



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

Distr. générale
22 mars 2024
Français
Original : anglais

**Groupe de travail
sur la coopération internationale**
Vienne, 5 et 6 juin 2024
Point 2 de l'ordre du jour provisoire*
**Rôle et incidences de la technologie
en ce qui concerne la coopération internationale
en matière pénale : possibilités, défis et besoins
en matière de renforcement des capacités**

Rôle et incidences de la technologie en ce qui concerne la coopération internationale en matière pénale : possibilités, défis et besoins en matière de renforcement des capacités

Document d'information établi par le Secrétariat

I. Introduction

1. Le présent document d'information a été établi par le Secrétariat pour faciliter les discussions que le Groupe de travail sur la coopération internationale doit tenir à sa quinzième réunion au titre du point 2 de l'ordre du jour provisoire. Portant sur le rôle et les incidences de la technologie en ce qui concerne la coopération internationale en matière pénale, il fournit une vue d'ensemble des considérations juridiques et pratiques à garder à l'esprit, ainsi qu'une analyse des possibilités, des défis et des besoins en matière de renforcement des capacités.

2. Ces dernières années, cette question a pris de l'importance tant dans la pratique que dans les différentes instances intergouvernementales d'élaboration des politiques. La technologie permet en effet de gagner en efficacité et de se doter de capacités accrues pour ce qui est de prévenir et de détecter les infractions, d'enquêter à leur sujet et d'en poursuivre les auteurs, grâce, par exemple, à des systèmes numériques de gestion des dossiers, au renforcement de la coopération internationale en matière pénale et à la constitution de réseaux permettant la transmission sécurisée d'informations.

3. En outre, sur le plan de l'élaboration des politiques, depuis 2016, la Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée encourage les États parties à exploiter le plus efficacement possible les technologies disponibles pour faciliter la coopération entre les autorités centrales¹. À sa quatorzième réunion, en septembre 2023, le Groupe de travail sur la coopération

* CTOC/COP/WG.3/2024/1.

¹ Résolution 8/1 de la Conférence.



internationale a lui-même proposé qu'en la matière, les trois sous-thèmes suivants soient examinés plus avant² :

- a) Transmission électronique des demandes de coopération internationale ;
- b) Recours à la vidéoconférence, notamment en matière d'extradition ;
- c) Élaboration de programmes de formation des praticiennes et praticiens en matière d'extradition et d'entraide judiciaire.

4. Ces sous-thèmes font partie des sujets de débat exposés ci-après, à l'instar d'autres aspects et paramètres présentant un intérêt par rapport à la place des innovations technologiques dans le domaine de la coopération internationale en matière pénale.

II. Considérations juridiques et pratiques ayant trait au rôle et aux incidences de la technologie en ce qui concerne la coopération internationale en matière pénale

A. Recours à l'intelligence artificielle

5. L'avènement de l'intelligence artificielle est susceptible d'entraîner d'importants gains d'efficacité dans le domaine de la justice pénale, aux niveaux tant national qu'international. Les structures de justice pénale, de détection et de répression connaissent une transformation numérique, et l'intelligence artificielle, qui recouvre différentes technologies, a un rôle important à jouer s'agissant d'aider les autorités compétentes à agir plus efficacement.

6. La police prédictive constitue un exemple caractéristique de l'incidence qu'a l'intelligence artificielle sur l'administration de la justice : l'utilisation d'algorithmes traitant d'énormes quantités de données a amené un nombre croissant de services de détection et de répression à adopter 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 apparition³. Sur le plan de la collecte de preuves, en dehors même de la police prédictive, les systèmes d'intelligence artificielle peuvent être d'une grande utilité à ces services. Ainsi, l'analyse de l'ADN ou des profils de médias sociaux génère de grandes quantités de données complexes sous forme électronique, qui peuvent présenter des schémas instructifs, non discernables par l'analyse humaine. Les outils basés sur l'intelligence artificielle peuvent également servir à identifier des personnes au moyen de logiciels de reconnaissance faciale. En outre, l'intelligence artificielle peut aider à localiser des événements et des endroits : la confrontation de vidéos, de photos, d'images satellitaires et d'autres données permet de vérifier que des événements se sont produits à un moment et à un endroit précis. Bien que, dans le cas de la vérification d'événements, l'analyse soit essentiellement effectuée par des êtres humains, elle pourrait à l'avenir être en grande partie automatisée ou améliorée par l'apprentissage automatique.

7. Si de nouvelles approches et solutions en matière de preuve sont nécessaires au niveau national, la situation est encore plus complexe dans les contextes internationaux. Il importe donc d'évaluer les implications internationales de l'utilisation de l'intelligence artificielle et les difficultés qui en découlent pour la coopération judiciaire. L'échange transfrontière d'éléments de preuve, en particulier du point de vue de leur recevabilité et de leur utilisation dans un État autre que celui où ils ont été recueillis, a toujours constitué un enjeu crucial pour la coopération internationale en matière pénale. En outre, les défis relativement nouveaux liés aux preuves électroniques ajoutent encore à la complexité.

² Voir le rapport de cette réunion, [CTOC/COP/WG.3/2023/4](#), par. 44.

³ [A/CONF.234/11](#), par. 72.

8. Dans ce contexte, la question de savoir si les instruments existants de coopération en matière pénale permettent de garantir de manière satisfaisante l'échange, la recevabilité et l'utilisation des éléments de preuve liés à l'intelligence artificielle reste ouverte. Si chaque pays finit par régler la question de l'intelligence artificielle et de la preuve pénale selon ses propres principes, règles voire normes techniques, la coopération judiciaire risque d'être entravée par l'existence de régimes différents, de sorte que l'on peut se demander si une approche coordonnée au niveau international ne serait pas plus appropriée.

9. Toutefois, comme dans tout autre cas se prêtant à l'utilisation de systèmes d'intelligence artificielle, il convient de ne pas oublier les effets positifs des nouvelles technologies. Il est à noter que, tout en faisant entrer la coopération internationale en territoire inconnu, l'intelligence artificielle pourrait également aider les autorités nationales à traiter plus efficacement les demandes de coopération. Selon l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI) et l'Organisation internationale de police criminelle (INTERPOL), à l'avenir, l'intelligence artificielle et la robotique pourraient servir précisément, par exemple, à automatiser les processus de façon à rendre autonomes la recherche et l'analyse des demandes d'entraide judiciaire internationale ainsi que les réponses apportées⁴.

10. L'un des cas les plus évidents d'utilisation de l'intelligence artificielle dans le cadre de la coopération judiciaire est celui du traitement automatisé des documents. Ce traitement comprend normalement au moins deux composantes : la vision par ordinateur pour la reconnaissance optique de caractères et le traitement du langage naturel pour l'analyse et le classement des documents. Les systèmes de traitement automatisé des documents peuvent répondre à des besoins professionnels tels que la conversion de documents papier numérisés, de fichiers PDF et d'images en documents modifiables permettant la recherche plein texte, le traitement de volumes importants de documents normalisés ainsi que le classement de documents et la création d'archives consultables⁵.

11. La traduction automatique est une autre application de l'intelligence artificielle très pertinente pour la collaboration transfrontière. Une grande variété de cas se prêtent à son utilisation dans le cadre de la coopération judiciaire internationale et notamment du travail des équipes d'enquête conjointes. L'une des difficultés les plus courantes auxquelles les membres de ces équipes doivent faire face est la nécessité de communiquer et d'analyser des éléments de preuve dans plusieurs langues. Dans la pratique, cela implique souvent de traduire de grandes quantités de documents, dont beaucoup contiennent une terminologie spécialisée ou qui sont rédigés dans des langues moins répandues. Même si les documents qui résultent de la traduction automatique ne peuvent pas servir de preuves, celle-ci peut au moins fournir un aperçu rapide et des indications sur les sections des documents susceptibles d'être les plus importantes et, par conséquent, nécessitant le plus une traduction officielle.

