Nations Unies E/CN.15/2018/6

Conseil économique et social

Distr. générale
22 février 2018
Français
Original : anglais

Commission pour la prévention du crime et la justice pénale
Vingt-septième session
Vienne, 14-18 mai 2018
Point 5 de l'ordre du jour provisoire*
Débat thématique sur les mesures de justice pénale propres à prévenir et à combattre la cybercriminalité sous toutes ses formes, y compris par le renforcement de la coopération aux niveaux national et international

Guide destiné au débat thématique sur les mesures de justice pénale propres à prévenir et à combattre la cybercriminalité sous toutes ses formes, y compris par le renforcement de la coopération aux niveaux national et international

Note du Secrétariat

Résumé

Le présent guide destiné au débat thématique sur les mesures de justice pénale propres à prévenir et à combattre la cybercriminalité sous toutes ses formes, y compris par le renforcement de la coopération aux niveaux national et international, que la Commission pour la prévention du crime et la justice pénale tiendra à sa vingt-septième session, a été établi par le Secrétariat en application de la décision 18/1 de la Commission. Dans sa décision 2016/241, le Conseil économique et social a décidé que le thème principal de la vingt-septième session de la Commission serait le suivant : « Mesures de justice pénale propres à prévenir et à combattre la cybercriminalité sous toutes ses formes, y compris par le renforcement de la coopération aux niveaux national et international ». La présente note propose une série de questions, relevant de différents axes thématiques, qui pourraient être examinées dans le cadre du débat, expose brièvement certains points visant à orienter le débat et donne des informations générales.

* E/CN.15/2018/1.

V.18-00974 (F) 230318 260318

Merci de recycler

I. Introduction

1. Dans sa décision 2016/241, le Conseil économique et social a décidé que le thème principal de la vingt-septième session de la Commission serait le suivant : « Mesures de justice pénale propres à prévenir et à combattre la cybercriminalité sous toutes ses formes, y compris par le renforcement de la coopération aux niveaux national et international ».

2. À la reprise de sa vingt-sixième session, les 7 et 8 décembre 2017, la Commission a approuvé la proposition du Président en faveur d'une organisation du débat thématique de la vingt-septième session sur une séance du matin et une séance de l'après-midi. Le débat du matin serait consacré au sous-thème « Problèmes actuels » et celui de l'après-midi au sous-thème « Réponses envisageables ».

3. Le Secrétariat a établi la présente note conformément à la décision 18/1 de la Commission, intitulée « Principes directeurs pour les débats thématiques de la Commission pour la prévention du crime et la justice pénale », dans laquelle cette dernière a décidé que le débat sur le thème principal serait fondé sur un guide de discussion comprenant une liste de questions à aborder par les participants.

II. Informations générales : préparation du débat thématique

4. Si la croissance rapide d'Internet et de l'informatique a transformé les sociétés partout dans le monde, elle a aussi créé de nouvelles possibilités d'infractions. Les ordinateurs, les réseaux et les données peuvent être associés à diverses formes de criminalité de presque toutes les manières imaginables. Ils sont devenus à la fois des objets de crime et des outils servant à les commettre, et ont fait naître de nouveaux motifs et de nouvelles possibilités d'expansion de la criminalité. Pour les auteurs d'infractions, ils font souvent pencher la balance entre les risques et les avantages en faveur de ces derniers. En outre, l'architecture qui sous-tend Internet étant numérique et les technologies de l'information et de la communication (TIC) pouvant être utilisées partout dans le monde, la cybercriminalité, qui est associée à la criminalité organisée, est souvent de nature transnationale[1].

5. Dans sa résolution 65/230, l'Assemblée générale a fait sienne la « Déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux : les systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation », adoptée par le douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, et elle a prié la Commission pour la prévention du crime et la justice pénale de créer, conformément au paragraphe 42 de la Déclaration de Salvador, un groupe intergouvernemental d'experts à composition non limitée chargé de faire une étude approfondie du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, notamment l'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, en vue d'examiner les options envisageables pour renforcer les mesures juridiques ou autres prises aux échelons national et international contre la cybercriminalité et pour en proposer de nouvelles.

