utilisés tant par les migrants que par les passeurs pour transmettre des informations sur les itinéraires, les services et les prix[56]. En outre, les médias sociaux permettent aux trafiquants d'être plus à même de modifier les itinéraires de trafic en fonction des mesures prises par les services de détection et de répression dans les pays de transit, ce qui contribue à accroître l'efficacité des opérations de trafic et à entraver tant la conduite des enquêtes sur ce type d'infractions que les poursuites contre leurs auteurs[57].

42. Le développement rapide de la technologie mobile est susceptible d'avoir des incidences sur les relations entre migrants et passeurs. Grâce à plusieurs groupes Facebook, les migrants peuvent vérifier la fiabilité de certains passeurs et échanger des informations sur les personnes les plus sûres à contacter. Ce phénomène est décrit comme une « hiérarchie de la fiabilité »[58].

43. Les technologies pourraient également être utilisées pour procéder au paiement. En effet, les passeurs sont essentiellement rémunérés au moyen de systèmes de paiement en ligne. Les cybermonnaies peuvent aider les passeurs à recevoir, dissimuler et transférer de l'argent plus aisément. Elles peuvent 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.

44. La technologie joue en outre un rôle majeur dans la production de faux documents de voyage ou d'identité qui facilitent le trafic de migrants. Divers équipements sont utilisés pour produire, modifier ou copier des passeports de manière frauduleuse. Dans certains cas, des outils à la pointe de la technologie sont utilisés pour créer des faux de qualité (passeports « miroirs »)[59].

45. Cependant, les innovations technologiques peuvent être envisagées sous de multiples angles et ne pas être uniquement associées aux avantages qu'elles offrent

---

[53] Business for Social Responsibility, « List of technology tools and initiatives identified by tech against trafficking », 15 janvier 2019.

[54] Groupe interinstitutions de coordination contre la traite des personnes, « Human trafficking and technology », p. 4.

[55] Voir Mark Latonero, Bronwyn Wex et Meredith Dank, *Technology and Labor Trafficking in a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study* (Los Angeles, University of Southern California, Annenberg Center on Communication Leadership and Policy, 2015), p. 11.

[56] Europol et INTERPOL, « Migrant smuggling networks: executive summary » (mai 2016), p. 8.

[57] CTOC/COP/WG.7/2018/2, par. 25.

[58] Judith Zijlstra et Ilse van Liempt, « Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys », *International Journal of Migration and Border Studies*, vol. 3, nº 2 et 3 (mars 2017), p. 176 et 177.

[59] Bureau régional pour l'Asie du Sud-Est et le Pacifique de l'ONUDC, *Facilitators of Smuggling of Migrants in Southeast Asia: Fraudulent Documents, Money Laundering, and Corruption* (Bangkok, 2019), p. 26.

aux passeurs. La numérisation atténue également les lacunes en matière d'information sur lesquelles les passeurs peuvent s'appuyer pour faire fructifier leurs activités. Internet peut permettre aux migrants de se connecter à des réseaux sociaux de soutien et d'information. Une tendance récente née de l'évolution technologique tient au fait que de plus en plus de migrants sont autonomes tout au long du processus migratoire et dépendent donc moins des passeurs, ce qui leur confère une plus grande indépendance et les rend moins vulnérables à l'exploitation[60].

46. La manière dont les migrants utilisent les médias sociaux diffère selon leur nationalité, leur appartenance ethnique, leur région d'origine et leur niveau d'éducation, ainsi que leur accès à Internet[61]. Selon diverses études, il existe une fracture numérique entre les différents groupes de migrants, qui découle des inégalités en matière d'accès à la technologie numérique et d'utilisation de cette technologie, des compétences nécessaires pour exploiter efficacement les différentes technologies et de la capacité à payer ces services[62].

47. Dans le domaine de la détection et de la répression, la recherche de moyens d'exploitation de la technologie en vue de mettre à mal les réseaux de trafic illicite de migrants suscite un intérêt croissant. En outre, le recours à des éléments de preuve obtenus au moyen des médias sociaux ou de la technologie peut étayer les témoignages des migrants victimes de trafic recueillis dans le cadre de procédures pénales.