12. La mise en place d'outils de traduction automatique dans le flux de travail des équipes d'enquête conjointes peut en améliorer considérablement l'efficacité en réduisant le temps consacré à la traduction des documents présentés en tant que preuves et en rendant les éléments de preuve plus directement accessibles à l'équipe. Une traduction assermentée restera nécessaire pour que les éléments de preuve traduits soient recevables devant les tribunaux. Toutefois, la traduction automatique peut présenter un grand intérêt au stade de l'enquête et réduire considérablement les

⁴ Centre pour l'intelligence artificielle et la robotique de l'UNICRI et Centre d'innovation d'INTERPOL, « Artificial Intelligence and Robotics for Law Enforcement » (2019), disponible à l'adresse [ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW_ENFORCEMENT_WEB_0.pdf \(unicri.it\)](https://www.unicri.it/artificial-intelligence-robotics-law-enforcement-web-0.pdf), p. 10.

⁵ Artificial intelligence supporting cross-border cooperation in criminal justice, rapport conjoint établi par eu-LISA (Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice) et Eurojust (Agence de l'Union européenne pour la coopération judiciaire en matière pénale), 2022, p. 16 et 17.

délais et les coûts de la traduction assermentée, étant donné que dans la plupart des cas, au lieu d'une traduction, une simple postédition sera nécessaire⁶.

13. Une autre application pouvant présenter un intérêt dans le contexte de la coopération internationale en matière de justice pénale consiste dans l'utilisation de systèmes de résumé automatique de textes. Ces systèmes sont utiles dans les cas où de grandes quantités d'informations doivent être traitées dans un délai restreint, en particulier lorsque le traitement de ces informations par des humains n'est pas possible et que la précision n'est pas cruciale.

14. Les solutions de résumé de texte reposent en grande partie sur deux techniques : l'extraction et l'abstraction. Le résumé extractif produit des résumés en sélectionnant un sous-ensemble de phrases du texte d'origine à l'aide de méthodes statistiques. Le résumé abstraitif, qui s'appuie sur des méthodes d'apprentissage automatique, vise à produire des résumés de texte lisibles par l'être humain et renfermant les informations les plus pertinentes⁷.

15. Même si les solutions de résumé peuvent aider les organismes à traiter de grands volumes d'informations textuelles, comme les documents ayant fait l'objet d'une saisie, le résumé automatique ne peut pas égaler le travail humain et permet seulement une compréhension rapide et synthétique de la teneur des documents, ce qui rend l'information plus accessible pour une analyse humaine approfondie. Dans tous les cas, les documents utilisés comme preuves devront être vérifiés et analysés par des humains. Bien que des progrès notables aient été réalisés ces vingt dernières années dans la mise au point de systèmes de résumé de textes, il n'existe pas aujourd'hui de solution unique. Cependant, on tente de plus en plus de combiner les techniques extractives et abstraitives afin d'améliorer la qualité des résumés produits.

16. Malgré l'importance des preuves textuelles dans les enquêtes pénales, les éléments de preuve disponibles ne se limitent souvent pas au texte et comprennent d'autres supports très divers, notamment des images, des vidéos et des supports audio ou vocaux. Les technologies de base utilisées pour l'analyse criminalistique des supports visuels (images et vidéos) sont exactement les mêmes que celles dont les autorités chargées du contrôle aux frontières et les services de détection et de répression se servent pour la reconnaissance faciale. Il est donc relativement facile d'exécuter les algorithmes d'identification biométrique dans les systèmes d'analyse criminalistique d'images et de vidéos. Des technologies analogues peuvent être utilisées pour identifier certains objets ou évaluer l'authenticité d'enregistrements vidéo ou d'images (détection des hypertrucages, par exemple).

B. Rationalisation des systèmes de gestion des dossiers et numérisation

17. De nombreux pays dans le monde ont adopté des systèmes numériques de gestion des dossiers pour rationaliser les processus administratifs, réduire le volume de documents papier et accélérer la gestion des dossiers au sein de leurs systèmes judiciaires. L'automatisation des flux de travail, les systèmes d'archivage électronique et les outils de gestion des documents en ligne peuvent améliorer l'efficacité et la productivité des institutions judiciaires et des juristes. En outre, la collecte et l'analyse des données générées par les technologies numériques permettent aux autorités de se faire une meilleure idée des tendances, des délais de traitement des dossiers et des besoins en ressources. La prise de décision fondée sur des données permet d'éclairer l'élaboration des politiques, d'améliorer la gestion des ressources et de renforcer l'efficacité des interventions connexes.

18. La gestion des dossiers par les autorités centrales rend évidemment compte des progrès, des avancées ou des lacunes de l'ensemble des mécanismes institutionnels

⁶ Ibid., p. 18.

⁷ Ibid., p. 19.

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 observées⁸.

19. Les systèmes de gestion des dossiers sont essentiels pour assurer l'efficacité et l'efficacité des autorités centrales dans le renforcement de la coopération internationale, de plus en plus nécessaire. Pour réduire le nombre sans cesse plus important de dossiers en attente, un premier pas pourrait consister à mettre en place au sein des autorités centrales des structures ou unités spécialisées dans les formes de criminalité nouvelles et sophistiquées, aux caractéristiques de plus en plus complexes, qui sont à l'origine d'une charge de travail croissante. En outre, l'utilisation de statistiques peut faciliter un suivi plus efficace de la gestion des dossiers et le réajustement des ressources correspondant.

20. Le traitement automatisé des documents peut faire partie intégrante d'un système de gestion des dossiers, en aidant non seulement les procureurs et le personnel administratif participant aux enquêtes pénales, mais aussi les autorités intervenant dans la coopération internationale en matière pénale, à s'acquitter des fonctions administratives liées au traitement des documents. Les systèmes automatisés peuvent extraire efficacement les données nécessaires pour classer le document et l'enregistrer comme se rapportant à une affaire donnée, ce qui permet de réduire considérablement le besoin de traitement manuel des documents. Cette automatisation pourrait être utile pour la création de formulaires de renseignements sur les affaires, qui sont utilisés pour recueillir et stocker des informations auxquelles les autorités peuvent accéder pour bénéficier des connaissances, de l'expérience et des meilleures pratiques pertinentes.

21. La récente crise de la maladie à coronavirus (COVID-19) et ses retombées sur la coopération judiciaire en matière pénale ont montré qu'il fallait poursuivre la transformation numérique de la justice. Une initiative intéressante visant à numériser la coopération internationale est menée en Asie centrale. Dans le cadre du Réseau de coopération judiciaire pour l'Asie centrale et le Caucase du Sud (réseau CASC), le programme mondial pour le renforcement de la coopération en matière de justice pénale le long des itinéraires du trafic de drogues (CRIMJUST) et le Bureau régional de l'Office des Nations Unies contre la drogue et le crime (ONUDD) pour l'Asie centrale mettent en œuvre un projet consacré à la numérisation des processus de coopération juridique internationale en Ouzbékistan. Ce projet vise à renforcer les capacités techniques de l'autorité centrale ouzbèke par la création d'une plateforme électronique sécurisée destinée à la transmission numérique des demandes de coopération judiciaire internationale. Il contribuera à promouvoir la coopération internationale en matière pénale aux niveaux régional et international.

22. En outre, le projet susmentionné aidera à renforcer l'efficacité du suivi des demandes de coopération internationale reçues et envoyées, grâce à la mise en place d'une base de données intelligente. Cette solution numérique améliorera la collecte et le tri des informations, ce qui permettra d'analyser efficacement les tendances et favorisera l'adoption de mesures de justice pénale efficaces pour parer aux menaces de la criminalité transnationale organisée. L'initiative sera facilitée par la mise en place d'outils juridiques, de mécanismes d'intervention et d'activités de renforcement des capacités à l'intention du personnel de l'autorité centrale.

