Nations Unies A/CONF.234/L.4/Add.1

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

Distr. limitée
11 mars 2021
Français
Original : anglais

Kyoto (Japon), 7-12 mars 2021

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

Rapport du Comité II : atelier 4

Additif

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

Déroulement des séances

1. À ses 4e à 6e séances, les 10 et 11 mars 2021, le Comité II a organisé un atelier sur 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. L'Institut coréen de criminologie et l'Institut national pour la justice du Ministère de la justice des États-Unis d'Amérique, qui font tous deux partie du réseau du programme des Nations Unies pour la prévention du crime et la justice pénale, ont aidé l'Office des Nations Unies contre la drogue et le crime (ONUDC) à préparer et organiser l'atelier. Le Comité était saisi des documents suivants :

a) Document d'information établi par le Secrétariat pour l'atelier sur 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 (A/CONF.234/11) ;

b) Document de travail établi par le Secrétariat sur la situation concernant la prévention de la criminalité et la justice pénale dans le contexte de la pandémie de maladie à coronavirus 2019 (COVID-19) (A/CONF.234/15) ;

c) Guide de discussion pour le quatorzième Congrès (A/CONF.234/PM.1) ;

d) Rapports des réunions régionales préparatoires au quatorzième Congrès (A/CONF.234/RPM.1/1, A/CONF.234/RPM.2/1, A/CONF.234/RPM.3/1, A/CONF.234/RPM.4/1 et A/CONF.234/RPM.5/1).

2. Les trois sessions de l'atelier ont été animées respectivement par les experts suivants : Phelan Wyrick, directeur de la Division des recherches et de l'évaluation du National Institute of Justice ; Han-kyun Kim, chercheur à l'Institut coréen de criminologie ; et Dimosthenis Chrysikos, spécialiste de la prévention du crime et de la justice pénale à l'ONUDC.

3. À la 4e séance du Comité II, le Président du Comité a fait une déclaration liminaire. Les intervenantes et intervenants suivants ont examiné la question des cryptomonnaies et des marchés du darknet, ainsi que les problèmes posés par l'utilisation des technologies dans le domaine des armes à feu : Anthony Teelucksingh, du Ministère de la justice des États-Unis, l'intervenant principal ; Hayato Shigekawa, de Chainalysis ; Thomas Holt, de l'Université de l'État du Michigan (États-Unis) ; José Romero Morgaz, de la Commission européenne ; Anna Alvazzi del Frate, de l'Alliance des organisations non gouvernementales pour la prévention du crime et la justice pénale ; et María Jiménez Victorio, de la Garde civile espagnole.

4. Les représentantes et représentants des pays suivants ont fait des déclarations : Fédération de Russie, États-Unis, Maroc, France, Mexique, Indonésie et Chine.

5. À la 5e séance du Comité II, la table ronde sur l'utilisation de la technologie et la traite des personnes, le trafic illicite de personnes migrantes et la maltraitance et l'exploitation d'enfants a été animée par les intervenantes et intervenants suivants : Douglas Durán, de l'Institut pour la prévention du crime et le traitement des délinquants en Amérique latine, l'intervenant principal ; Jo Harlos et Amber Hawkes, de Facebook ; Phiset Sa-ardyen, du Thailand Institute of Justice ; Michele LeVoy, de la Plateforme pour la coopération internationale concernant les sans-papiers ; Jane Annear, du Ministère australien de l'intérieur ; et Irakli Beridze, de l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice.

6. Les représentantes et le représentant de l'Italie, des Philippines et du Brésil ont fait des déclarations.

7. À la 6e séance du Comité II, la table ronde sur l'intelligence artificielle et la robotique, les considérations éthiques et la coopération internationale en matière pénale a été animée par les intervenantes et intervenants suivants : Cheol-kyu Hwang, de l'Association internationale des procureurs et poursuivants, l'intervenant principal ; Roderic Broadhurst, de l'Université nationale australienne ; Irakli Beridze, de l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice ; Luciano Kuppens, de l'Organisation internationale de police criminelle (INTERPOL) ; Arisa Ema, de l'Université de Tokyo ; Taegyung Gahng, de l'Institut coréen de criminologie ; Danka Hržina, du Bureau du procureur municipal en Croatie ; et Frances Chang, du Ministère de la justice des États-Unis.

8. Les représentantes du Canada et de l'Argentine ont fait des déclarations. La représentante de l'Institut pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient a également fait une déclaration.