6. Ce mandat a été renouvelé dans la Déclaration de Doha sur l'intégration de la prévention de la criminalité et de la justice pénale dans le programme d'action plus large de l'Organisation des Nations Unies visant à faire face aux problèmes sociaux et économiques et à promouvoir l'état de droit aux niveaux national et international et la participation du public, qui a été adoptée par le treizième Congrès des Nations Unies

[1] *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (publication des Nations Unies, numéro de vente : F.10.IV.6), p. 204 [en anglais seulement] ; et *Rapport mondial sur les drogues 2017 : Le problème de la drogue et la criminalité organisée, les flux financiers illicites, la corruption et le terrorisme* (publication des Nations Unies, numéro de vente de la version anglaise : E.17.XI.11), p. 15 [version française en cours d'élaboration].

pour la prévention du crime et la justice pénale et approuvée par l'Assemblée générale dans sa résolution 70/174.

7. Le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité a tenu quatre réunions au total, qui ont eu lieu respectivement en 2011, 2013, 2017 et 2018. Dans sa résolution 22/7 du 26 avril 2013, la Commission pour la prévention du crime et la justice pénale a pris note de l'étude approfondie sur la cybercriminalité réalisée par l'Office des Nations Unies contre la drogue et le crime (ONUDC) sous l'égide du Groupe d'experts, et de l'échange de vues sur son contenu intervenu lors de la deuxième réunion du Groupe, tenue à Vienne du 25 au 28 février 2013 (voir UNODC/CCPCJ/EG.4/2017/3), au cours de laquelle divers avis avaient été exprimés quant au contenu, aux conclusions et aux options présentés dans l'étude, et elle a prié le Groupe d'experts de poursuivre ses travaux, avec l'aide du Secrétariat, selon qu'il conviendrait, en vue d'accomplir son mandat.

8. Dans la résolution 26/4 qu'elle a adoptée à sa vingt-sixième session, le 26 mai 2017, la Commission pour la prévention du crime et la justice pénale a prié le Groupe d'experts de poursuivre ses travaux et, dans ce cadre, de tenir des réunions périodiques et d'offrir une tribune pour les débats à venir sur les questions de fond relatives à la cybercriminalité, en suivant l'évolution des tendances dans ce domaine et conformément à la Déclaration de Salvador et à la Déclaration de Doha, et l'a également prié de continuer d'échanger des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin de trouver des moyens de renforcer les mesures juridiques ou autres prises aux niveaux national et international face à la cybercriminalité et d'en proposer de nouvelles. Dans la même résolution, la Commission a décidé que le Groupe d'experts consacrerait ses prochaines réunions à l'examen, de manière structurée, de chacun des grands thèmes qui font l'objet de l'étude, sans préjudice d'autres questions relevant de son mandat et compte tenu, selon qu'il convient, des contributions reçues conformément à la résolution 22/7 de la Commission ainsi que des délibérations de ses réunions précédentes.

9. Dans un contexte plus large, il est de plus en plus admis, comme en témoigne le Programme de développement durable à l'horizon 2030 adopté par l'Assemblée générale dans sa résolution 70/1, qu'il est essentiel de réduire les conflits, la criminalité, la violence et la discrimination et de garantir l'inclusion, la bonne gouvernance et l'état de droit pour assurer un développement durable. À cet égard, l'objectif 16 du Programme 2030 (« Promouvoir l'avènement de sociétés pacifiques et inclusives aux fins du développement durable, assurer l'accès de tous à la justice et mettre en place, à tous les niveaux, des institutions efficaces, responsables et ouvertes à tous ») est particulièrement pertinent. Cet objectif est lié à la lutte contre la cybercriminalité, qui, comme d'autres formes de criminalité, notamment la criminalité organisée, compromet la bonne gouvernance et l'état de droit, met en péril la sécurité et le développement et a un effet déstabilisateur sur les États Membres (voir E/CN.7/2016/CRP.1-E/CN.15/2016/CRP.1, par. 4).