⁸ A/CONF.234/11, par. 66.

C. Vidéoconférence

23. La vidéoconférence occupe désormais une place de choix dans le domaine de la coopération internationale en matière pénale, car elle permet d'entendre un témoin dont le déplacement n'est pas possible ou souhaitable, tout en limitant les frais et les délais associés. Autorisée dans la plupart des États, cette pratique s'est intensifiée pendant la pandémie de COVID-19⁹.

24. Dans les contextes internationaux, la communication entre les autorités judiciaires des différents États Membres est capitale, et la vidéoconférence est l'un des moyens de la simplifier et de l'encourager. L'utilisation d'équipements de vidéoconférence offre aux tribunaux une plus grande latitude quant au choix du moment et des modalités de l'audition de témoins ou d'experts se trouvant dans d'autres États.

25. La vidéoconférence était autrefois une technologie coûteuse, mais les coûts ont suivi une tendance à la baisse au fil des ans. L'expérience acquise en la matière par les pays pendant la crise de la COVID-19, conjuguée à la baisse des coûts et à la disponibilité accrue de divers systèmes de vidéoconférence, a permis aux autorités compétentes de déployer cette technique plus efficacement que jamais. De plus, l'utilisation de la vidéoconférence, en particulier dans les affaires transfrontières, permet de ne pas avoir à dépenser d'argent pour le transport de témoins, de personnes détenues ou d'experts. Par ailleurs, les inspections sur place par le tribunal et les coûts y afférents peuvent également être évités, car les juges n'ont pas besoin de se déplacer hors de la salle d'audience. En outre, il devient moins impératif d'assurer l'hébergement et la protection de témoins à l'étranger, ce qui permet d'économiser les coûts associés¹⁰.

26. Les commentaires de nombreux professionnels témoignent d'une utilisation accrue de la vidéoconférence à mesure que celle-ci fait ses preuves en tant qu'outil fiable, efficace et économique, non seulement pour l'audition de témoins à distance, mais aussi pour un large éventail d'autres utilisations telles que la formation, la communication ou l'éducation.

27. Dans le domaine de la coopération internationale en matière pénale, les instruments multilatéraux applicables prévoient le recours à la vidéoconférence dans leurs dispositions relatives à l'entraide judiciaire. Le paragraphe 18 de l'article 18 de la Convention des Nations Unies contre la criminalité transnationale organisée et le paragraphe 18 de l'article 46 de la Convention des Nations Unies contre la corruption sont pertinents à cet égard. Les *Travaux préparatoires des négociations en vue de l'élaboration de la Convention des Nations Unies contre la criminalité transnationale organisée et des Protocoles s'y rapportant* mentionnent également un ensemble de points qui peuvent servir d'orientations afin de veiller au respect des droits de la défense lorsque des témoins sont entendus par vidéoconférence¹¹.

28. Au niveau régional, on peut citer le Deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale de 2001 (article 9)¹², la Convention ibéro-américaine sur l'utilisation de la vidéoconférence dans la coopération internationale entre les systèmes judiciaires et son protocole additionnel relatif aux coûts, au régime linguistique et à la présentation des demandes, adopté le 3 décembre 2010, le Protocole de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) sur la lutte contre la corruption de 2001 (article 8)¹³, la Convention d'entraide judiciaire et d'extradition contre le terrorisme de 2008 signée par les pays francophones d'Afrique (article 29), la Convention de Chisinau sur

⁹ E/CN.15/2024/7, par. 21.

¹⁰ ONUDC, *Manual on Videoconferencing: Legal and Practical Use in Criminal Cases*, 2017, p. 16.

¹¹ *Travaux préparatoires des négociations en vue de l'élaboration de la Convention des Nations Unies contre la criminalité transnationale organisée et des Protocoles s'y rapportant* (publication des Nations Unies, numéro de vente : F.06.V.5), p. 204 et 205.

¹² STE n° 182.

¹³ ECOWAS_Protocol_on_Corruption (cartercenter.org).

l'entraide judiciaire et les relations judiciaires en matière civile, familiale et pénale de 2002 (articles 6 et 105) et le Mécanisme du Commonwealth pour l'assistance mutuelle en matière criminelle (article 14)¹⁴.

29. Dans le contexte de l'Union européenne, les vidéoconférences transfrontières, notamment aux fins de l'audition de témoins, d'experts ou de victimes, peuvent se dérouler conformément à des instruments juridiques tels que la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (article 10)¹⁵, la directive du Conseil relative à l'indemnisation des victimes de la criminalité (article 9-1)¹⁶, la décision-cadre du Conseil relative au statut des victimes dans le cadre de procédures pénales (article 11-1)¹⁷ et la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (article 24)¹⁸.

30. En ce qui concerne les normes juridiques non contraignantes, les lignes directrices du Conseil de l'Europe sur la visioconférence dans les procédures judiciaires¹⁹ fournissent un ensemble de mesures de référence que les États et les tribunaux devraient suivre pour garantir que l'utilisation de la vidéoconférence dans les procédures judiciaires ne porte pas atteinte au droit à un procès équitable consacré par l'article 6 de la Convention européenne des droits de l'homme et répond aux exigences de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

31. Par ailleurs, la septième Réunion spécialisée des ministères publics du MERCOSUR et des États associés, qui s'est tenue le 29 mai 2009 à Asunción, a approuvé le « Guide d'Asunción sur l'utilisation de la vidéoconférence dans les procédures pénales ». Ce guide établit la nécessité d'harmoniser les lignes directrices législatives, techniques et opérationnelles relatives à l'utilisation de la vidéoconférence. Il recommande également que chaque ministère public désigne un coordonnateur national pour l'utilisation de la vidéoconférence, qui servirait de point de contact pour les pays requérants et d'intermédiaire avec le reste des institutions nationales afin de garantir la coordination nécessaire pour que la vidéoconférence soit un succès.

32. En pratique, la vidéoconférence est également utilisée dans des affaires liées à des procédures d'extradition. Du point de vue de la personne faisant l'objet d'une enquête, qui peut également, à un certain stade, être visée par une demande d'extradition, la vidéoconférence offre de multiples avantages. Une audition par vidéoconférence pourrait constituer une mesure efficace, proportionnée et moins intrusive que l'extradition de la personne accusée ou, dans le contexte de l'Union européenne, l'émission d'un mandat d'arrêt européen. C'est notamment le cas aux premiers stades de l'enquête, lorsque la présence du suspect devant l'autorité judiciaire n'est pas encore absolument indispensable, par exemple au début de la procédure. Pour un suspect visé par une enquête qui a lieu dans un pays différent de celui dans lequel il se trouve, la vidéoconférence peut être une méthode plus pratique pour témoigner et exercer sa défense sans avoir besoin de se rendre dans le pays où la procédure se déroule. Grâce à la vidéoconférence, le suspect peut exercer son droit à un avocat en témoignant ou en s'abstenant de témoigner, ce qui permet à la procédure de suivre son cours et offre au suspect la possibilité de rester lié à celle-ci sans risquer d'être considéré comme défaillant.

¹⁴ [P15370_13_ROL_Schemes_Int_Cooperation.pdf \(production-new-commonwealth-files.s3.eu-west-2.amazonaws.com\)](#).

¹⁵ *JO C 197* du 12 juillet 2000, p. 1 à 23.

¹⁶ *JO L 261* du 6 août 2004, p. 15 à 18.

¹⁷ *JO L 315* du 14 novembre 2012, p. 57 à 73.

¹⁸ *JO L 130* du 1^{er} mai 2014, p. 1 à 36.

¹⁹ Adoptées en juin 2021 par la Commission européenne pour l'efficacité de la justice (CEPEJ). Disponibles à l'adresse [151221GBR_Guidelines videoconferencing.pdf](#).