Résumé de la présidence

9. La première table ronde s'est ouverte sur une allocution liminaire dans laquelle il a été souligné que malgré leur utilisation légitime, les cryptomonnaies et les autres techniques de cryptage rendaient difficiles les enquêtes sur les délits commis en ligne. En outre, les délinquants continuaient à utiliser des actifs virtuels pour transférer et dissimuler des fonds illicites, en particulier dans les juridictions dépourvues de législation sur la lutte contre le blanchiment d'argent. Un intervenant a souligné que les recherches consacrées aux interventions illicites sur les marchés effectuées en ligne avaient considérablement augmenté depuis une vingtaine d'années et que, depuis peu, on s'intéressait plus particulièrement aux cryptomarchés liés aux drogues. Des données récentes laissaient penser qu'une économie parallèle s'était développée autour de l'usurpation d'identité et de la vente de données volées. Deux personnes ont mentionné le succès remarquable d'opérations concertées de démantèlement de marchés du darknet. D'autres ont parlé du développement de la fabrication additive (impression 3D) des armes à feu ; de la technologie utilisée pour cacher des armes, échapper aux contrôles de sécurité et faciliter le transport des armes à feu ; et de la menace que représentaient les armes à feu dites « hybrides ».

10. Dans le débat qui a suivi, plusieurs personnes ont fait le point sur les mesures préventives, les bonnes pratiques et les réformes législatives adoptées par leur pays pour faire face aux diverses difficultés posées par l'utilisation des technologies de l'information et des communications à des fins criminelles. Plusieurs personnes ont souligné qu'il importait qu'il y ait des structures spécialisées dans la cybercriminalité au sein des services chargés des poursuites et des services de détection et de répression. L'accent a été mis sur la nécessité de dispenser une formation ciblée aux autorités compétentes. Un certain nombre de personnes ont répété qu'une coordination interinstitutions et des partenariats public-privé étaient nécessaires pour faire face aux enjeux de la cybercriminalité. Il a été noté que la protection des droits humains et des libertés fondamentales, en particulier du droit à la vie privée, devait être prise en considération dans le cadre de la prévention de la cybercriminalité et des enquêtes menées sur ce phénomène.

11. Un certain nombre de personnes ont souligné qu'il importait de renforcer la coopération entre les autorités nationales et les prestataires de services de communication afin de garantir la préservation des données et l'accès à celles-ci et de permettre des interventions rapides dans les affaires de cybercriminalité. Des personnes ont salué la création, en application de la résolution 74/247 de l'Assemblée générale, d'un comité intergouvernemental spécial d'experts à composition non limitée 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.

12. Il a été noté que les instruments juridiques multilatéraux existants, tels que la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention sur la cybercriminalité, constituaient le fondement d'une coopération internationale efficace visant à prévenir et combattre la cybercriminalité.

13. Des personnes ont mis en évidence la valeur ajoutée du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité – ou de tout mécanisme qui pourrait être créé à l'avenir au sein de l'ONUDC, compte dûment tenu de la nécessité d'éviter que leurs activités se chevauchent –, qui sert de plateforme d'échange d'informations sur les mesures nationales et internationales prises pour lutter contre la cybercriminalité.

14. Au cours de la deuxième table ronde, l'intervenant principal et les autres intervenantes et intervenants ont noté que, même si l'utilisation des technologies numériques, rapidement adoptées partout dans le monde, procurait d'importants avantages à la société, des possibilités nouvelles d'exploitation – traite des personnes et trafic illicite de personnes migrantes – reposant sur l'utilisation d'Internet, des médias sociaux et des sites de jeux en ligne, étaient apparues. La pandémie de maladie à coronavirus (COVID-19) avait aggravé les menaces criminelles connexes. Un intervenant a souligné que la technologie pouvait être mise à profit pour améliorer les mesures tenant compte du genre, notamment en facilitant les enquêtes à distance pour réduire la victimisation secondaire. La traque des flux financiers illicites pouvait être un autre moyen par lequel la technologie (technologie de la chaîne de blocs et intelligence artificielle, par exemple) permettait d'appuyer les politiques de lutte contre la traite des personnes.

