Nations Unies CTOC/COP/WG.3/2015/2

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

Distr. générale
18 août 2015
Français
Original: anglais

Groupe de travail sur la coopération internationale
Vienne, 27-28 octobre 2015
Point 2 de l'ordre du jour provisoire*
Collecte et partage de preuves électroniques

Collecte et partage de preuves électroniques

Document d'information établi par le Secrétariat

I. Introduction

1. Les infractions faisant intervenir des preuves électroniques présentent des difficultés particulières pour les autorités chargées d'adopter des mesures adéquates pour y faire face, tant au niveau national (législateurs, enquêteurs, procureurs et juges) que sur le plan de la coopération internationale.

2. D'une manière générale, les preuves électroniques peuvent comprendre n'importe quelle donnée générée ou conservée sous forme numérique chaque fois qu'il est fait usage d'un ordinateur. Cela englobe les informations saisies manuellement par un particulier sur un appareil électronique, les informations générées lors du traitement d'une opération informatique ou de la réponse à la demande d'un particulier, lorsque des appareils électroniques génèrent des informations de façon automatique, ou les informations produites et stockées, lorsque des appareils traitent les informations dans leur matrice de données. Peuvent donc constituer des preuves électroniques toutes les informations saisies, générées ou conservées dans des bases de données, des systèmes d'exploitation, des programmes d'application, des modèles générés par ordinateur servant à extrapoler des résultats, des messages électroniques et vocaux, ou même des instructions demeurées inactive dans la mémoire d'un ordinateur[1].

3. Le présent document, établi par le Secrétariat, présente des informations générales sur des éléments et concepts de base en matière de preuves électroniques

* CTOC/COP/WG.3/2015/1.

[1] Ireland Law Reform Commission, "Documentary and Electronic Evidence", document d'information, décembre 2009, p. 8.

et vise à faciliter les travaux du Groupe de travail au titre du point de l'ordre du jour correspondant.

II. Collecte et partage de preuves électroniques: questions à examiner et mesures adoptées aux niveaux national et international

4. La collecte et le partage de preuves électroniques sont étroitement liés, de sorte que les législations nationales et les accords ou arrangements régionaux et internationaux prévoient souvent des pouvoirs d'enquête pour recueillir les preuves électroniques ainsi que des mécanismes de coopération destinés à les partager.

A. Collecte de preuves électroniques

1. Cadres juridiques nationaux

5. Les règles de procédure pénale traditionnelles contiennent généralement des dispositions concernant la collecte et la recevabilité des preuves. En ce qui concerne les preuves se présentant sous forme électronique, les données informatiques et les dossiers électroniques peuvent être facilement modifiés. La collecte et la gestion des preuves électroniques devraient donc en garantir l'intégrité, la continuité et l'authenticité, depuis leur saisie jusqu'à leur utilisation dans les procès.

a) Pouvoirs légaux en matière de collecte et de gestion de preuves électroniques

6. Les pouvoirs d'enquête nationaux jouent un rôle déterminant dans la collecte de preuves électroniques. Comme l'indique l'Étude sur la cybercriminalité réalisée par l'ONUDC, les États peuvent, afin de conduire des enquêtes efficaces et recueillir des preuves électroniques, adopter une législation procédurale conférant les pouvoirs voulus aux services de détection et de répression compétents. Ces pouvoirs peuvent inclure l'application des règles de procédure traditionnelles, des pouvoirs d'enquête généraux interprétés au sens large, des pouvoirs d'enquête prévus pour la mise en œuvre d'un ensemble de mesures spécifiquement adaptées à la cybercriminalité et des pouvoirs d'enquête complets mis en place en vue d'obtenir des preuves électroniques[2].

7. Comme le souligne également l'Étude sur la cybercriminalité, l'examen des fondements juridiques des pouvoirs exercés dans les enquêtes relatives aux infractions pour lesquelles il existe des éléments de preuve électroniques révèle que les approches adoptées sur le plan national sont très variées. Ces approches sont d'abord liées à la mesure dans laquelle les pouvoirs "traditionnels" peuvent être interprétés comme étant applicables aux données intangibles, ainsi qu'à la mesure dans laquelle il existe une autorisation légale pour adopter des mesures intrusives, comme les enquêtes de criminalistique informatique à distance.

---

[2] ONUDC, Comprehensive Study on Cybercrime: Draft – 2013, document établi par l'ONUDC pour examen par le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité (www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf), chap. 5, p. 125.

8. Néanmoins, si leurs pouvoirs judiciaires varient, les États ayant contribué à l'Étude sur la cybercriminalité semblent s'accorder assez largement sur les types de pouvoirs d'enquête auxquels il devrait être possible de recourir pour collecter des preuves électroniques. Parmi les mesures évoquées figurent la protection rapide des données informatiques; l'injonction de produire des données stockées relatives au contenu; l'injonction de produire des données stockées relatives au trafic; l'injonction de communiquer des informations concernant les abonnés; la collecte en temps réel des données relatives au contenu; la collecte en temps réel des données relatives au trafic; la perquisition de matériel ou de données informatiques; la saisie de matériel ou de données informatiques; l'accès transfrontière à un système ou à des données informatiques; et le recours à des outils d'enquête criminalistique à distance[3].

9. Pour enquêter efficacement sur la cybercriminalité et recueillir des preuves électroniques s'y rapportant, les services de détection et de répression accordent ces dernières années une importance croissante à la coopération avec d'autres acteurs concernés, y compris ceux du secteur privé. D'une manière générale, les fournisseurs d'accès Internet jouent un rôle important en matière d'accessibilité aux preuves électroniques. Les lois nationales relatives à la protection de la vie privée peuvent également influer sur la capacité des fournisseurs d'accès Internet à transmettre des renseignements aux services compétents dans le cadre d'une enquête. Les États peuvent ainsi, par exemple, imposer des restrictions sur le type de données auxquelles il est possible d'accéder, fixer des délais d'accès, exiger l'existence de "motifs raisonnables et suffisants", et assurer le contrôle des poursuites et procédures judiciaires[4]. En raison des dispositions prévues dans la législation nationale en matière de protection de la vie privée, les fournisseurs d'accès Internet peuvent être tenus de ne pas divulguer les informations dont elles disposent sur leurs abonnés (renseignements personnels, données relatives au contenu et données relatives au trafic). Parallèlement aux lois en vigueur au niveau national, le droit international des droits de l'homme établit des normes spécifiques pour le respect de la vie privée des personnes qui font l'objet d'une enquête menée par les services de détection et de répression.