D. Transmission électronique des demandes de coopération internationale

33. La technologie a beaucoup aidé à surmonter les restrictions imposées par la pandémie de COVID-19 dans le domaine de la coopération internationale en matière pénale. Par exemple, les conditions créées par la pandémie ont donné davantage de poids à l'idée selon laquelle les outils électroniques constituaient un moyen sûr, rapide, souple et valable pour envoyer des demandes de coopération internationale et pour y répondre²⁰.

34. Dans sa résolution 11/1²¹, la Conférence des Parties à la Convention contre la criminalité organisée a également encouragé le recours à des technologies telles que la transmission électronique des demandes dans les procédures d'extradition et autres, les signatures électroniques (utilisation et acceptation) et, plus généralement, la dématérialisation des travaux des autorités centrales et autres autorités compétentes. Elle a notamment encouragé les États Membres à faire preuve de souplesse en ce qui concerne l'acceptation de documents officiels portant des signatures électroniques ou numériques²². Les États Membres ont aussi été encouragés à renforcer encore leur aptitude à utiliser les moyens électroniques pour transmettre des demandes d'entraide judiciaire et pour solliciter, à la suite de ces demandes, des éclaircissements et l'acceptation des éléments pertinents sous forme électronique, conformément aux principes fondamentaux de leur droit interne, notamment en vue d'améliorer leurs capacités dans l'ère post-COVID-19²³. Compte tenu des niveaux variables d'acceptation et de disponibilité des technologies et des communications basées sur celles-ci, la mise en œuvre d'une norme relativement harmonisée en matière de communication électronique constituerait déjà une entreprise considérable.

35. Lors de la sixième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, qui s'est tenue du 27 au 29 juillet 2020, la nécessité de moderniser, de rationaliser et d'accélérer la pratique de l'entraide judiciaire grâce à la transmission électronique des demandes de coopération internationale a été mise en avant. À cet égard, il a été souligné que les autorités centrales et autres autorités compétentes pourraient transmettre, par courrier électronique, les demandes d'entraide tant formelles qu'interinstitutionnelles, ainsi que les demandes de conservation de données, en utilisant des réseaux « 24/7 »²⁴.

36. De plus en plus d'autorités centrales à travers le monde acceptent que les demandes d'entraide judiciaire soient transmises par courrier électronique. Comme l'indique une étude de l'ONUDC consacrée aux incidences de la pandémie de COVID-19 sur la coopération internationale en matière pénale, qui fait le point sur les difficultés rencontrées, les bonnes pratiques suivies et les enseignements tirés au lendemain de la pandémie (à paraître prochainement), depuis la fin de cette dernière, les autorités centrales sont généralement plus enclines qu'auparavant à communiquer par voie électronique, notamment à recevoir et à envoyer des demandes d'entraide judiciaire par cette voie et en utilisant des signatures électroniques. On observe également une évolution plus marquée vers la présentation d'éléments de preuve par voie électronique.

37. Du point de vue normatif, le paragraphe 14 de l'article 18 de la Convention contre la criminalité transnationale organisée prévoit que les demandes d'entraide judiciaire sont adressées par écrit ou, si possible, « par tout autre moyen pouvant produire un document écrit [...] dans des conditions permettant [à l'État partie requis] d'en établir l'authenticité ». Une disposition similaire figure au paragraphe 14 de

²⁰ CTOC/COP/WG.3/2021/2, par. 23 et suiv.

²¹ Résolution 11/1, annexe I, « Incidences de la maladie à coronavirus (COVID-19) sur la coopération internationale en matière pénale : bilan sur une année » : approbation des recommandations du Groupe de travail sur la coopération internationale, *al. r*).

²² *Ibid.*, *al. v*).

²³ *Ibid.*, *al. w*).

²⁴ UNODC/CCPCJ/EG.4/2020/2, par. 32.

l'article 46 de la Convention contre la corruption. Selon le paragraphe 9 de l'article 4 du Deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, « [l]es demandes d'entraide judiciaire ou toute autre communication [...] peuvent être faites par voie de moyens électroniques de communication, ou par tout autre moyen de télécommunication, à condition que la Partie requérante soit prête à produire à tout moment, sur demande, une trace écrite de l'expédition ainsi que l'original. Cependant, tout État contractant peut, à tout moment, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, indiquer les conditions dans lesquelles il est prêt à accepter et à mettre en exécution des demandes reçues par voie électronique ou tout autre moyen de télécommunication. »

38. La Loi type d'entraide judiciaire en matière pénale de l'ONU²⁵, récemment actualisée, mentionne les conditions de la transmission électronique de preuves électroniques. Son article 29 fait référence à la nécessité de garantir : a) la sécurité et l'intégrité des éléments de preuve ; b) l'identification, l'authentification et la vérification de l'expéditeur et du destinataire ; et c) le respect de toutes les lois internes applicables en matière de protection des données et de la vie privée. Le développement de capacités technologiques dans le domaine de l'entraide judiciaire doit tenir compte de ces exigences ou critères.

39. Les capacités en matière de sécurité des courriers électroniques varient d'une autorité centrale à l'autre, certains pays possédant leur propre domaine d'administration public, doté d'une technologie de chiffrement de pointe, tandis que d'autres, à l'opposé, utilisent des domaines de courriel gratuits, dont les niveaux de sécurité sont intrinsèquement plus faibles. Il serait recommandé de réduire la fracture numérique qui persiste entre les autorités centrales chargées de l'entraide judiciaire en favorisant la mise en place de canaux sécurisés de communication par courriel.

40. Ces dernières années, il est devenu crucial de veiller à ce que la coopération internationale soit adaptée aux défis et aux possibilités que présente la nouvelle ère numérique. À cet égard, il convient de s'employer en priorité à passer de la communication physique à la communication électronique, en utilisant des plateformes sécurisées dotées d'un système de certification électronique et de signature numérique, qui garantissent la protection des données et la légitimité des parties concernées et qui permettent aux documents de produire tous leurs effets juridiques dans les procédures judiciaires.

41. Le Réseau ibéro-américain de coopération judiciaire internationale (IberRed), dispose d'un système de communication sécurisé appelé « Iber@ », qui permet d'envoyer des demandes d'entraide judiciaire internationale. Le Traité de 2019 sur la transmission électronique des demandes d'entraide judiciaire internationale entre autorités centrales (Traité de Medellín) n'oblige pas les parties à utiliser ce système pour la transmission des demandes, mais lorsque l'autorité centrale reçoit une demande par son intermédiaire, les communications ultérieures relatives à l'exécution de cette dernière doivent être adressées à l'autorité centrale requérante par la même voie, à moins que la nature de la demande ou des circonstances nouvelles ne rendent la chose inopportune, ce dont l'expéditeur doit alors être informé.

²⁵ [Model_Law_Mutual_Legal_Assistance_2022.pdf \(unodc.org\)](#).

E. Rôle de la technologie dans la promotion de la coopération judiciaire et de l'échange d'informations

1. Communication et échange d'informations sécurisés dans le cadre de la coopération judiciaire

42. Il est largement admis qu'il importe de réagir rapidement aux demandes de coopération internationale en matière pénale. Le paragraphe 13 de l'article 18 de la Convention contre la criminalité organisée prévoit la communication directe entre les autorités centrales et la transmission des demandes à ces autorités. Sur le plan stratégique, depuis les premières phases de ses travaux, la Conférence des Parties à la Convention contre la criminalité organisée accorde une attention particulière aux moyens d'exploiter la technologie de manière à améliorer la communication entre les autorités centrales intervenant dans la coopération internationale en matière pénale²⁶.