15. Deux personnes ont parlé des approches adoptées dans leur entreprise pour garantir la sécurité en ligne, à savoir la prévention (avertissements relatifs à la sécurité et suppression de comptes utilisés pour des échanges potentiellement déplacés avec des enfants), la détection (réduction des contenus dangereux, détection proactive et démantèlement de réseaux) et les mesures connexes (blocage des faux comptes, collaboration avec les services de détection et de répression et création de centres d'aide auxquels signaler des contenus liés à la traite des personnes). Une autre intervenante a noté qu'il fallait être vigilant face à l'utilisation croissante des technologies numériques dans le cadre des contrôles aux frontières et de l'immigration. Deux personnes ont fait référence à la menace nouvelle que constituait la commission d'abus sexuels sur enfants diffusée en ligne en direct.

16. Dans le débat qui a suivi, un certain nombre de personnes ont estimé que les stratégies multipartites constituaient un moyen de prévention essentiel dans la lutte contre la cybercriminalité. Un intervenant s'est déclaré favorable à la collaboration avec les services nationaux de l'immigration et les organisations internationales pour mieux comprendre les modes opératoires des réseaux de traite des personnes qui agissent en ligne.

17. La troisième table ronde s'est ouverte sur une allocution liminaire dans laquelle il a été fait référence aux avantages qu'il y avait à associer intelligence artificielle et communication directe avec les autorités chargées de la coopération internationale en matière pénale. Un intervenant a examiné le rôle de l'intelligence artificielle – utilisée de manière transparente – dans la prise de décisions judiciaires, ainsi que dans l'analyse criminalistique, les modèles d'action policière fondés sur le renseignement et les systèmes de surveillance existants. Un autre intervenant a parlé du Centre pour l'intelligence artificielle et la robotique, qui avait été créé au sein de l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice dans le but de mieux connaître à la fois les risques et les avantages de ces technologies. Un autre intervenant a présenté le travail du Centre d'innovation d'INTERPOL, qui avait pour but d'aider les services de détection et de répression à suivre le rythme des innovations en matière d'action policière.

18. Deux personnes ont soulevé des considérations éthiques liées à l'utilisation de l'intelligence artificielle. L'une d'elles a noté que les milieux universitaires pouvaient jouer un rôle important dans la recherche et dans l'éducation pour les chercheurs et les praticiens. L'autre a souligné les risques de conflit entre, d'une part, l'utilisation des mégadonnées et de l'intelligence artificielle pour prédire la criminalité et, d'autre part, le respect des droits humains. Des principes directeurs éthiques étaient donc nécessaires pour garantir un contrôle efficace, le respect des formes régulières, l'équité, l'absence de discrimination et le respect du principe de responsabilité. Une intervenante a parlé des difficultés liées aux conséquences de la pandémie de COVID-19 sur la coopération internationale en matière pénale et des enseignements à tirer de cette crise, mentionnant l'adaptation et l'utilisation de méthodes innovantes (transmission des demandes par voie électronique, tenue de visioconférences, renforcement de la communication directe et des réseaux judiciaires). Une autre intervenante a souligné qu'il importait que les autorités centrales soient entièrement équipées et dotées de moyens d'action, citant les bonnes pratiques consistant à affecter à l'étranger des attachés des services de détection et de répression et des attachés judiciaires, et à passer par les services de détection et de répression avant de soumettre des demandes d'entraide judiciaire.

19. Dans le débat qui a suivi, les intervenantes et intervenants ont répété qu'il importait de renforcer la coopération internationale, notamment par le recours à des magistrats de liaison. Un intervenant a cité des exemples d'outils technologiques utilisés dans les enquêtes nationales qui ne cessaient d'évoluer. Une intervenante a demandé s'il y avait des affaires dans lesquelles la question de la recevabilité et de la crédibilité des données obtenues au moyen de l'intelligence artificielle avait été soulevée. En réponse à sa question, il a été noté que ce point serait examiné ultérieurement et que les outils nécessaires à cet examen existaient dans les législations nationales et les instruments multilatéraux (dispositions relatives au recours à des techniques d'enquête spéciales et aux conditions d'un tel recours).

20. Le Programme mondial de l'ONUDC contre la cybercriminalité, ainsi que les outils mis au point par l'ONUDC – le portail de gestion des connaissances pour la mise en commun de ressources électroniques et de lois contre la criminalité (SHERLOC), le Répertoire des autorités nationales compétentes, le *Guide pratique sur la demande de preuves électroniques à l'étranger* et le Rédacteur de requêtes d'entraide judiciaire – ont continué à susciter l'adhésion.