10. Compte tenu de l'importance des fournisseurs d'accès Internet dans la collecte de preuves électroniques, le Conseil de l'Europe a adopté les "Lignes directrices pour la coopération entre organes de répression et fournisseurs de services Internet contre la cybercriminalité". Ces lignes directrices visent à aider les services de détection et de répression et les fournisseurs d'accès Internet à bien structurer leurs interactions sur les questions relatives à la cybercriminalité. Elles se veulent souples et sont applicables à n'importe quel pays, dans le respect de la législation nationale et des droits fondamentaux des citoyens. Elles encouragent notamment les services de détection et de répression et les fournisseurs d'accès Internet à échanger des informations; à promouvoir une culture de coopération; à élaborer des procédures

---

[3] On trouvera des exemples de lois nationales relatives à ces mesures d'enquête dans le répertoire en ligne de l'ONUDC sur la cybercriminalité (http://cybrepo.unodc.org) et sur le portail SHERLOC (http://sherloc.unodc.org).

[4] Comprehensive Study on Cybercrime, chap. 5, p. 134.

écrites de coopération mutuelle; à envisager l'établissement de partenariats officiels; et à protéger les droits fondamentaux des citoyens[5].

b) Renforcement des capacités de traitement des preuves électroniques au sein des services de détection et de répression et du système de justice pénale

11. De par leur nature même, les preuves électroniques sont fragiles. Elles peuvent être altérées, endommagées ou détruites si elles font l'objet d'un traitement ou d'un examen inapproprié. C'est pourquoi des précautions spéciales devraient être prises pour identifier, collecter, conserver et examiner ce type de preuves. Faute de quoi, elles risquent de s'avérer inutilisables ou d'entraîner des conclusions erronées.

12. Le renforcement des capacités nationales dans les domaines de la détection et la répression et de la justice pénale est donc capital. La majorité des pays ont commencé à mettre en place des structures spécialisées chargées d'enquêter sur la cybercriminalité et les infractions pour lesquelles il existe des éléments de preuve électroniques, mais les ressources et les capacités dont disposent ces structures sont souvent insuffisantes. Alors que l'existence de preuves numériques se banalise dans les enquêtes sur des infractions classiques, les services de détection et de répression peuvent être amenés à établir des distinctions claires entre les enquêteurs travaillant sur des affaires de cybercriminalité et le personnel des laboratoires de criminalistique numérique, et à définir clairement l'articulation de leurs activités respectives. Les agents de première ligne auront probablement également de plus en plus besoin d'acquérir des compétences de base et de les mettre à profit, par exemple pour produire une copie-image fiable d'un appareil de stockage électronique.

13. L'utilisation de nouvelles technologies, telles que les réseaux d'anonymisation, le cryptage de haut niveau et les monnaies virtuelles, étant devenue chose courante dans les infractions faisant intervenir des preuves électroniques, les enquêteurs devront également adopter de nouvelles stratégies. Les services de détection et de répression pourraient par exemple chercher à renforcer les partenariats avec des groupes de recherche universitaire qui cherchent à développer de nouvelles méthodes dans des domaines tels que la typologie et l'analyse des opérations impliquant des monnaies virtuelles[6]. Les enquêteurs devront peut-être également étudier la façon dont les techniques d'enquête spéciales, comme la surveillance, les opérations d'infiltration, le recours à des informateurs et à des livraisons surveillées dans le cas de la vente en ligne de marchandises illicites, pourraient être utilisées parallèlement aux enquêtes sur Internet et aux techniques de criminalistique numérique afin de collecter des éléments de preuve électroniques sensibles et fragiles. De manière générale, il est clair que le renforcement des capacités des agents de détection et de répression et des acteurs de la justice pénale, aux fins de la lutte contre la cybercriminalité et les infractions impliquant l'existence de preuves

---

[5] Lignes directrices pour la coopération entre organes de répression et fournisseurs de services Internet contre la cybercriminalité, disponibles à l'adresse: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_fr.pdf.

[6] Voir, par exemple, Sarah Meiklejohn et autres, "A fistful of bitcoins: characterizing payments among men with no names", dans Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference (New York, ACM, 2013).

électroniques, sera un processus permanent et continu, étant donné la vitesse à laquelle évoluent les technologies et les activités criminelles[7].

c) Le rôle des structures ou unités spécialisées dans la cybercriminalité: approches nationales

14. Les services nationaux de détection et de répression se spécialisent de plus en plus fréquemment dans la conduite d'enquêtes relatives à la cybercriminalité et aux infractions pour lesquelles interviennent des éléments de preuves électroniques. Cette spécialisation est primordiale pour faciliter les processus de collecte, d'analyse et de partage de preuves électroniques. Elle se justifie avant tout par la nature particulière de la cybercriminalité, qui présente des difficultés spécifiques concernant la définition des infractions, l'applicabilité des lois ainsi que la collecte et l'analyse des preuves. Le niveau des compétences et capacités techniques des services de détection et de répression aura donc une incidence directe sur l'efficacité des mesures de prévention du crime et de justice pénale adoptées pour lutter contre la cybercriminalité[8]. Par ailleurs, compte tenu de la place grandissante qu'occupent au quotidien les appareils électroniques, Internet et la connectivité mondiale, l'exploitation de preuves électroniques telles que les SMS, les courriels et les données de navigation sur Internet est devenue chose courante dans beaucoup d'enquêtes "classiques"[9]. De ce fait, à tous les niveaux des services de détection et de répression (aussi bien sur le plan local que national), on constate également un besoin croissant de disposer au minimum de compétences de base pour enquêter sur la cybercriminalité.