43. Au niveau régional et dans le contexte de l'Union européenne, Eurojust a été appelé à créer une « justice pénale numérique transfrontière », une infrastructure informatique rapide, fiable et sécurisée qui permettrait aux autorités nationales chargées des poursuites d'interagir avec leurs homologues. Comme suite aux conclusions du Conseil « Justice et affaires intérieures » de décembre 2018, la Commission européenne a lancé un projet de justice pénale numérique. Celui-ci vise à définir de grandes orientations en vue de concevoir et de mettre en œuvre une série de mesures numériques pour la coopération internationale en matière pénale. Selon le rapport final sur la justice pénale numérique transfrontière (2020) de la Commission européenne, la nécessité de communiquer et d'échanger des informations en toute sécurité par des moyens numériques figure parmi les catégories de besoins opérationnels dégagées dans le cadre de ce projet²⁷. Cela implique de trouver des solutions permettant aux parties prenantes de communiquer de manière sécurisée, y compris pour l'envoi et la réception de données sensibles et confidentielles. Le rapport constate en outre que dans tout environnement informatique nécessitant l'échange d'informations entre différents systèmes et composants, l'interopérabilité (l'aptitude des systèmes informatiques ou des logiciels à échanger et à exploiter des informations) doit toujours être garantie, de même que la compatibilité des mesures de sécurité mises en œuvre²⁸.

44. Les plateformes de communication sécurisées peuvent constituer des solutions pratiques pour faciliter une communication rapide et efficace entre praticiens et promouvoir l'échange d'informations entre les autorités intervenant dans la coopération internationale en matière pénale, y compris aux fins du suivi de l'exécution des demandes de coopération internationale. S'agissant du fonctionnement quotidien des autorités compétentes, l'utilisation systématique de courriers électroniques s'est révélée très utile pour assurer une communication rapide. Cependant, les plateformes de communication sécurisées offrent davantage de fonctionnalités pour l'échange d'informations entre praticiens. Outre le partage de textes, de fichiers ou d'images, elles leur permettent d'envoyer des messages audio, de passer des appels audio ou vidéo et de s'assurer que les destinataires ont bien reçu ou lu leurs messages. Cette dernière fonction, en particulier, aiderait les praticiennes et praticiens à suivre leurs demandes et à réduire les délais de réponse.

45. Les praticiens ayant de plus en plus besoin de communiquer entre eux de manière sûre, l'ONUDC étudie la possibilité de mettre en place une plateforme de communication sécurisée pour faciliter la communication directe et les échanges informels entre les autorités centrales chargées de traiter les demandes d'entraide judiciaire. Une option à l'étude consiste à s'inspirer de l'exemple de la plateforme de communication sécurisée du Réseau opérationnel mondial des services de détection et de répression de la corruption (Réseau GlobE) (voir le paragraphe 53 pour de plus

²⁶ Voir décision 3/2, *al. u*) ; et décision 4/2, *al. w*). Voir également la résolution 8/1, par. 6, et annexe I, par. 1).

²⁷ Commission européenne, « Cross-border digital criminal justice », Rapport final de 2020, p. 3.

²⁸ *Ibid.*, p. 3 et 51.

amples informations) et à faire appel aux services du même fournisseur externe pour la conception d'une application similaire que les autorités centrales intervenant dans l'entraide judiciaire utiliseraient comme plateforme de communication sécurisée.

46. Au moment de la rédaction du présent document, le secrétariat testait les fonctionnalités techniques de l'application et leur adaptabilité à des fins de promotion de la communication dans le domaine de l'entraide judiciaire. Il se penchait également sur la manière de connecter l'application au répertoire en ligne des autorités nationales compétentes du portail de gestion des connaissances pour la mise en commun de ressources électroniques et de lois contre la criminalité (SHERLOC).

2. Faciliter l'échange d'informations dans le cadre de la coopération entre services de détection et de répression

47. Selon le paragraphe 3 de l'article 27 de la Convention contre la criminalité organisée, les États parties s'efforcent de coopérer en matière de détection et de répression pour faire face à la criminalité transnationale organisée perpétrée au moyen de techniques modernes. En outre, conformément au paragraphe 1, alinéa a), du même article, les États parties doivent adopter des mesures efficaces pour renforcer ou établir des voies de communication entre leurs autorités compétentes afin de faciliter l'échange sûr et rapide d'informations concernant tous les aspects des infractions visées par la Convention.

48. S'agissant du fonctionnement quotidien des services de détection et de répression compétents, l'utilisation systématique de courriers électroniques s'est révélée très utile pour assurer une communication rapide, et des outils tels que des bases de données sécurisées ont été mis au point pour permettre à ces services d'échanger des informations. D'après les *Travaux préparatoires des négociations en vue de l'élaboration de la Convention contre la criminalité organisée*, les États parties déterminent eux-mêmes le meilleur moyen d'assurer l'échange sûr et rapide d'informations²⁹.

49. En outre, conformément au paragraphe 1 de l'article 12 et au paragraphe 1 de l'article 13 du 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, les États parties devraient échanger des informations et coopérer aux niveaux bilatéral, régional et international pour prévenir, combattre et éradiquer la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions. La technologie peut contribuer à rendre cette coopération et cet échange d'informations plus rapides et plus efficaces. Des dispositions similaires concernant l'échange d'informations figurent également dans le Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants (article 10), et le Protocole contre le trafic illicite de migrants par terre, air et mer, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée (article 10), dans les limites du champ d'application de chaque protocole.

50. Dans le cadre de la gestion des frontières, le traitement à guichet unique aide à s'acquitter de la tâche épineuse consistant à faciliter la circulation des personnes et des biens tout en assurant la sécurité aux frontières, ainsi qu'à prévenir et à détecter le trafic d'armes à feu et de leurs pièces, éléments et munitions. Ce système permet à un importateur ou à un exportateur de fournir à un organisme public désigné du pays d'importation l'ensemble des informations et documents nécessaires au moyen d'une plateforme électronique. L'organisme transmet ensuite ces informations à tous les services concernés, lesquels appliquent des techniques d'évaluation des risques pour

²⁹ Voir *Travaux préparatoires des négociations en vue de l'élaboration de la Convention des Nations Unies contre la criminalité transnationale organisée et des Protocoles s'y rapportant* (publication des Nations Unies, numéro de vente : F.06.V.5), p. 251. Voir également [CTOC/COP/WG.3/2023/2](#), par. 17.

déterminer si les marchandises doivent être interceptées pour inspection. Cette approche peut être combinée avec des lignes directes de communication transfrontalière permettant aux services de contrôle des frontières de s'entretenir au sujet des opérations suspectes, ainsi qu'avec des procédures d'alerte précoce qui permettent de faire part des nouveaux événements nécessitant des contre-mesures immédiates³⁰.

51. Le paragraphe 4 de l'article 12 du Protocole relatif aux armes à feu exige que les États coopèrent pour le traçage des armes à feu, de leurs pièces, éléments et munitions ayant pu faire l'objet d'une fabrication ou d'un trafic illicites. Un traçage efficace repose sur des registres d'armes à feu complets qui contiennent des informations sur l'ensemble du cycle de vie d'une arme à feu – de sa fabrication ou de son importation aux différentes transactions dont elle fait l'objet et, enfin, à son exportation, sa disposition ou sa destruction. Les registres d'armes à feu intégrés et numérisés, tels que le logiciel de tenue de registres « goIFAR », élaboré par l'ONUSD et adaptable aux besoins nationaux, permettent l'identification et le traçage d'une arme à feu en temps réel. Par ailleurs, INTERPOL a mis au point plusieurs outils informatiques qui facilitent l'échange d'informations et la coopération entre les services de détection et de répression autorisés, notamment des outils spécialisés sur le trafic d'armes à feu et la criminalité liée aux armes à feu. Par exemple, grâce au Système INTERPOL de gestion des données sur les armes illicites et du traçage des armes, auquel plus de 180 pays ont accès, les membres peuvent retrouver les armes à feu saisies, perdues ou volées. En outre, le Réseau d'information balistique d'INTERPOL permet d'échanger et de comparer des données balistiques, y compris par-delà les frontières, afin de déterminer si une même arme à feu a été utilisée sur différentes scènes de crime. Ces systèmes spécifiques aux armements peuvent être utilisés en parallèle avec des outils plus généraux d'INTERPOL, tels que le réseau des bureaux centraux nationaux, le système des notices internationales et toute autre base de données d'INTERPOL, accessible au moyen du système mondial de communication policière I-24/7³¹.