48. Lorsqu'elle est exploitée de manière adaptée, la technologie aide les pouvoirs publics, le secteur privé et les organisations non gouvernementales à prévenir et à limiter le trafic illicite de migrants, dans leurs domaines de compétence respectifs. C'est pourquoi il est primordial de renforcer l'efficacité des mesures de justice pénale et de mettre en place des mesures incitatives et des partenariats pour encourager les prestataires de services en ligne à améliorer la surveillance, la détection et le signalement des contenus liés au trafic illicite de migrants.

F. Abus et exploitation des enfants en ligne

49. Bien que l'exploitation et les atteintes sexuelles visant les enfants avaient cours avant l'avènement d'Internet, le caractère numérique que revêtent désormais ces infractions permet à leurs auteurs de communiquer entre eux et d'obtenir des images d'abus pédosexuels en ligne. Par ailleurs, le fait que de plus en plus de jeunes enfants ont accès à Internet donne aux délinquants la possibilité d'entrer en contact plus facilement avec eux (par rapport au monde réel), ce qui a de fortes répercussions sur les modes opératoires auxquels les auteurs de ces infractions ont recours.

50. Les avancées technologiques jouent un rôle déterminant dans l'exploitation sexuelle des enfants à des fins commerciales. Les touristes pédophiles peuvent recourir à l'informatique en nuage pour stocker des images ou des vidéos et éviter ainsi les risques liés au transport physique d'images d'abus pédosexuels. En outre, la téléphonie mobile met en relation les entremetteurs, les victimes et les auteurs d'exploitation et d'abus sexuels d'enfants, ce qui évite non seulement aux producteurs et aux distributeurs de ce type d'images d'être physiquement présents lors des transactions, mais réduit également leurs risques de se faire repérer.

---

[60] ONUDC, Déclaration de Doha, Supérieur, Éducation pour la justice, Série de modules universitaires, Traite des personnes et trafic illicite de migrants, « Module 14 : Liens entre la cybercriminalité, le trafic illicite de migrants et la traite des personnes – Technologie et trafic illicite de migrants ». Disponible à l'adresse suivante : www.unodc.org/e4j/fr/index.html.

[61] Commission européenne, « The use of social media in the fight against migrant smuggling », fiche d'information du réseau européen des migrations (REM) (septembre 2016).

[62] Alam Khorshed et Sophia Imran, « The digital divide and social inclusion among refugee migrants: a case in regional Australia », *Information Technology and People*, vol. 28, nº 2 (juin 2015), p. 344 ff.

51. Les principales formes d'abus et d'exploitation d'enfants facilitées par les technologies de l'information et de la communication comprennent l'exposition à la pornographie, la sollicitation sur Internet à des fins sexuelles et les demandes à caractère sexuel non désirées sur Internet. Nombre de ces actes d'exploitation concernent des activités sexuelles inappropriées impliquant des enfants. Dans une étude sur la question, l'ONUDC attire l'attention sur les nouvelles formes d'abus et d'exploitation des enfants, telles que les contenus générés par les utilisateurs, les contenus auto-générés, y compris la textopornographie, la diffusion d'abus sexuels en direct et les images d'abus pédosexuels générées à la demande[63].

52. Selon Europol, la diffusion d'abus sexuels en direct constitue désormais une menace établie, qui se déroule sur les médias sociaux, les chats vidéo, les plateformes de jeux et les forums de discussion en ligne. En outre, il semble que l'ordinateur soit progressivement remplacé par les smartphones et les tablettes, de même que l'accès à Internet via une connexion Wi-Fi ou mobile supplée l'Internet par câble[64].

53. Le recours de plus en plus fréquent au darknet constitue l'une des principales menaces concernant la distribution en ligne d'images d'abus pédosexuels. Selon la Internet Watch Foundation, les sites Web masqués dotés d'une « passerelle numérique » pour dissimuler des images d'abus pédosexuels demeurent un problème majeur. En outre, la fondation a constaté une augmentation constante au cours des dernières années du nombre d'adresses de sites Web montrant des abus sexuels d'enfants, dont le nombre est passé de 68 092 en 2015 à 105 047 en 2018[65].