15. D'après l'Étude sur la cybercriminalité, les techniques d'enquête sur la cybercriminalité en général étaient le domaine dans lequel une assistance technique était requise. Parmi les pays nécessitant une assistance, 60 % ont déclaré que les services de détection et de répression avaient besoin d'une assistance dans ce domaine[10]. Les États ayant communiqué des informations aux fins de cette étude ont en outre indiqué que, très souvent, les antennes de police locales transféraient les affaires de cybercriminalité à un organe responsable de la détection et de la répression au niveau national[11].

16. L'implantation de structures ou d'unités spécialisées dans la cybercriminalité au sein même des services de détection et de répression peut aider les États à concentrer des ressources limitées en un même lieu, afin de développer des techniques d'enquête spécialisées, de collecter et d'analyser efficacement les preuves électroniques et de réaliser des expertises de criminalistique numérique. Parallèlement, ces structures ou unités peuvent former les services locaux de détection et de répression, coordonner les mesures nationales de lutte contre la cybercriminalité, faciliter la coopération entre les partenaires impliqués dans les

---

[7] Treizième Congrès des Nations Unies pour la prévention du crime et la justice pénale, Document d'information établi par le Secrétariat pour l'Atelier 3: Renforcement des mesures en matière de prévention du crime et de justice pénale visant à combattre les formes de criminalité en constante évolution, notamment la cybercriminalité et le trafic de biens culturels, enseignements tirés et coopération internationale, A/CONF.222/12, par. 37 et 38.

[8] Comprehensive Study on Cybercrime, chap. 5, p. 152.

[9] Voir note de bas de page 7 ci-dessus, A/CONF.222/12, par. 16.

[10] Comprehensive Study on Cybercrime, Executive Summary, p. xxiii.

[11] Comprehensive Study on Cybercrime, chap. 5, p. 118.

enquêtes, et cibler les formes de cybercriminalité susceptibles d'être particulièrement préoccupantes pour les pouvoirs publics, comme la pédopornographie sur Internet, la criminalité liée à l'identité, les fraudes et escroqueries par Internet, etc.

d) Recevabilité des preuves électroniques devant les tribunaux

17. Une fois que les preuves électroniques sont collectées et partagées, il faudrait idéalement qu'elles soient recevables dans le cadre des procédures pénales. Le droit de la preuve repose traditionnellement sur des documents papier, bien que le recours au témoignage oral et à des objets matériels ait toujours eu sa place dans les procédures judiciaires. Cela étant, l'importance croissante des éléments de preuve électroniques dans les procédures pénales soulève des questions qui ne se posaient pas auparavant; de ce point de vue, l'Étude sur la cybercriminalité a permis de faire un état des lieux des approches juridiques nationales concernant la recevabilité de ce type de preuves devant les juridictions pénales.

18. En l'occurrence, 85 % des pays ayant répondu ont déclaré que les preuves électroniques étaient recevables dans le cadre des procédures pénales. La plupart des pays admettant ce type de preuves ont indiqué qu'elles étaient considérées de la même façon que les preuves matérielles. Moins de 40 % des pays ont signalé qu'une distinction juridique existait entre preuves électroniques et matérielles. Quelques rares pays ont indiqué l'existence de lois régissant spécifiquement les preuves électroniques; dans ces cas-là, les lois en question portaient sur des questions telles que les conditions juridiques établissant la qualité de propriétaire ou d'auteur de données et de documents électroniques, ainsi que sur les critères permettant de juger de l'authenticité des preuves électroniques[12].

2. Coopération internationale

19. Les infractions impliquant des preuves numériques constituent un défi unique pour la coopération internationale. En raison de la nature transitoire des preuves électroniques, la coopération internationale dans le domaine de la cybercriminalité suppose qu'une réponse rapide soit apportée et que des mesures d'enquête spécialisées, dont la conservation et la production de données par des prestataires du secteur privé, puissent être demandées. Les obstacles fréquemment rencontrés dans le cadre des demandes adressées à d'autres pays pour obtenir ce genre de données sont notamment les délais de réponse, le manque de volonté et de flexibilité de la part des autorités sollicitées, la forme sous laquelle les preuves sont fournies aux juridictions ayant présenté la demande et l'usage qui peut être fait de ces preuves dans les procédures pénales, ainsi que les différences existant d'un pays à l'autre quant à la définition des infractions pénales[13].

20. S'il existe de nombreux modes de coopération informelle entre les services de détection et de répression, notamment des réseaux accessibles en permanence, les pays continuent de s'appuyer fortement sur les moyens judiciaires officiels, en particulier les instruments bilatéraux d'entraide judiciaire, pour obtenir des preuves

---

[12] Comprehensive Study on Cybercrime, chap. 6, p. 165 à 167.

[13] ONUDC, Comparative study on current practices in electronic surveillance in the investigation of serious and organized crime, p. 9 (www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf).

électroniques extraterritoriales; plus de 70 % des pays formulent ainsi des demandes officielles d'entraide judiciaire[14]. En général, pour les enquêtes sur la cybercriminalité, les délais de réponse à ces demandes sont d'environ 150 jours. Souvent, ces délais peuvent excéder la durée de conservation des données appliquée par les prestataires de services ou permettre aux délinquants de détruire définitivement des preuves numériques capitales.

21. C'est pourquoi, dans les affaires impliquant des preuves numériques, l'efficacité de la coopération internationale passe par l'existence de mécanismes permettant d'assurer rapidement la conservation des données en attendant que d'autres mesures d'enquête soient envisagées. Cette coopération pourrait également être renforcée si des approches communes étaient adoptées pour formuler des demandes relatives à des formes particulières de preuves, notamment les preuves acquises à travers les réseaux, les journaux de connexion et l'imagerie judiciaire.