10. Au quatorzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, qui se tiendra au Japon en avril 2020, divers aspects de la cybercriminalité seront examinés, notamment dans le cadre du quatrième atelier du Congrès, consacré au thème « Tendances actuelles de la criminalité, évolutions récentes et solutions nouvellement apparues, en particulier le recours aux nouvelles technologies pour commettre des actes criminels et lutter contre la criminalité ».

11. Cela étant, le débat thématique sur la cybercriminalité qui se tiendra lors de la vingt-septième session de la Commission vise à faire le point sur les évolutions récentes. Il sera l'occasion pour les États Membres de poursuivre le débat et d'échanger des vues et des expériences. Afin de faciliter le débat, huit axes thématiques relatifs à la cybercriminalité ont été recensés, y compris ceux qui sont expressément mentionnés dans le thème principal. Chacun de ces axes thématiques fait l'objet, dans la section III ci-dessous, d'un examen qui s'articule autour des problèmes actuels et des réponses envisageables (comme convenu à la reprise de la vingt-sixième session de la

Commission, voir par. 2) et qui donne lieu à une liste indicative de questions ou de points à examiner plus avant.

III. Axes thématiques : questions à examiner

A. Types d'infractions relevant de la cybercriminalité et menaces connexes

Problèmes actuels

12. Le terme « cybercriminalité » n'est pas un terme juridique ou criminalistique et ne définit, ni ne décrit une catégorie d'infractions précise. On s'accorde généralement sur une liste des principaux types d'abus et d'infractions directement liés à l'informatique, mais aucun consensus mondial ne s'est encore dégagé en ce qui concerne la signification ou la définition de ce terme. Cette situation s'explique par la polyvalence et l'omniprésence des ordinateurs, ainsi que par l'évolution des TIC et les diverses utilisations qui en ont été faites depuis la fin des années 1950.

13. Selon le contexte, le terme « cybercriminalité » peut désigner des infractions commises à l'aide des TIC, des infractions commises contre des installations informatiques et de communication et leurs utilisateurs en tant que tels, ou des scénarios dans lesquels ces technologies jouent un rôle indirect ou secondaire[2]. Il est employé pour décrire un large éventail d'infractions, notamment des infractions commises contre des données et des systèmes informatiques (telles que le piratage informatique), des activités de contrefaçon et de fraude informatiques (telles que le phishing), des infractions liées au contenu (telles que la diffusion de matériel relatif à la maltraitance sexuelle des enfants)[3] et aux droits d'auteur (telles que la diffusion de contenus pirates).

14. Le recours croissant aux technologies informatiques et la tendance à la numérisation des données ont rendu les données informatiques toujours plus importantes. En conséquence, celles-ci sont devenues la cible d'attaques fréquentes allant de l'atteinte à leur intégrité à l'espionnage. Il existe aujourd'hui une économie numérique souterraine complexe dans laquelle les données sont la marchandise de base. Les données personnelles et financières volées, qui peuvent notamment être utilisées pour accéder à des comptes bancaires et à des cartes de crédit existants, ou pour ouvrir de manière frauduleuse une nouvelle ligne de crédit, ont une valeur monétaire. Cette situation alimente de nombreuses activités criminelles, telles que le phishing, le dévoiement, la diffusion de logiciels malveillants et le piratage de bases de données d'entreprises, qui reposent sur une véritable infrastructure composée de développeurs de codes malveillants, de serveurs Web spécialisés et d'individus capables de louer des réseaux d'ordinateurs compromis pour perpétrer des attaques automatisées.

15. En particulier, le développement et la distribution de logiciels malveillants continuent d'être l'élément essentiel de la majorité des affaires de cybercriminalité. Depuis la fin 2013, le logiciel « cryptoware » (logiciel rançonneur qui chiffre les données) est devenu le plus redoutable des logiciels malveillants, compte tenu de la menace qu'il représente et des dégâts qu'il cause. Suivant la tendance en matière de piratage informatique, les campagnes de cryptage de données à l'aide de ce logiciel prennent de plus en plus pour cible les organismes des secteurs public et privé[4].