54. De plus, à mesure que les délinquants pédosexuels qui sévissent en ligne auront recours à des moyens techniques plus complexes, ils continueront de chercher de nouvelles façons d'éviter de se faire repérer. Les grands forums ont récemment été délaissés au profit de petits groupes d'utilisateurs, dont la constitution est facilitée par les applications de messagerie mobile qui permettent d'encoder l'ensemble des conversations.

55. L'absence, dans un certain nombre de pays, de dispositions légales permettant de réglementer les nouvelles formes d'abus des enfants, ainsi que les disparités entre les lois destinées à protéger les enfants et celles fixant l'âge du consentement posent de graves problèmes et entravent le bon déroulement des activités de détection, des enquêtes et des poursuites.

56. La technologie peut aussi offrir aux services de détection et de répression les moyens de lutter contre les problèmes qui y sont liés[66]. Les méthodes et techniques novatrices, telles que l'exploration et l'analyse des données, améliorent le processus criminalistique et facilitent ainsi la conduite des enquêtes. Il convient de recourir aux techniques qui s'appuient sur la technologie de l'information en respectant les droits de la personne, compte tenu de la nature traumatisante de l'exploitation sexuelle des enfants et de l'âge et de la vulnérabilité des victimes.

57. Des bases de données, comme la base de données internationale sur l'exploitation sexuelle des enfants de l'Organisation internationale de police criminelle (INTERPOL), ont également été créées afin de télécharger des images d'abus pédosexuels pour les besoins des enquêtes. Aux États-Unis d'Amérique, la base de données du National Center for Missing and Exploited Children (Centre national pour les enfants disparus et exploités) sert à centraliser ce type d'images[67].

---

[63] ONUDC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienne, 2015), p. 21 ff.

[64] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, p. 35.

[65] Internet Watch Foundation, *Once Upon a Year* (Cambridge, Royaume-Uni, 2018), p. 19 et 43.

[66] Victoria Brains, « Online child sexual exploitation: towards an optimal international response », *SSRN Electronic Journal*, 29 août 2018.

[67] ONUDC, Déclaration de Doha, Supérieur, Éducation pour la justice, Série de modules universitaires, Cybercriminalité, « Module 12 : Cybercriminalité interpersonnelle – Exploitation et abus sexuels d'enfants en ligne ». Disponible à l'adresse suivante : www.unodc.org/e4j/fr/index.html.

58. Les efforts visant à lutter efficacement contre l'exploitation et les abus d'enfants facilités par les technologies de l'information et de la communication nécessitent l'adoption d'une approche multipartite prévoyant la participation active des enfants, des familles, des collectivités, des pouvoirs publics, de la société civile et du secteur privé[68].

G. Intelligence artificielle et robotique

59. Après l'avènement de la « troisième révolution industrielle » grâce à l'apparition d'Internet et de la technologie mobile, les technologies de l'intelligence artificielle, sous-tendues par les mégadonnées[69], sont à l'origine d'une « quatrième révolution industrielle ». Si cette évolution est susceptible de présenter un intérêt pour le développement mondial et la transformation de la société et contribuer à la réalisation des objectifs de développement durable, elle laisse néanmoins apparaître des préoccupations et des défis d'ordre juridique, éthique et sociétal. S'agissant de détection et de répression, les avancées de l'intelligence artificielle peuvent être synonymes à la fois de possibilités nouvelles et de risques. Il est donc nécessaire d'adopter une approche stratégique en y consacrant les ressources voulues[70].

60. Presque toutes les réunions régionales préparatoires au quatorzième Congrès ont souligné la nécessité et l'importance qu'il y avait à étudier par quels moyens on pouvait permettre aux praticiens de la justice pénale et des services de détection et de répression d'utiliser les technologies, telles que l'intelligence artificielle et les technologies de l'information et de la communication, y compris les mégadonnées, dans la lutte contre la criminalité[71].

61. Le recours à l'intelligence artificielle aux fins de la réalisation d'autopsies virtuelles, les systèmes de prévision de la criminalité destinés à aider la police à utiliser au mieux ses ressources, les outils de détection de comportements à risque, les méthodes de traçabilité reposant sur la technologie de la chaîne de blocs et respectueuses de la vie privée, ainsi que les véhicules de patrouille autonomes, entre autres éléments, font l'objet de débats à cet égard[72]. En outre, encouragés par les avancées de l'intelligence artificielle qui rendent 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 adoptent ces technologies dans plusieurs de leurs opérations. Le degré d'utilisation de la robotique est très disparate, étant donné que certains pays sont plus avancés que d'autres dans la recherche sur ces technologies et dans l'usage qu'ils en font[73].