22. Certains instruments multilatéraux existants établissent des mécanismes qui visent à faciliter l'accès aux données pour les services de détection et de répression, notamment des points de contact joignables 24 heures sur 24 pendant les enquêtes, l'accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public, et les demandes urgentes d'entraide.

23. La Convention du Conseil de l'Europe sur la cybercriminalité prévoit par exemple l'établissement de points de contact joignables 24 heures sur 24 et 7 jours sur 7 qui faciliteront ou, si le droit et la pratique internes le permettent, appliqueront directement les mesures suivantes: i) apport de conseils techniques; ii) conservation des données; et iii) recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

24. Un certain nombre d'accords internationaux traitent de questions relatives à la collecte des preuves électroniques. La Convention du Conseil de l'Europe sur la cybercriminalité, par exemple, précise que les dispositions de droit procédural qu'elle énonce s'appliquent aux pouvoirs et procédures mis en place aux fins de la collecte des preuves électroniques de toute infraction pénale.

25. Des dispositions relatives aux fournisseurs d'accès Internet figurent dans le projet de loi type sur la cybersécurité (2011) élaboré par le Marché commun de l'Afrique de l'Est et de l'Afrique australe (COMESA). Ces dispositions portent notamment sur les points suivants: obligations de contrôle (art. 17); communication d'informations à titre volontaire (art. 17 b)); notifications de retrait (art. 16); responsabilité des fournisseurs d'accès (art. 12); stockage en mémoire cache (art. 13), hébergement (art. 14) et fournisseurs d'hyperliens/moteurs de recherche (art. 15). D'autre part, des dispositions similaires, quoique moins nombreuses, figurent dans la directive 2000/31/EC de l'Union européenne et dans les modèles de textes législatifs élaborés par l'Union internationale des télécommunications (UIT), la Communauté des Caraïbes (CARICOM) et l'Union des télécommunications des Caraïbes (CTU) sur les thèmes: i) cybercriminalité et ii) preuve électronique.

26. Une coopération informelle peut être établie entre différents services de détection et de répression afin de recueillir des preuves électroniques provenant d'autres pays. Ce type de coopération peut faciliter la mise en œuvre de diverses mesures visant à obtenir des preuves extraterritoriales, notamment des perquisitions

[14] Comprehensive Study on Cybercrime, Executive Summary, p. xxv.

et des saisies; la conservation des données informatiques et l'injonction de communiquer ce type de données; la collecte des données en temps réel; le recours à des outils d'enquête criminalistique à distance; et la possibilité pour les services de détection et de répression d'accéder directement aux données extraterritoriales[15].

27. Les services de détection et de répression devront peut-être trouver des façons toujours plus innovantes de collaborer dans les enquêtes transnationales sur la cybercriminalité. Le fait que des entités telles que le Complexe mondial INTERPOL pour l'innovation[16] et le Centre européen de lutte contre la cybercriminalité de l'Office européen de police (Europol)[17] participent à la coordination des enquêtes transnationales et y apportent leur soutien pourrait se révéler particulièrement important à cet égard. D'autres forums et initiatives, comme la Conférence mondiale sur le cyberespace, ont également fourni aux pays une occasion d'envisager des mesures innovantes dans le domaine de la coopération internationale contre la cybercriminalité.

28. L'informatique en nuage constitue aussi un défi grandissant pour la coopération internationale, car les services informatiques sont de plus en plus souvent transférés vers des serveurs et des centres de données dispersés sur le plan géographique, ce qui rend difficile la "localisation" des preuves électroniques[18]. Un utilisateur de Google, par exemple, peut avoir accès à des données qui sont stockées ou traitées en Amérique du Nord, en Asie du Sud-Est, en Europe du Nord ou en Europe occidentale[19].

B. Partage de preuves électroniques

1. Cadres juridiques nationaux

29. Certains États ont mis en place une législation interne qui prévoit le partage de preuves dans le cadre de la coopération internationale. En matière d'entraide judiciaire, la législation interne de plusieurs États autorise également le partage de preuves électroniques.

2. Coopération internationale

30. Pour faciliter le partage de preuves électroniques avec d'autres pays, les États ont la possibilité de conclure des accords bilatéraux, régionaux et internationaux. Ces accords peuvent prévoir une assistance pour la conservation de données informatiques; une assistance pour la saisie, la consultation, la collecte et la divulgation de données informatiques; l'accès transfrontière à des données informatiques; la communication spontanée de renseignements et l'échange d'informations; et des demandes d'entraide judiciaire d'ordre général[20]. Les dispositions figurant dans ce type d'accords constituent des sources primaires du droit et établissent à la fois les droits et les obligations des parties, qui sont donc

---

[15] Comprehensive Study on Cybercrime, chap. 5, p. 126 à 133.

[16] http://www.interpol.int/fr/Internet/%C3%80-propos-d'INTERPOL/Le-Complexe-mondial-INTERPOL-pour-l%E2%80%99innovation.

[17] www.europol.europa.eu/ec3.

[18] Comprehensive Study on Cybercrime, chap. 7, p. 216.

[19] Comprehensive Study on Cybercrime, chap. 7, p. 216 et 217.

[20] Comprehensive Study on Cybercrime, annexe 3, p. 273 et 274.

soumises à des modalités juridiques contraignantes. Toutefois, les États n'ont pas tous besoin qu'un traité officiel de coopération judiciaire existe pour partager des preuves électroniques: certains peuvent fournir une assistance sur la simple base de la réciprocité ou de la courtoisie internationale.