52. En outre, en avril 2022, l'ONUSD a mis sur pied un pôle de connaissances sur la traite des personnes et le trafic illicite de personnes migrantes, utilisé par environ 1 400 personnes issues de 114 pays. Grâce au partage de connaissances et à des événements en direct, cet outil favorise l'échange informel et interactif d'informations entre praticiens de la justice pénale et le renforcement des réseaux de praticiens. Cela a facilité l'échange d'informations portant sur des affaires précises tout en contribuant à la mise en place d'une coopération plus souple et plus rapide en parallèle des démarches relatives aux demandes formelles.

53. Le Réseau opérationnel mondial des services de détection et de répression de la corruption (Réseau GlobE) a été créé en juin 2021 par l'ONUSD pour faciliter la coopération informelle et pallier l'absence d'un réseau véritablement mondial de services de détection et de répression de la corruption. Il dispose d'un pôle numérique unique qui sert de cadre de coopération et qui inclut une plateforme sécurisée pour les communications confidentielles entre les membres du Réseau. La solution de communication d'entreprise sécurisée GlobE Threema a été déployée gratuitement en 2022, à l'intention exclusive des praticiennes et praticiens du Réseau GlobE. L'accès à GlobE Threema est octroyé à des représentantes et représentants désignés des membres du Réseau³².

³⁰ Nations Unies, Bureau des affaires de désarmement, Recueil de modules sur le contrôle des armes légères, MOSAIC 05.60, « Contrôle aux frontières et coopération en matière d'application des lois » (2018), p. 26 et suiv.

³¹ ONUDC, *Technical Guide to the Implementation of the Protocol against the Illicit Manufacturing of and Trafficking in Firearms*, p. 101 et suiv.

³² CAC/COSP/EG.1/2023/2, par. 39.

F. Favoriser la coopération internationale grâce à des innovations technologiques et à des outils sur mesure

54. Comme celles et ceux de tout autre domaine ou secteur, les praticiennes et praticiens intervenant dans la coopération internationale en matière pénale bénéficient au quotidien d'un ensemble d'applications technologiques. L'ONUDC a entrepris de promouvoir la coopération internationale, notamment au moyen d'outils sur mesure et d'innovations technologiques, dont le portail SHERLOC et son module sécurisé « RevMod », spécialement conçu pour faciliter la conduite des examens de pays dans le cadre du Mécanisme d'examen de l'application de la Convention des Nations Unies contre la criminalité transnationale organisée et des Protocoles s'y rapportant, le Répertoire des autorités nationales compétentes qu'il tient à jour et la version révisée du Rédacteur de requêtes d'entraide judiciaire.

55. Les systèmes fondés sur des données et dotés d'un moteur de recherche, tels que le répertoire susmentionné, permettent de trouver, sous une forme sécurisée et authentifiée, les coordonnées des autorités centrales et compétentes du monde entier. Une technologie d'analyse de données peut être intégrée et appliquée dans le Répertoire des autorités nationales compétentes afin de produire des visualisations statistiques destinées à en faciliter et à en étoffer l'utilisation.

56. Le Rédacteur de requêtes d'entraide judiciaire est un outil numérique mis au point par l'ONUDC pour aider les praticiennes et praticiens de la justice pénale, en particulier le personnel des autorités centrales intervenant dans l'entraide judiciaire, à rédiger rapidement des demandes d'entraide judiciaire. Conformément aux normes de sécurité applicables, il est actuellement en train d'être amélioré de façon à mieux répondre aux normes de sécurité de l'ONU. Sa version révisée bénéficiera d'une configuration et d'une intégration plus sécurisées dans l'infrastructure de réseau existante et sera incorporée dans le Répertoire des autorités nationales compétentes de l'ONUDC, protégé par un mot de passe. Le degré de synchronisation et d'interopérabilité des deux outils s'en trouvera accru.

G. Technologie et entraide judiciaire aux fins de l'obtention ou de la préservation de preuves électroniques

57. Du fait que les preuves électroniques peuvent être obtenues par l'intermédiaire d'un tiers (les fournisseurs de services de communication), l'accès aux données provenant de différents types de fournisseurs est devenu déterminant pour le succès des enquêtes transfrontières ces dernières années. C'est la raison pour laquelle il est extrêmement important d'établir des partenariats entre les fournisseurs de services de communication et les services de détection et de répression³³.

58. Une réflexion approfondie sur les impératifs et les limites de la collecte de preuves électroniques auprès de ces acteurs privés pourrait s'inscrire dans un débat plus large sur le rôle de la technologie en matière de détection et de répression et sur les enjeux créés par l'évolution constante des technologies, notamment la collecte et l'examen d'éléments de preuve au moyen de l'Internet des objets et de l'intelligence artificielle.

59. La nécessité de recourir à telle ou telle technologie dépend du stade et du degré de complexité de l'enquête ou de la procédure pénale au moment de la réception d'une demande d'assistance, ainsi que de la mesure dans laquelle la fourniture de cette assistance amène à devoir traiter des données ou des preuves électroniques. Pour ce qui est de la préservation, de la communication et de la production de données informatiques stockées, l'utilisation de portails en ligne spécialement conçus pour la coopération entre services de détection et de répression passe pour être le moyen le plus rapide et le plus efficace de contacter les fournisseurs de services de

³³ E/CN.15/2022/6, par. 7.

communication. Ces portails sont généralement mis en place par lesdits fournisseurs ou, dans certains cas, par des sociétés tierces spécialisées dans la facilitation de la communication entre les entreprises et les services de détection et de répression, autorités de réglementation et autres organismes publics. Les portails de communication sécurisés destinés aux activités de détection et de répression constituent des solutions de sécurité plus solides que les modes de communication manuels traditionnels ou les logiciels qui, n'ayant pas été conçus à cette fin, peuvent être plus vulnérables et exposés à davantage de risques³⁴.

60. La gestion des preuves électroniques exige une chaîne de possession aussi solide que celle des preuves matérielles. Toutefois, le stockage et la préservation des éléments de preuve électroniques posent de multiples problèmes spécifiques dans le cadre des opérations transfrontières de gestion de preuves. Les opérations de gestion viable des éléments de preuve doivent établir un juste équilibre en ce qui concerne la portée et le niveau de la gestion des preuves électroniques et suivre le rythme des progrès technologiques pour s'adapter à l'évolution des besoins dans ce domaine. Elles tirent presque toutes parti des technologies disponibles pour gagner en efficacité et en efficience. La mise en œuvre et l'adoption de normes et de pratiques en matière de technologie et de preuves électroniques contribuent à l'instauration d'un solide cadre de référence organisationnel pour une gestion viable des éléments de preuve.

61. Le stockage des éléments de preuve dans des conditions qui en préservent l'état d'origine et l'intégrité à des fins criminalistiques est un principe fondamental de la gestion des preuves. Un stockage efficace suppose de conjuguer des systèmes d'organisation et de classement à des méthodes et techniques de stockage appropriées, afin d'optimiser l'espace disponible dans les locaux. L'utilisation de solutions technologiques à cet effet aide à retrouver et à consulter rapidement tout élément de preuve. Du point de vue de la protection des données, des délais de conservation doivent être fixés afin que les données ne soient pas conservées plus longtemps que ne l'exige l'objectif de leur traitement et de leur stockage.

H. Considérations relatives aux droits humains

62. Les outils technologiques peuvent offrir un angle d'attaque utile pour lutter contre les menaces liées à la criminalité. Toutefois, la prudence est de mise lors de leur utilisation, qui doit être responsable et éthique et ne pas entraîner de conséquences imprévues. 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.