62. L'intelligence artificielle et l'apprentissage automatique semblent constituer un rempart de plus en plus efficace contre le blanchiment d'argent. 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, et ce de manière plus fiable. De plus, les médias sociaux ont de plus en plus recours à l'apprentissage automatique pour bloquer les contenus illicites et les infox. Les entreprises utilisent quant à elles l'intelligence artificielle pour mieux

---

[68] ONUDC, *Study on the Effects of New Information Technologies*.

[69] Victor Mayer-Schönberger et Kenneth Cukier, *Big Data : La révolution des données est en marche* (Robert Laffont, 2014).

[70] L'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI) a créé, à La Haye, un Centre pour l'intelligence artificielle et la robotique, qui fait office de ressource internationale sur ces questions.

[71] A/CONF.234/RPM.1/1, par. 61 j) ; A/CONF.234/RPM.2/1, par. 79 k) ; A/CONF.234/RPM.3/1, par. 56 f) ; et A/CONF.234/RPM.4/1, par. 57 e).

[72] INTERPOL et UNICRI, « Artificial intelligence and robotics for law enforcement » (Turin (Italie), 2019), p. v.

[73] Ibid., p. 6.

gérer les risques et détecter les fraudes de manière plus efficace, afin de prévenir et de limiter la commission d'infractions.

63. Toutefois, l'intelligence artificielle est une arme à double tranchant, en ce qu'elle est susceptible de faire profondément évoluer la manière dont les services de détection et de répression abordent leurs activités de contrôle, mais améliore aussi les modes opératoires des groupes criminels et terroristes et peut même faciliter l'émergence de nouvelles formes de criminalité[74]. Dans ce que l'on pourrait qualifier de lutte pour la « survie du plus fort »[75], la priorité consiste à encourager le recours à l'intelligence artificielle dans le cadre de la surveillance policière en vue de lutter contre les infractions commises à l'aide de cette même technologie.

H. Coopération internationale en matière pénale et utilisation de la technologie

64. S'agissant de la coopération internationale en matière pénale, la question de savoir comment les autorités centrales peuvent pleinement tirer profit des technologies modernes fait actuellement débat. Sur le plan politique, en 2016, la Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée a encouragé les États parties à exploiter le plus efficacement possible les technologies disponibles pour faciliter la coopération entre les autorités centrales[76].

65. Le renforcement de la coopération internationale, de plus en plus nécessaire, est subordonné à la disponibilité des ressources, notamment des ressources technologiques, telles que des réseaux permettant de transmettre des informations en toute sécurité ou des outils facilitant la communication (téléconférences et vidéoconférences, par exemple), et des systèmes de gestion des dossiers assurant le suivi des demandes reçues et envoyées. Davantage de ressources peuvent également être nécessaires pour garantir un traitement plus efficace des demandes d'entraide judiciaire portant sur des éléments de preuve électroniques (une solution serait, par exemple, de créer des unités spécialisées relevant des autorités centrales).

66. La gestion des dossiers par les autorités centrales rend évidemment compte des progrès, des avancées ou des lacunes de l'ensemble des mécanismes institutionnels du système de justice pénale des États Membres, à différents niveaux de capacité. Dans de nombreux pays où les dossiers continuent d'être consignés sur support papier, la recherche d'informations et la transmission des documents voulus au pays requérant peuvent constituer une tâche extrêmement fastidieuse. Dans les pays dotés d'outils numériques, la technologie moderne permet de recourir aux plateformes électroniques pour gérer les demandes d'entraide judiciaire reçues et envoyées ou pour compiler des données statistiques sur les affaires traitées et sur les tendances observées[77].