31. L'examen des accords régionaux et internationaux montre que les États disposent de différents modes de partage des preuves électroniques. Ces formes de coopération incluent les principes généraux de la coopération internationale; des modalités générales d'entraide judiciaire; des mécanismes d'assistance accélérée; une assistance pour la conservation de données informatiques; une assistance pour la saisie, la consultation, la collecte et la divulgation de données informatiques; l'accès transfrontière à des données informatiques; et la communication spontanée de renseignements ainsi que l'échange d'informations. Diverses formes de coopération, parmi celles susmentionnées, sont prévues par les accords ci-après:

Nations Unies, Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants (2000);

Communauté d'États indépendants, Accord de coopération en matière de lutte contre les infractions dans le domaine informatique (2001);

Conseil de l'Europe, Convention sur la cybercriminalité et Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (2001);

Conseil de l'Europe, Convention sur la protection des enfants contre l'exploitation et les abus sexuels (2007);

Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), Projet de directive portant lutte contre la cybercriminalité dans l'espace de la CEDEAO (2009);

Ligue des États arabes, Convention de la Ligue des États arabes sur la lutte contre les infractions liées aux technologies de l'information (2010);

Organisation de Shanghai pour la coopération, Accord pour la coopération dans le domaine de la sécurité internationale de l'information (2010);

Marché commun de l'Afrique de l'Est et de l'Afrique australe (COMESA), Projet de loi type sur la cybersécurité (2011);

Union africaine, Projet de convention portant adoption d'un cadre juridique propice à la cybersécurité en Afrique (2012);

Union européenne, Décision-cadre du Conseil 2001/413/JAI concernant lutte contre la fraude et la contrefaçon des moyens de paiement (2001);

Union européenne, Décision-cadre du Conseil 2005/222/JAI relative aux attaques visant les systèmes d'information (2005);

Union européenne, Proposition de directive du Parlement européen et du conseil COM(2010) 517 final, relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI (2010).

32. Le partage de preuves électroniques s'appuie principalement sur les méthodes de coopération traditionnelles, comme les demandes officielles d'entraide judiciaire. Un certain nombre d'accords bilatéraux, régionaux et internationaux existent pour les procédures d'entraide judiciaire. Parmi les instruments régionaux et internationaux susmentionnés sur la cybercriminalité, beaucoup comportent des dispositions relatives à l'entraide judiciaire. Les procédures et les demandes d'entraide judiciaire se font essentiellement selon des modalités dictées par des accords régionaux et bilatéraux. Le Traité d'entraide juridique en matière pénale conclu en 2004 par l'Association des nations de l'Asie du Sud-Est (ASEAN), ainsi que la Convention européenne d'entraide judiciaire en matière pénale établie en 2000 par le Conseil de l'Europe entre les États membres de l'UE, sont deux exemples d'accords régionaux en la matière.

33. Compte tenu du fait que les preuves électroniques sont souvent fragiles et peuvent facilement être corrompues, les mesures rapides qu'elles exigent ne peuvent pas toujours être mises en œuvre selon des mécanismes de coopération formels. Le recours à des mécanismes informels peut donc également s'avérer utile et les réseaux accessibles en permanence, 24 heures sur 24 et 7 jours sur 7, en particulier, offrent des possibilités considérables pour simplifier ce type de coopération ou même, par la suite, faciliter la coopération formelle. Cependant, les moyens d'enquêtes rendus disponibles par la coopération informelle peuvent varier considérablement. Pour le partage de preuves électroniques, l'une des principales difficultés posées par ce type de coopération découle du fait que de nombreux pays interdisent, dans le cadre des procédures judiciaires, l'utilisation des preuves obtenues par le biais de mécanismes informels[21].

34. Dans le cadre de leur contribution à l'Étude sur la cybercriminalité, les pays ayant recours à la coopération informelle ont indiqué que les mécanismes nécessaires à cette coopération étaient conditionnés par l'existence d'un interlocuteur étranger compétent et bien organisé. Certains pays ont fait observer que c'était plus souvent le cas lorsqu'il existait une forme d'accord régissant la coopération informelle entre services de détection et de répression. Un certain nombre de pays ont indiqué que, de ce fait, la coopération informelle se fondait sur des accords régionaux et bilatéraux, au travers de réseaux établis par des organisations et institutions internationales et régionales; avec l'appui des ambassades et consulats; et par l'intermédiaire de réseaux privés établis entre responsables des services de détection et de répression.

35. Ainsi, l'article 27 de la Convention des Nations Unies contre la criminalité transnationale organisée, qui contient des dispositions relatives à la coopération des services de détection et de répression, encourage les États à envisager de conclure des accords ou des arrangements bilatéraux ou multilatéraux permettant une coopération directe entre différents services de détection et de répression. Par ailleurs, les États ont aussi adopté diverses lois relatives à la coopération des services de détection et de répression, y compris sur l'échange d'informations, les enquêtes conjointes, la surveillance électronique ou d'autres formes de surveillance, etc.

---

[21] Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, chap. 4, p. 47, disponible à l'adresse www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.

36. Tandis que certains pays font état d'une coopération directe entre les services de police, d'autres privilégient une coopération informelle par l'intermédiaire d'INTERPOL, dont les bureaux, établis dans 190 pays, sont souvent en relation avec les services nationaux de détection et de répression[22]. Ces bureaux peuvent donc contribuer à l'établissement de relations informelles, et par conséquent favoriser des solutions susceptibles de remplacer efficacement les procédures formelles de coopération internationale.

37. Qu'elles soient formelles ou informelles, les procédures de coopération concernant les preuves électroniques en matière pénale peuvent se heurter à un certain nombre d'obstacles qui entravent la collecte et le partage de ce type de preuves. Il peut s'agir par exemple de divergences quant au champ d'application que les instruments multilatéraux et bilatéraux attribuent aux dispositions relatives à la coopération, du fait qu'aucun délai n'est exigé pour répondre à une demande, de la multiplicité des réseaux informels établis entre services de détection, ou encore de disparités entre les garanties offertes en matière de coopération[23].