63. Malgré leurs apports dans le domaine de la coopération internationale en matière pénale, les outils technologiques comportent un certain nombre de risques potentiels, tels que l'opacité du processus décisionnel, différentes formes de discrimination, la nature intrusive de leur utilisation et des atteintes à la protection de la vie privée et des données à caractère personnel. Ces risques potentiels sont aggravés dans les secteurs de la détection et de la répression et de la justice pénale, tant au niveau national que dans la sphère de la coopération internationale, car ils peuvent compromettre la présomption d'innocence et les droits fondamentaux des personnes à la liberté et à la sécurité ainsi qu'à un recours effectif et à un procès équitable.

64. À titre d'exemple, le recours à l'intelligence artificielle et à des algorithmes d'apprentissage automatique dans les processus décisionnels soulève des préoccupations éthiques et juridiques en matière de transparence, de responsabilité, de partialité et d'équité. Veiller à ce que les systèmes d'intelligence artificielle fonctionnent conformément aux principes relatifs aux droits humains, sans perpétuer

³⁴ Pour une vue d'ensemble des pratiques générales élaborées par les fournisseurs de services internationaux pour répondre aux demandes de données des gouvernements étrangers, voir le dispositif de divulgation de données de l'ONUDC, disponible sur le Centre d'information sur les preuves électroniques du portail SHERLOC.

la discrimination ni renforcer les inégalités existantes, est une entreprise complexe. L'utilisation du résultat de calculs algorithmiques effectués par ces systèmes, en particulier comme preuve devant une juridiction pénale, peut entraîner une violation du droit fondamental à un procès équitable pour au moins deux raisons différentes. Premièrement, les processus algorithmiques servant à analyser les données et à fournir aux autorités publiques un élément de preuve donné sont souvent obscurs. Dès lors que, dans le cadre d'une procédure judiciaire, des personnes n'ont pas la possibilité de comprendre et de contester, même avec le concours d'un avocat, les systèmes algorithmiques complexes utilisés pour traiter les éléments de preuve censés les concerner, il existe une menace importante pour le droit à une procédure régulière. Deuxièmement, et en conséquence, si les enquêtes reposent sur des techniques d'intelligence artificielle, le défendeur devrait être en mesure de comprendre comment les preuves ont été recueillies. Dans le cas contraire, l'utilisation de preuves obtenues à l'aide de l'intelligence artificielle risque de nuire au principe de l'égalité des armes.

65. L'Assemblée générale a adopté, pour la première fois, une résolution historique sur la promotion de systèmes d'intelligence artificielle « sûrs, sécurisés et dignes de confiance » qui favoriseront également un développement durable pour tous³⁵. Elle a demandé à tous les États Membres et aux autres parties prenantes « de s'abstenir ou de cesser de se servir des systèmes d'intelligence artificielle qu'il [était] impossible d'utiliser dans le respect du droit international des droits humains ou qui présent[ai]ent des risques excessifs pour l'exercice des droits humains ». Elle a aussi réaffirmé que « les droits dont les personnes jou[issaient] hors ligne [devaient] également être protégés en ligne, y compris tout au long du cycle de vie des systèmes d'intelligence artificielle ».

66. Il faut bien comprendre que le respect des règles procédurales est important pour garantir l'admissibilité devant les tribunaux des preuves recueillies grâce aux techniques d'enquête spéciales, notamment celles impliquant l'utilisation de technologies modernes. Dans la plupart des pays, les éléments de preuve doivent être recueillis dans le strict respect d'un certain nombre de garanties établies contre les éventuels abus de pouvoir, ce qui implique notamment un contrôle judiciaire ou indépendant du recours à ces techniques, et conformément aux principes de légalité, de subsidiarité et de proportionnalité³⁶. Ces considérations sont étroitement liées à l'obligation positive qu'ont les États de mettre en place des lois, règlements et procédures permettant d'assurer, dans un souci de sécurité juridique, la bonne administration de la justice, la protection des droits de la personne et le respect des normes garantissant un procès équitable.

67. Par ailleurs, les conditions et précautions relatives à la collecte et à l'utilisation des preuves électroniques exigent avant tout un contrôle judiciaire ou un autre contrôle indépendant qui permette de circonscrire les procédures, processus, méthodes et outils utilisés pour recueillir, acquérir, conserver et analyser ce type de preuves. Par conséquent, il faudrait se pencher en priorité sur la nécessité d'adopter une législation procédurale conférant aux services de détection et de répression compétents les pouvoirs voulus pour recueillir efficacement les éléments de preuve électronique tout en respectant la confidentialité, la vie privée, les droits de la personne, la régularité des procédures et d'autres mesures de protection juridique³⁷.

68. En un mot, il convient d'adopter une approche équilibrée pour trouver des solutions dans les cas où la technologie semble nuire à la vie privée ou à d'autres droits humains.³⁸ L'application de ces solutions dans les domaines de la justice, de la détection et de la répression ne peut être considérée comme un défi purement technique. La conception et le déploiement de solutions reposant sur l'intelligence

³⁵ Résolution 78/265 de l'Assemblée générale. Au moment de la rédaction du présent document, la résolution n'avait pas encore été publiée. Voir le projet de résolution (A/78/L.49).

³⁶ CTOC/COP/WG.3/2020/3, par. 66.

³⁷ CTOC/COP/WG.3/2023/2, par. 70.

³⁸ A/CONF.234/11, par. 78.

artificielle devraient notamment être évalués avec une attention particulière afin d'éviter que les libertés et droits fondamentaux des personnes puissent être lésés et que des personnes puissent être soumises à diverses formes de discrimination, de restriction des droits ou de traitement inéquitable.

69. Assurer la protection des droits humains dans le cadre du développement des technologies numériques et de leur utilisation dans l'administration de la justice nécessite d'adopter des approches multidisciplinaires et multisectorielles qui intègrent des garanties juridiques et techniques, ainsi que des mécanismes de contrôle visant à garantir le respect des libertés et droits fondamentaux. La réalisation d'études d'impact sur les droits humains préalables à l'élaboration et au déploiement des technologies numériques est une composante essentielle d'une gouvernance responsable dans le cadre du développement des technologies numériques et de leur utilisation dans l'administration de la justice. Ces études permettent de cerner et d'analyser les risques et les incidences potentiels des technologies numériques sur les droits humains, notamment les droits à la vie privée, à un procès équitable, à la non-discrimination et à l'accès à la justice. En outre, des mécanismes de suivi et d'évaluation continus, mis en place à des stades ultérieurs du processus de déploiement des technologies numériques dans l'administration de la justice, permettent de suivre l'efficacité, l'incidence et les retombées des technologies numériques au regard des normes et principes relatifs aux droits humains.

I. Besoins en matière de renforcement des capacités et d'assistance technique

70. L'adoption des technologies numériques doit s'accompagner d'activités de formation et de renforcement des capacités visant à doter les autorités intervenant dans la coopération internationale en matière pénale des compétences et des connaissances dont elles ont besoin pour s'en servir efficacement. Le manque d'équipements technologiques entraîne des disparités entre les pays dans l'accès à la technologie et dans sa maîtrise. Les compétences inégales des praticiennes et praticiens empêchent d'engager une coopération internationale constructive qui passe par des moyens technologiques, ce qui fait ressortir la nécessité d'un renforcement des capacités équitable. Il convient en outre de s'employer activement à combler le fossé numérique et à assurer un accès équitable à la technologie en améliorant les compétences des praticiennes et praticiens.