67. S'agissant de la transmission des demandes d'entraide judiciaire, la réunion régionale pour l'Amérique latine et les Caraïbes préparatoire au quatorzième Congrès a débattu de l'utilisation des moyens électroniques à cette fin, considérée comme une

---

[74] Un rapport de 2018 sur l'exploitation de l'intelligence artificielle à des fins criminelles a identifié trois grandes catégories de menaces en la matière, à savoir : a) les menaces liées à la sécurité numérique ; b) les menaces liées à la sécurité physique ; et c) les menaces liées à la sécurité politique (prolifération d'infox et de campagnes automatisées de désinformation ou d'influence destinées à modifier le comportement des électeurs et, éventuellement, à compromettre la tenue d'un débat public basé sur des informations véridiques). Voir Miles Brundage *et al.*, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (février 2018).

[75] INTERPOL Innovation Paper, « Artificial intelligence », Complexe mondial INTERPOL pour l'innovation, 2018, p. 2.

[76] Résolution 8/1 de la Conférence.

[77] Banque asiatique de développement et Organisation de coopération et de développement économiques, *Mutual Legal Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions* (2017), p. 31.

bonne pratique dans certains pays de la région [78]. La réunion préparatoire a recommandé d'encourager l'utilisation de la technologie pour rendre la coopération internationale en matière pénale plus efficace, en tenant compte, entre autres, des accords passés entre les autorités centrales concernant la transmission électronique des demandes de coopération internationale dans le respect de la législation nationale[79].

68. L'ONUDC a entrepris de promouvoir la coopération internationale, notamment au moyen d'outils sur mesure et d'innovations technologiques, à savoir : le portail de gestion des connaissances SHERLOC (mise en commun de ressources électroniques et de lois contre la criminalité), le Répertoire des autorités nationales compétentes et la version révisée du Rédacteur de requêtes d'entraide judiciaire[80].

69. L'ONUDC soutient activement les processus intergouvernementaux qui font de la coopération internationale s'agissant des éléments de preuve électroniques une priorité politique et juridique. On peut citer, à titre d'exemple, le groupe intergouvernemental d'experts à composition non limitée chargé de réaliser une étude approfondie sur le problème de la cybercriminalité [81], le débat thématique sur la cybercriminalité tenu lors de la vingt-septième session de la Commission pour la prévention du crime et la justice pénale, organisée en mai 2018 [82], et les travaux pertinents du Groupe de travail sur la coopération internationale de la Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée.

I. Considérations éthiques : garanties procédurales et garanties de respect des droits de l'homme

70. Les outils technologiques peuvent constituer un angle d'attaque utile pour lutter contre les menaces liées à la criminalité. Toutefois, la prudence est de mise lorsqu'il s'agit de recourir à ces outils, afin d'en garantir une utilisation responsable et éthique et d'éviter les imprévus. Ces considérations sont d'autant plus importantes que nombre de technologies actuelles et futures peuvent avoir de graves implications pour la vie privée et les libertés civiles.

71. Les services de détection et de répression utilisent, par exemple, les logiciels de reconnaissance faciale pour identifier beaucoup plus rapidement les suspects. Cependant, d'aucuns craignent que ces logiciels entraînent une surveillance abusive par les gouvernements, poussent les entreprises à la manipulation et mettent un terme au principe du respect de la vie privée. En outre, la conservation des données issues des systèmes biométriques est susceptible de porter atteinte à la vie privée, s'il en est fait une utilisation abusive[83].

72. On peut aussi citer l'exemple des mesures et analyses prévisionnelles. Ces dernières années, un nombre croissant de services de détection et de répression ont adopté des logiciels qui permettent d'analyser des données statistiques, d'établir des liens entre diverses activités et affaires, et même de prévoir là où la prochaine menace fera son apparition. Cependant, le recours aux mesures prévisionnelles aux fins du

---

[78] A/CONF.234/RPM.3/1, par. 72.

[79] Ibid., par. 79 n).

[80] Accessible à l'adresse suivante : www.unodc.org/mla/en/index.html [en anglais seulement].

[81] ONUDC, Cybercriminalité, « Meetings of the IEG on Cybercrime ». Disponible à l'adresse suivante : www.unodc.org/unodc/fr/index.html.

[82] Voir le guide concernant le débat thématique (E/CN.15/2018/6).