21. Le Président a invité les participantes et les participants à examiner les points suivants, soulevés au cours des débats :

a) La combinaison d'informations géographiques tirées des cryptomonnaies et de données tirées de la chaîne de blocs révèle des tendances qui reflètent les résultats également rapportés sur le marché « classique » du trafic de drogues. Toutefois, il est nécessaire de recueillir plus de connaissances sur la manière dont les interventions sur les marchés effectuées sur le darknet se recoupent. Pour de meilleurs résultats opérationnels, les services de détection et de répression devraient travailler en synergie avec différents partenaires, notamment le secteur privé et les chercheurs en sécurité, afin de faciliter les enquêtes en ligne ;

b) Les États Membres devraient évaluer la nécessité de définir des règles sur la détention et le commerce de plans de fabrication pour impression 3D qui pourraient rendre possible la fabrication illicite d'éléments essentiels d'armes à feu ;

c) Un soutien a été exprimé en faveur de l'application des nouvelles technologies pour le marquage des armes à feu, la conservation des informations les concernant, leur traçage et la destruction des armes désignées. Il est nécessaire de suivre le rythme des progrès technologiques, qui peuvent s'appliquer à de nombreux domaines, pour empêcher la production non autorisée d'armes à feu, leur transformation et leur réactivation illicites, les pratiques de détournement et le trafic illicite d'armes à feu en ligne ;

d) Il faudrait tenir compte de l'adoption de nouvelles technologies pour la gestion des stocks d'armes et la sécurité dans le domaine des armes à feu, ainsi que de l'utilisation de nouvelles technologies pour la gestion des stocks et le suivi et la protection des armes en transit ;

e) Les États Membres devraient prévenir la corruption et renforcer leurs mécanismes de transparence, en s'appuyant sur le rôle important joué par l'industrie, les milieux universitaires et les organisations de la société civile, en ce qui concerne les armes à feu et les menaces pour la sécurité liées à la technologie, par exemple en recoupant davantage les informations des bases de données, en utilisant les mégadonnées et les nouvelles technologies pour améliorer la sécurité des documents numériques, et en assurant la transparence du commerce autorisé ;

f) Le signalement anonyme de cas de traite des personnes et la transmission de preuves électroniques par des citoyens à l'aide d'un téléphone mobile ou sur une plateforme Internet pourrait être encouragé pour faciliter la tâche des autorités qui disposent d'effectifs et de ressources limités ;

g) La technologie en nuage, les mégadonnées et l'intelligence artificielle pourraient contribuer à améliorer les moyens techniques et permettre une action plus efficace et concertée contre la traite des personnes aux niveaux national et international ;

h) Les États Membres devrait examiner attentivement les incidences, pour les groupes à risque, de l'utilisation des technologies dans les domaines de l'action policière et du contrôle de l'immigration, élaborer des directives claires et veiller à la transparence de l'utilisation des technologies dans le cadre du contrôle de l'immigration, tout en mettant en place des moyens accessibles pour contester leur utilisation abusive ;

i) Les États Membres devraient veiller à ce que leur législation prévoie suffisamment de dispositions pour lutter contre les abus sexuels sur enfants diffusés en ligne en direct. Il est nécessaire d'analyser plus avant la manière dont les données et le renseignement nationaux peuvent être utilisés pour détecter des abus diffusés en ligne en direct, et il est également nécessaire de coopérer avec l'industrie du numérique et le secteur financier pour trouver des moyens de détecter de manière proactive les abus diffusés en ligne en direct et veiller à ce qu'ils soient signalés aux services de détection et de répression ;

j) Les États Membres devraient veiller à ce que leur législation soit actualisée au rythme des progrès technologiques, notamment en ce qui concerne l'intelligence artificielle, et s'efforcer de moderniser la coopération internationale en matière pénale en faisant utiliser la technologie et des outils novateurs aux praticiennes et praticiens et aux autorités centrales, lesquelles sont équipées et dotées de moyens d'action pour en bénéficier pleinement ;

k) Les États Membres sont encouragés à surveiller et à comprendre les risques posés par l'utilisation malveillante des technologies fondées sur l'intelligence artificielle afin de garantir le respect du principe de responsabilité et l'intégrité, à promouvoir des normes éthiques régissant l'utilisation de ces technologies et à s'assurer que l'application des nouvelles technologies suscite la confiance des citoyens et des populations.