III. Outils élaborés par l'Office des Nations Unies contre la drogue et le crime

38. Ces dernières années, l'ONUDC a mis au point plusieurs outils permettant d'aborder la question des preuves électroniques selon différents points de vue, disciplines et mandats. Ces outils regroupent un ensemble de connaissances se renforçant mutuellement, souvent recueillies dans le cadre de consultations approfondies avec les États Membres et les acteurs concernés. Cette combinaison multiforme d'outils de connaissances relatives à la collecte et au partage de preuves électroniques permet de mener des activités variées, allant de l'analyse fondée sur la recherche des formes spécifiques de criminalité, jusqu'à l'accès direct à des ressources juridiques via des plates-formes électroniques.

39. Bien qu'aucun outil de l'ONUDC ne soit consacré exclusivement à la question des preuves électroniques, on trouvera ci-après un aperçu des outils pratiques et travaux de recherche pouvant présenter un intérêt en la matière.

A. Études de l'Office des Nations Unies contre la drogue et le crime, réalisées conformément aux résolutions de l'Organisation des Nations Unies

40. Dans le cadre des mandats confiés au Conseil économique et social, l'ONUDC a entrepris ces dernières années de réaliser les études ci-après, qui abordent notamment la question de la collecte et du partage de preuves électroniques relatives à certaines formes de criminalité: a) *Handbook on Identity-related Crime*[24]; et b) Study on the Effects of New Information Technologies on the Abuse and

---

[22] Comprehensive Study on Cybercrime, chap. 7, p. 187.

[23] Comprehensive Study on Cybercrime, chap. 7, p. 197 à 215.

[24] www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.

Exploitation of Children[25] (ci-après dénommée “Étude sur la maltraitance et l’exploitation des enfants”).

41. De même, en application des résolutions 65/230 et 67/189 de l’Assemblée générale, l’ONUDC a fourni des services de secrétariat et un soutien technique aux réunions du groupe intergouvernemental d’experts à composition non limitée chargé de réaliser une étude approfondie sur le problème de la cybercriminalité. À cette occasion, sur la base des informations communiquées par les États Membres, il a établi un projet d’étude approfondie sur la cybercriminalité, auquel il est fait référence dans différentes parties du présent document d’information.

1. Manuel sur la criminalité liée à l’identité

42. Publié par l’ONUDC en 2011, en application des résolutions 2007/20 et 2009/22 du Conseil économique et social relatives à la coopération internationale en matière de prévention, d’enquêtes, de poursuites et de sanctions concernant la fraude économique et la criminalité liée à l’identité, le manuel intitulé “Handbook on identity-related crime” met l’accent sur certaines questions juridiques et politiques en rapport avec la criminalité liée à l’identité, notamment la collecte et l’utilisation de données et informations électroniques. Il vise principalement à présenter une série d’options et d’éléments à prendre en compte pour aborder les questions relatives à la justice pénale interne (typologie de la criminalité, approches en matière d’incrimination, protection des victimes), certaines difficultés spécifiques dans le domaine de la coopération internationale en matière pénale ou les possibilités offertes par les synergies et partenariats entre les secteurs public et privé, en particulier pour ce qui est de la prévention de la criminalité liée à l’identité. Le manuel combine des éléments reposant sur des documents de recherche et d’autres axés sur la pratique, ce qui contribue à éclairer différents aspects et paramètres des problèmes complexes que pose cette forme de criminalité.

43. Compte tenu de la diversité des questions abordées, le manuel est destiné aux législateurs, décideurs, services de poursuite, de détection et de répression et praticiens, ainsi qu’à d’autres acteurs concernés (représentants d’organisations internationales et intergouvernementales actives dans ce domaine, représentants du secteur privé et experts des milieux universitaires).

44. Le manuel peut également être utilisé à des fins didactiques dans les programmes d’assistance technique et les activités de renforcement des capacités, en vue de parfaire les connaissances spécialisées dont on dispose pour traiter les problèmes juridiques, institutionnels et opérationnels relatifs à la nouvelle forme de criminalité qu’est la criminalité liée à l’identité.

45. Par ailleurs, le guide pratique sur la coopération internationale dans la lutte contre la criminalité liée à l’identité, figurant dans le manuel, offre un aperçu des différents aspects de la dimension transnationale de la criminalité liée à l’identité et contient des informations de base et des orientations sur la manière de traiter au mieux les demandes de coopération internationale dans ce domaine, en donnant notamment des exemples d’affaires pertinentes.

---

[25] Voir note de bas de page 21.

2. Étude sur les effets des nouvelles technologies de l'information sur la maltraitance et l'exploitation des enfants

46. Pour donner suite à la résolution 2011/33 du Conseil économique et social, intitulée "Prévention, protection et coopération internationale contre l'utilisation des nouvelles technologies de l'information à des fins de maltraitance ou d'exploitation des enfants", l'ONUDC a publié en 2015 une étude sur les effets des nouvelles technologies de l'information sur la maltraitance et l'exploitation des enfants (initialement présentée à la vingt-troisième session de la Commission pour la prévention du crime et la justice pénale, en mai 2014). Cette étude se fonde sur des recherches menées à ce sujet à partir de sources librement accessibles, ainsi que sur les travaux d'un groupe d'experts que l'ONUDC a réuni à Vienne du 23 au 25 septembre 2013, et qui était constitué d'experts issus d'organisations internationales, de représentants de services de détection et de répression, d'autres praticiens compétents et d'universitaires. L'étude présente des éléments d'information générale sur les points suivants:

a) Définitions et termes nouveaux;

b) Typologie des infractions;

c) Types et formes de comportements connexes les plus fréquents;

d) Principales formes de technologies de l'information et de la communication favorisant certains types d'infraction, notamment la maltraitance et l'exploitation des enfants;

e) Profil et degré de sophistication technologique des délinquants;

f) Facteurs de risque de victimisation;

g) Nature des éléments tels que photographies, négatifs, diapositives, magazines, livres, dessins, films, cassettes vidéo et disques ou fichiers informatiques;

h) Types d'appareils ou de plates-formes utilisés à des fins criminelles, notamment: téléphones mobiles, services de stockage à distance dotés de technologies intégrées de cryptage, informatique en nuage et nouvelles applications permettant aux utilisateurs de diffuser de façon temporaire des images qui disparaissent quelques secondes après réception (telles que Snap Chat et Wickr).