[83] Max Snijder, *Biometrics, Surveillance and Privacy* (Ispra, Italie, European Reference Network for Critical Infrastructure Protection (ERNCIP) Thematic Group Applied Biometrics for the Security of Critical Infrastructure, 2016), p. 4 ff.

profilage risque de conduire à la stigmatisation de certaines personnes et de certains groupes et, partant, à des formes de discrimination basées sur des algorithmes[84].

73. S'agissant de la traite des personnes et du lien entre recours à la technologie, d'une part, et droits de l'homme et protection des données, d'autre part[85], il est essentiel de protéger au mieux les victimes. Les mesures de lutte contre la traite des personnes doivent être conçues avec précaution afin qu'elles ne portent pas atteinte au droit à la vie privée et ne ciblent pas indûment certains groupes[86]. Il s'agit également de veiller à ce que les victimes bénéficient d'un accès sans danger à la technologie[87].

74. Un autre facteur important porte sur le respect des garanties procédurales afin de s'assurer que les éléments de preuve recueillis au moyen de techniques d'enquête spéciales, y compris celles impliquant l'utilisation de technologies, soient admissibles devant les tribunaux. Le recours aux techniques d'enquête spéciales est soumis aux dispositions pertinentes de la législation nationale et des instruments multilatéraux applicables[88]. Dans la plupart des juridictions, les éléments de preuve doivent être recueillis dans le strict respect des garanties établies contre les éventuels abus de pouvoir, notamment au moyen d'un contrôle judiciaire ou indépendant du recours à ces techniques, et conformément aux principes de légalité, de subsidiarité et de proportionnalité[89]. Pour être recevables, les éléments de preuve électroniques doivent être conformes aux procédures établies[90]. L'application des principes généraux des règles de procédures internes et de la jurisprudence nationale quant à la recevabilité des éléments de preuve recueillis dans le cadre d'enquêtes de criminalistique sur les cybermonnaies constitue une question nouvelle et épineuse qui requiert un examen plus approfondi et la mise en commun de données d'expérience[91].

75. Alors que les services de détection et de répression ont de plus en plus largement recours à l'intelligence artificielle et à la robotique, il est d'autant plus important de veiller à ce qu'il en soit fait un usage éthique. Des initiatives de type « droit souple » ont été prises pour minimiser les risques de violation des droits fondamentaux liés à l'utilisation de systèmes d'intelligence artificielle par les services de détection et de répression et pour éclaircir la question de la responsabilité juridique quant à l'utilisation éthique de l'intelligence artificielle et de la robotique en général[92].

---

[84] Voir Eva Schlehahn *et al.*, « Benefits and pitfalls of predictive policing », in *2015 European Intelligence and Security Informatics Conference: EISIC 2015* ; Joel Brynielsson et Moi Hoon Yap, éd. (Piscataway, New Jersey, Institute of Electrical and Electronics Engineers, Inc, 2015), p. 145 à 148 ; Albert Meijer et Martijn Wessels, « Predictive policing: review of benefits and drawbacks », *International Journal of Public Administration*, vol. 42, nº 12 (février 2019).

[85] Voir Groupe interinstitutions de coordination contre la traite des personnes, « Human trafficking and technology », p. 5.

[86] Mark Latonero *et al.*, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, Research Series on Technology and Human Trafficking (novembre 2012), p. 38.

[87] Gerry, Muraszkiewicz et Vavoula, « The role of technology in the fight against human trafficking », p. 211.

[88] Voir l'article 20 de la Convention des Nations Unies contre la criminalité transnationale organisée et l'article 50 de la Convention des Nations Unies contre la corruption.

[89] Pour la jurisprudence pertinente de la Cour européenne des droits de l'homme, voir Dimosthenis Chrysikos, « Article 50: special investigative techniques », in *The United Nations Convention against Corruption. A Commentary* ; Cecily Rose, Michael Kubiciel et Oliver Landwehr, éd., Oxford Commentaries on International Law Series (Oxford, Oxford University Press, 2019), p. 507 ff.

[90] E/CN.15/2018/6, par. 30.

[91] Michael Fröwis *et al.*, « Safeguarding the evidential value of forensic cryptocurrency investigations » (2019).