71. Lors d'une transition vers des plateformes numériques, il n'est pas rare de se heurter à une résistance au changement et de devoir apporter un appui technique continu. Pour que les autorités intervenant dans la coopération internationale en matière pénale aient accès à la technologie et puissent en faire bon usage, elles ont besoin de ressources financières, de formations et de compétences techniques. Ces autorités doivent s'adapter aux évolutions de leur environnement afin de limiter les possibilités que les progrès technologiques offrent aux délinquants. S'ils se laissent distancer dans ce domaine, les mécanismes de coopération internationale ne pourront pas lutter efficacement contre la criminalité transnationale organisée, qui exploite ces avancées.

72. Certaines techniques et technologies sont devenues indispensables dans le cadre de la coopération internationale en matière pénale pour lutter contre la cybercriminalité organisée. Bien que l'utilisation de logiciels spécialisés, de techniques de renseignement d'origine sources ouvertes et de matériel de pointe améliore incontestablement l'efficacité et la rapidité des enquêtes, il demeure impératif de reconnaître les problèmes et les lacunes auxquels il faut encore remédier. En outre, l'utilisation impropre des technologies exacerbe les obstacles à la promotion de la coopération internationale, ce qui souligne la nécessité de mettre en place des stratégies globales pour atténuer ces risques et encourager une utilisation responsable des outils technologiques dans les efforts collaboratifs.

73. Les États Membres doivent promouvoir, en coopération avec l'ONUUDC et d'autres organisations internationales, l'assistance technique et la formation afin de renforcer les compétences des praticiennes et praticiens et des autorités centrales concernant l'utilisation de la technologie, le but étant de renforcer la coopération internationale³⁹. Selon l'une des recommandations issues de 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, organisé lors du Congrès des Nations Unies pour la prévention du crime et la justice pénale qui s'est tenu à Kyoto, il faudrait que les États Membres s'efforcent 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 qui sont équipés et dotés de moyens d'action pour en bénéficier pleinement⁴⁰.

74. L'Initiative mondiale sur le traitement des preuves électroniques a été lancée en 2017 par l'ONUUDC, en collaboration avec la Direction exécutive du Comité contre le terrorisme et l'International Association of Prosecutors. Elle vise à renforcer les capacités dont disposent : a) les services de détection et de répression pour repérer, recueillir, acquérir et préserver les données électroniques nécessaires aux enquêtes sur les infractions de terrorisme et d'autres infractions graves ; b) les autorités de poursuite et les autorités judiciaires pour utiliser ces données comme preuves devant les tribunaux ; et c) les autorités centrales et compétentes pour traiter et échanger ces données indépendamment des frontières et des périmètres de compétence, sans en compromettre la recevabilité et la valeur probante devant les tribunaux⁴¹.

75. En mai 2021, l'Initiative mondiale a lancé le Centre d'information sur les preuves électroniques (Electronic Evidence Hub), un guichet unique proposant divers outils pratiques conçus expressément pour répondre aux besoins des services de détection et de répression, des autorités judiciaires et des autorités centrales⁴². Le Centre d'information comprend toutes sortes de ressources, parmi lesquelles les première et deuxième éditions du Guide pratique sur la demande de preuves électroniques à l'étranger, le panorama des fournisseurs de services, le module de formation des formateurs et le catalogue des exercices transfrontières (Catalogue of Cross-Border Exercises)⁴³.

76. Le Programme mondial contre la cybercriminalité a pour mandat d'aider les États Membres à lutter contre la cybercriminalité grâce au renforcement de leurs capacités et à une assistance technique. L'assistance technique et la coopération internationale jouent un rôle essentiel pour ce qui est de faciliter la mise en commun d'informations essentielles, de promouvoir l'échange de meilleures pratiques d'enquête et de développer les compétences spécialisées dans le domaine du cyberspace.

77. Dans le cadre de ses six domaines d'intervention (preuves numériques, cyberenquêtes, actifs virtuels, atteintes sexuelles visant les enfants en ligne, prévention et criminalistique numérique), le Programme mondial contre la cybercriminalité travaille avec un large éventail d'acteurs, notamment le secteur de la justice, les ministères de l'éducation, les fournisseurs de services de communication, les entreprises technologiques et les sociétés privées. Il a ainsi aidé les États Membres à améliorer leur connaissance et leur compréhension des preuves numériques et de la façon de demander celles-ci aux entreprises technologiques et aux fournisseurs de services de communication. Dans le domaine de l'exploitation et des atteintes sexuelles visant les enfants en ligne, il a encouragé l'utilisation de logiciels spécialisés qu'il a mis à disposition. Cette technologie permet non seulement d'accélérer les enquêtes pénales, mais aussi de garantir l'échange sécurisé de données

³⁹ A/CONF.234/11, par. 82 l).

⁴⁰ A/CONF.234/16, par. 192 j).

⁴¹ E/CN.15/2022/6, par. 25 ; CTOC/COP/2022/6, par. 47.

⁴² Disponible à l'adresse <https://sherloc.unodc.org/cld/en/st/evidence/electronic-evidence-hub.html>.

⁴³ CTOC/COP/2022/6, par. 48.

dans les affaires qui font intervenir des contenus montrant des atteintes sexuelles sur enfant. Dans le domaine de la criminalistique numérique, le Programme mondial a été le fer de lance de la création de laboratoires de criminalistique numérique et il a fait bénéficier les professionnels de services de détection et de répression d'une formation complète sur l'extraction de preuves numériques à partir de sources en nuage, afin de les doter des compétences requises pour exploiter efficacement ces preuves.

78. Dans le cadre de l'initiative STARSOM visant à renforcer l'action et la lutte transrégionales menées contre le trafic illicite de personnes migrantes, qui a permis aux pays situés le long des itinéraires de trafic transcontinentaux, de l'Asie du Sud à l'Amérique du Nord, de collaborer plus étroitement afin de lutter efficacement contre ce trafic tout en protégeant la vie et en défendant les droits des personnes qui en font l'objet, l'ONUDC a aidé à la création d'unités spéciales, en accordant une attention particulière à la formation à la collecte de preuves électroniques, aux dispositifs mobiles d'extraction de données numériques et à la criminalistique mobile, ou au rassemblement d'éléments décrivant les ressorts du trafic illicite de personnes migrantes. Cela pourrait contribuer à la détection précoce des affaires de trafic et à leur renvoi aux fins d'enquête et de poursuites dans de nombreux pays⁴⁴.

III. Conclusions et recommandations

79. Le Groupe de travail souhaitera peut-être recommander à la Conférence des Parties à la Convention contre la criminalité organisée de prendre les mesures suivantes :

a) Encourager les États parties à rationaliser les mécanismes de coopération internationale grâce à l'utilisation de la technologie et d'outils novateurs par les praticiennes et praticiens et les autorités compétentes, équipés et dotés des moyens requis pour en bénéficier pleinement ;

b) Encourager les États parties à organiser des activités de formation destinées aux autorités centrales et autres autorités compétentes intervenant dans la coopération internationale en matière pénale, ainsi qu'aux autres professions concernées, pour leur permettre d'utiliser efficacement et dans le respect des droits humains les technologies modernes dont ils disposent ; et inviter le secrétariat, sous réserve de la disponibilité de ressources, à élaborer et à mettre en œuvre des activités d'assistance technique dans ce domaine ;

c) Encourager les États parties à surveiller et à bien cerner les risques que présente l'utilisation malveillante des technologies, et à promouvoir des normes éthiques régissant leur utilisation à des fins de coopération internationale ;

d) Encourager les États parties à échanger, lors de rencontres organisées dans le cadre de la Conférence des Parties à la Convention contre la criminalité organisée, des informations sur les bonnes pratiques suivies, les difficultés rencontrées et les propositions formulées s'agissant de renforcer la coopération internationale en matière pénale grâce à l'utilisation de la technologie et d'outils novateurs.

⁴⁴ Voir ONUDC, *The scope of transcontinental migrant smuggling from South Asia to North America*, initiative STARSOM (Strengthening transregional action and responses against the smuggling of migrants), 2023, p. 41.