47. Par ailleurs, le chapitre III de l'étude est consacré aux enquêtes visant des infractions de maltraitance et d'exploitation des enfants commises à l'aide de technologies de l'information et de la communication.

48. L'étude s'intéresse de près aux possibilités d'accès et d'application pratique que présentent les logiciels et technologies de l'image utilisés par les services de détection et de répression pour identifier les victimes repérées sur des supports en ligne et leur venir en aide, ainsi que pour trier leurs enquêtes criminalistiques en comparant les données numériques des suspects aux images dont ils disposent dans leurs bases de données. L'étude fournit des informations utiles sur les technologies innovantes qui sont utilisées pour réduire les redondances des enquêtes tout en contribuant à protéger les intérêts des victimes. Ces technologies incluent, entre autres:

"PhotoDNA" de Microsoft: logiciel gratuit utilisé pour créer une signature unique associée à une image numérique, semblable à une empreinte digitale, qui peut ensuite être comparée avec les signatures d'autres images afin de trouver des copies de cette image;

Bases de données répertoriant les images de maltraitance et intégrant des informations relatives aux victimes, identifiées ou non identifiées[26];

Base de données internationale d'INTERPOL sur l'exploitation sexuelle des enfants: base de données utilisée pour identifier des victimes jusqu'alors non identifiées et leur venir en aide, grâce à l'utilisation d'un logiciel sophistiqué de comparaison d'images permettant de faire des recoupements entre des victimes et des lieux.

49. Les fournisseurs d'accès Internet ont également recours aux innovations techniques susmentionnées pour trouver, au moyen d'algorithmes, les contenus pédopornographiques et les supprimer de leurs serveurs.

50. Par ailleurs, l'étude présente la criminalistique numérique comme la branche des sciences criminalistiques consacrée à la collecte et à l'analyse des traces numériques générées informatiquement. À cet égard, elle aide à y voir plus clair sur le type de données informatiques et de communications électroniques susceptibles d'être liées à un acte criminel, la variété des formats et des systèmes qu'il est possible d'utiliser pour classer les données collectées, ainsi que les outils employés pour les examiner.

51. L'étude s'intéresse également à l'utilisation d'un logiciel de "recherche automatique" dans les enquêtes criminalistiques. Elle souligne l'intérêt de cet outil pour trouver facilement et rapidement les sites et contenus auxquels sont associés certains mots clefs fréquemment utilisés.

52. L'étude se penche en outre sur les évolutions amorcées au cours des 10 dernières années en matière de développement et de déploiement d'outils technologiques et de logiciels permettant de rechercher rapidement des données utiles dans des milliers de bases de données, documents comptables, échantillons d'ADN, extraits sonores, séquences vidéo, cartes, plans, rapports basés sur le renseignement humain et réseaux sociaux. Ces outils, qui réunissent des données pertinentes et permettent de retracer une trajectoire précise, cohérente et utile, offrent une analyse conceptuelle des corrélations observées.

53. Par ailleurs, l'étude s'intéresse aux opérations d'infiltration dans le cadre d'enquêtes relatives à la criminalité sur Internet, pour tenter d'en évaluer la pertinence et les spécificités.

3. Projet d'étude approfondie sur la cybercriminalité

54. Le chapitre 6 du projet d'étude approfondie sur la cybercriminalité s'intéresse de près à la question des preuves électroniques et de la justice pénale et, en premier lieu, à la nécessité de repérer, de collecter et d'analyser ces preuves au moyen de la criminalistique informatique. Il examine la recevabilité et l'utilité des preuves

[26] Telles que les bases de données mises au point par INTERPOL et le National Center for Missing and Exploited Children (NCMEC), basé aux États-Unis.

électroniques dans les procédures pénales et explique comment, dans le cadre des poursuites, un ensemble de difficultés peuvent influer sur le bon fonctionnement du système de justice pénale. Il établit aussi un lien entre les capacités requises en matière de détection et de répression et en matière de justice pénale, l'accent étant mis sur les activités d'assistance technique déjà mises en place ou nécessaires.

55. D'autre part, certains aspects relatifs aux preuves électroniques sont abordés sous l'angle de la détection et de la répression et de la coopération internationale. Dans cette optique, le chapitre 5 (Détection et répression et enquêtes) porte sur l'examen, l'utilisation, le stockage, la conservation et la préservation des données électroniques susceptibles de constituer des preuves électroniques; la collecte des données en temps réel; le recours à des outils d'enquête criminalistique à distance; la possibilité pour les services de détection et de répression d'accéder directement à des données extraterritoriales; les droits de l'homme et les enquêtes policières; et l'obtention de données auprès de prestataires de services privés. De son côté, le chapitre 7 (Coopération internationale), qui porte sur la question des preuves extraterritoriales provenant de systèmes informatiques en nuage et de prestataires de services, s'attarde sur des domaines tels que la localisation des données; l'accès à des données extraterritoriales lors de la collecte de preuves; l'obtention de données auprès de prestataires de services extraterritoriaux.

B. Outils mis au point par l'Office des Nations Unies contre la drogue et le crime destinés à être utilisés dans le cadre des activités d'assistance technique

56. Les programmes d'assistance technique de l'ONUDC ont conduit à l'élaboration d'outils pratiques qui abordent la question des preuves électroniques du point de vue des praticiens. À cet égard, les participants à la deuxième réunion interrégionale sur le thème "Mise en commun des pratiques en matière de demande et de communication de preuves électroniques dans le cadre des enquêtes et poursuites relatives à la criminalité organisée" ont formulé une série de conseils de base à l'intention des enquêteurs et des procureurs[27] pour faire une demande de preuves électroniques ou de données numériques auprès d'une juridiction étrangère.