[92] L'Institute of Electrical and Electronics Engineers (IEEE) a publié un traité mondial sur l'éthique des systèmes autonomes et intelligents (conception éthique) afin d'aligner les technologies sur les valeurs morales et les principes éthiques. Voir IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (Pascataway, New Jersey, 2019).

76. Cependant, une question fondamentale est de savoir si la société, de manière générale, est prête et pleinement disposée à accepter certaines pratiques, telles que l'établissement d'un vaste réseau de dispositifs de surveillance, même lorsque celles-ci sont dans l'intérêt de la sûreté et de la sécurité publiques[93]. Les décisions arrêtées en matière de technologie doivent faire l'objet d'un large dialogue social sur les coûts et les avantages qui y sont associés, ainsi que sur les normes applicables en la matière. La question de convaincre le public des avantages offerts par la technologie dans les domaines de la détection et de la répression ainsi que de la justice pénale s'inscrit dans le cadre d'un dialogue plus large qui ne doit jamais être rompu, afin de s'assurer que les autorités compétentes ne perdent pas la confiance des collectivités et des citoyens qu'elles ont pour mission de protéger. Ce dialogue devrait également tenir compte des questions plus polémiques, notamment les critiques selon lesquelles un recours accru à la technologie pourrait aussi encourager l'adoption de mesures de surveillance coercitives et de stratégies de contrôle[94].

77. Le Groupe de haut niveau sur la coopération numérique a recommandé au Secrétaire général d'évaluer, dans l'ensemble du système, la manière dont les normes et accords internationaux existants en matière de droits de l'homme s'appliquaient aux technologies numériques nouvelles et émergentes. La société civile, les gouvernements, le secteur privé et le public devraient être encouragés à donner leur avis sur la façon dont il convient d'appliquer les instruments relatifs aux droits de l'homme à l'ère numérique, dans le cadre d'un processus dynamique et transparent[95].

78. Il convient de poursuivre une approche équilibrée pour trouver des solutions dans les cas où la technologie semble nuire à la vie privée ou à d'autres droits de l'homme. Pour éviter que la technologie ne soit utilisée comme cheval de Troie aux fins d'éventuelles violations des droits fondamentaux, les avancées technologiques doivent faire l'objet d'un suivi continu et ses effets doivent être évalués.

III. Conclusions et recommandations

79. En s'inspirant de la mythologie grecque, on peut s'interroger comme suit : la technologie est-elle, en définitive, une panacée (du nom de la fille d'Asclépios, remède prétendument capable de guérir toutes les maladies) pour la prévention de la criminalité ? Ou, à l'instar de la boîte de Pandore, peut-elle avoir des conséquences déplorables et ouvrir de nouvelles voies à la délinquance (conformément au mythe, où Pandore ouvre une jarre et laisse s'échapper tous les maux de l'humanité) ?

80. La réponse, loin d'être manichéenne, se trouve à mi-chemin. La technologie s'accompagne immanquablement de bons et de mauvais côtés. Si les services de détection et de répression et le système de justice pénale tirent parti des progrès technologiques, ceux-ci offrent aussi un terrain propice à l'essor de la criminalité. La situation en matière de criminalité ayant considérablement évolué en raison des différentes utilisations de la technologie moderne, les autorités compétentes doivent combler leur retard.

81. L'issue du bras de fer qui oppose actuellement les criminels et les défenseurs de l'état de droit dépendra largement de la question de savoir si des investissements sont réalisés dans la formation et si les stratégies de prévention de la criminalité et de justice pénale sont continuellement mises à jour afin de relever les nouveaux défis, tout en tenant compte des considérations éthiques et des droits de l'homme.

---

[93] INTERPOL et UNICRI, « Artificial intelligence and robotics for law enforcement », p. 14.

[94] James Byrne et Gary Marx, « Technological innovations in crime prevention and policing: a review of the research on implementation and impact », *Cahiers Politiestudies*, vol. 20, nº 3 (2011), p. 30.

[95] Nations Unies, *The Age of Digital Interdependence: Report of the Secretary-General's High-level Panel on Digital Cooperation* (juin 2019), recommandation 3A.