57. Cette série de conseils de base fournit des orientations pratiques pour formuler des demandes de preuves électroniques auprès de juridictions étrangères, et notamment pour obtenir ce type de preuves à partir de sources en accès libre ou directement auprès de fournisseurs d'accès Internet établis ou enregistrés dans le pays demandeur en tant que filiales de fournisseurs basés à l'étranger; pour préserver les preuves électroniques avant l'envoi de la demande visant à ce qu'elles soient divulguées; lorsque c'est possible, pour adresser directement la demande au fournisseur d'accès Internet et en envoyer une copie aux services chargés des enquêtes et des poursuites dans le pays requis; pour consulter la cellule chargée de la cybercriminalité sur les aspects techniques relatifs à la demande.

---

[27] Réunion tenue à Tbilissi, du 9 au 11 décembre 2014, dans le cadre de l'initiative de l'ONUDC visant à mettre en place et à renforcer le réseau de procureurs et d'autorités centrales des pays d'origine, de transit et de destination en vue de lutter contre la criminalité transnationale organisée en Asie centrale et dans le sud du Caucase.

58. Conformément à la résolution 7/4 de la Conférence des Parties à la Convention contre la criminalité organisée, l'ONUDC continue de développer des outils de coopération internationale, notamment le Rédacteur de requêtes d'entraide judiciaire. À ce sujet, il a organisé plusieurs réunions informelles d'experts pour étudier une refonte de cet outil et envisager les orientations futures relatives à son utilisation.

59. Lors de la dernière réunion informelle d'experts, en mai 2015, les participants sont convenus d'intégrer à la nouvelle version de cet outil un module consacré aux preuves numériques, qui aiderait les États à présenter des demandes d'assistance pour ce type de preuves. Dans cette optique, les experts ont fait part des expériences de leurs pays respectifs concernant la demande et l'obtention de preuves numériques, en expliquant notamment si des modèles étaient disponibles pour ce genre de démarches et si des approches harmonisées existaient pour la présentation de preuves électroniques. La réunion a donné des orientations à propos du format et de la structure que pourrait avoir le module consacré aux preuves numériques, en mettant l'accent sur différents types de preuves (données stockées dans des appareils, données stockées sur des réseaux, informations concernant des abonnés, données relatives au contenu...). La nouvelle version du Rédacteur de requêtes d'entraide judiciaire devrait être finalisée à l'issue d'une prochaine réunion informelle d'experts, qui se tiendrait les 22 et 23 octobre 2015 à Vienne.

C. Plates-formes de gestion des connaissances de l'Office des Nations Unies contre la drogue et le crime

1. Mise en commun de ressources électroniques et de lois contre la criminalité (SHERLOC)

60. L'ONUDC a poursuivi ses travaux relatifs au développement de SHERLOC, un portail de gestion des connaissances visant à mettre en commun les ressources juridiques disponibles en matière de criminalité. Le portail SHERLOC s'est attaché à rassembler les ressources relatives à différents types de criminalité et aux questions s'y rapportant, entre autres celle des preuves électroniques. Au 18 août 2015, il comprenait 44 textes législatifs établissant des normes en matière de preuves électroniques.

2. Répertoire sur la cybercriminalité

61. Outre le portail SHERLOC, l'ONUDC a créé un répertoire sur la cybercriminalité, qui constitue une base de données centrale permettant de rassembler la législation et les enseignements tirés en la matière, afin de faciliter l'évaluation permanente des besoins et des compétences dans le domaine de la justice pénale ainsi que la mise en œuvre et la coordination des activités d'assistance technique.

62. Lancé en 2015, le répertoire est le premier outil disponible au niveau mondial qui regroupe des textes législatifs, des cas concrets et des enseignements tirés de l'expérience en matière de cybercriminalité et de preuves électroniques, sur la base d'informations communiquées et mises à jour par les États Membres. Cet outil a de multiples objectifs, parmi lesquels: permettre aux législateurs de s'appuyer sur les textes législatifs disponibles dans la base de données lorsqu'ils élaborent des lois

relatives à la cybercriminalité ou aux preuves électroniques; faciliter la coopération internationale en aidant les services de détection et de répression ainsi que les procureurs à repérer les dispositions législatives sur la cybercriminalité qui sont applicables dans d'autres États Membres; et proposer aux utilisateurs des exemples de bonnes pratiques en matière de prévention, d'enquêtes et de poursuites dans le domaine de la cybercriminalité. Les législations nationales sur l'entraide judiciaire ne renvoient pas toutes aux fonctions d'une autorité centrale et ne les fixent pas nécessairement. Lorsqu'elles le font, elles peuvent désigner une institution gouvernementale comme autorité centrale, établir une liste de ses fonctions et, dans certains cas, prévoir une clause de sauvegarde confirmant que la loi ne limite pas le pouvoir de l'autorité d'établir ou recevoir des demandes ou de coopérer avec un État étranger par d'autres voies ou moyens. Par exemple, la loi d'entraide judiciaire d'un pays européen précise que l'autorité centrale "1) reçoit les demandes d'entraide...; 2) prend en charge, soit directement soit par l'intermédiaire d'une [autre] autorité, l'exécution des demandes...; 3) transmet les demandes aux fins d'entraide; et 4) effectue les traductions des documents".

IV. Conclusions et recommandations

63. Le Groupe de travail sur la coopération internationale souhaitera peut-être recommander ce qui suit à la Conférence des Parties:

a) Prier le Secrétariat d'établir, en coopération avec les organisations intergouvernementales concernées et sous réserve de la disponibilité de fonds extrabudgétaires, un manuel sur la collecte et le partage de preuves électroniques;

b) Prier le Secrétariat, dans le cadre de ses efforts pour mettre à niveau les outils de coopération internationale, d'intégrer la question des preuves électroniques;

c) Prier les États Membres de faire savoir au Secrétariat s'il existe des unités ou structures spécialisées sur la cybercriminalité, afin qu'elles soient inscrites au répertoire des autorités centrales nationales.