82. Le quatorzième Congrès des Nations Unies pour la prévention du crime et la justice pénale souhaitera peut-être examiner les recommandations suivantes :

a) Les États Membres devraient recenser et combler les lacunes que présentent leurs systèmes juridiques afin de garantir le bon déroulement des enquêtes et des poursuites concernant les infractions facilitées par la technologie, notamment en adoptant de nouvelles lois ou en mettant à jour la législation en vigueur, tout en prenant soin d'adopter des formules neutres sur le plan technologique, et en renforçant la coopération internationale ;

b) Les États Membres devraient encourager et développer les partenariats et les synergies avec les différentes parties prenantes, notamment les organisations internationales et régionales, la société civile, le secteur privé et le milieu universitaire, afin de renforcer la recherche, l'innovation, le développement et l'utilisation des technologies dans les domaines de la détection et de la répression et de la justice pénale ;

c) Les États Membres devraient recenser et évaluer les risques de blanchiment d'argent et de financement du terrorisme qui découlent des activités ou des opérations impliquant des prestataires de services d'actifs virtuels ; appliquer une approche fondée sur les risques afin de garantir que les mesures visant à prévenir ou à limiter le blanchiment d'argent et le financement du terrorisme sont proportionnées aux risques recensés ; et exiger des prestataires de services d'actifs virtuels qu'ils recensent et évaluent les risques de blanchiment d'argent et de financement du terrorisme et prennent des mesures efficaces pour en venir à bout ;

d) Les États Membres devraient investir de plus en plus dans une formation adaptée afin d'améliorer les capacités à résoudre efficacement les problèmes soulevés par les cybermonnaies lors des enquêtes ;

e) Les États Membres devraient inclure dans leur droit interne des dispositions relatives à la possession, à la publication et au transfert de matériel numérique pouvant servir à la fabrication éventuelle d'armes à feu, et poursuivre les activités de renforcement des capacités afin d'être davantage en mesure de prévenir ces actes ainsi que le trafic d'armes à feu sur le darknet, de les détecter, d'enquêter à leur sujet et d'en poursuivre les auteurs ;

f) L'ONUDC devrait continuer d'encourager la tenue de réunions régulières de praticiens pour s'assurer que les enquêteurs sont au courant des nouveaux modes opératoires suivis pour la fabrication et le transfert des armes à feu et adoptent des techniques d'enquête adaptées ;

g) Les États Membres devraient accorder une attention particulière au renforcement de l'expertise et des capacités des autorités compétentes dans tous les secteurs concernés afin de permettre une utilisation optimale des technologies dans la lutte contre la traite des personnes, tout en protégeant les droits des victimes ;

h) L'ONUDC devrait davantage mettre l'accent sur les orientations et le soutien techniques qu'il offre aux États Membres afin de définir et de mettre en œuvre plus efficacement des mesures pénales basées sur la technologie, le but étant de prévenir la traite des personnes et le trafic illicite de migrants, d'enquêter sur ces actes et d'en poursuivre les auteurs ;

i) Les États Membres devraient prendre des mesures législatives ou autres pour faciliter la détection, par les fournisseurs d'accès à Internet et de services en ligne et d'autres entités compétentes, des contenus montrant des actes d'exploitation sexuelle et des atteintes sexuelles visant les enfants et veiller à ce que ces contenus soient signalés et retirés ;

j) Les États Membres devraient mettre en œuvre des politiques et échanger des informations sur les meilleures pratiques, notamment sur les programmes d'aide aux victimes et la prise en compte des questions de genre, afin de protéger les enfants de l'exploitation et des abus sexuels ;

k) Les États Membres devraient approfondir leur compréhension des risques posés par l'utilisation de l'intelligence artificielle à mauvais escient et assurer un suivi permanent de l'évolution des nouvelles technologies afin d'être bien préparés et de garantir le respect des principes de responsabilité, de transparence et d'intégrité ; promouvoir des normes éthiques dans l'utilisation de ces technologies ; et veiller à ce que les citoyens et les populations aient confiance en cette utilisation ;

l) Les États Membres, en coopération avec l'ONUDC et d'autres organisations internationales, devraient promouvoir l'assistance technique et la formation afin de renforcer les compétences des praticiens et des autorités centrales concernant l'utilisation de la technologie, le but étant de renforcer la coopération internationale.