16. Les délinquants sont toujours à la recherche de méthodes et de techniques permettant de renforcer l'efficacité de leurs modèles économiques et d'accroître leurs profits. La nature anonyme des opérations en ligne et l'utilisation de cybermonnaies réduisent le risque d'être repéré par les services de détection et de répression. Le recours

---

[2] Christopher Ram, « Cybercrime » in *Routledge Handbook of Transnational Criminal Law*, éd. Neil Boister et Robert J. Currie (New York, Routledge, 2015), p. 379 [publication en anglais].

[3] Voir Office des Nations Unies contre la drogue et le crime, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienne, 2015) [en anglais seulement].

[4] Office européen de police, *European Union Serious and Organized Crime Threat Assessment: Crime in the age of technology* (La Haye, 2017), p. 30 [en anglais seulement].

accru aux réseaux privés virtuels, aux routeurs en oignon et à la traduction d'adresses réseau à grande échelle (qui permet le partage des adresses IP entre plusieurs clients) limite la capacité des enquêteurs à attribuer les éléments de preuve recueillis.

17. Les taux de cybercriminalité continuent d'augmenter à mesure de l'expansion d'Internet, accroissant par là même la vulnérabilité des victimes. En outre, la menace que représente la cybercriminalité sous ses diverses formes est multidimensionnelle et vise non seulement les citoyens, mais aussi, de plus en plus souvent, les entreprises et les gouvernements. Les outils de la cybercriminalité constituent une menace directe pour la sécurité et jouent un rôle toujours plus important dans la plupart des formes de criminalité organisée et de terrorisme.

Réponses envisageables

18. L'ampleur sans précédent du problème, associée à la multiplicité des comportements relevant de la cybercriminalité, limite la capacité des autorités à réagir de manière rationnelle et efficace. Cela étant, le cyberespace offre aussi des possibilités et des outils pour détecter la cybercriminalité. L'utilisation des TIC par les délinquants permet aux systèmes de justice pénale d'établir diverses pistes d'enquête et de recueillir des preuves. Les autorités n'ont jamais disposé d'autant de données sur les activités criminelles et peuvent désormais tirer parti de ces informations de manière à rendre la collecte d'informations et les enquêtes plus rentables. L'exploitation des cybermonnaies à des fins criminelles constitue à cet égard un exemple intéressant. Les cybermonnaies existent grâce à la technologie de la chaîne de blocs. Malgré quelques lacunes techniques et juridiques, plusieurs aspects de cette technologie pourraient en faire un outil de détection et de répression très utile pour la recherche d'opérations suspectes et la localisation des preuves (voir E/CN.15/2018/CRP.1, par. 164).

19. Des cyberenquêteurs qualifiés, formés dans le cadre d'activités intensives de renforcement des capacités, parviennent à obtenir des preuves électroniques relatives à des actes de cybercriminalité, même lorsque les auteurs de ces actes prennent le soin de ne pas laisser de traces numériques ou de les supprimer. En fonction des délais de conservation des données, le journal des connexions associées à l'adresse IP (Internet Protocol) peut être consulté afin de déterminer la date et l'heure, ainsi que la source et la destination des connexions Internet.

20. En outre, la dépendance croissante de la société à Internet et à la communication assistée par ordinateur a conduit les services de détection et de répression à mettre au point des outils pour enquêter sur les infractions commises en ligne ou à recourir à des logiciels, par exemple, pour mettre en évidence les diverses formes de criminalité. Ils ont également recours aux médias sociaux pour améliorer leurs relations avec les populations locales et pour solliciter la coopération du public aux enquêtes judiciaires.

21. Il est donc essentiel que les États envisagent d'élaborer des stratégies pluridisciplinaires pour s'attaquer aux différents problèmes et moderniser leurs capacités afin de mener des enquêtes et des poursuites efficaces et concluantes dans les affaires relatives à la cybercriminalité. Ces stratégies peuvent couvrir une gamme d'activités allant de l'élaboration de mesures réglementaires et de politiques à la prévention de la cybercriminalité et à la formation des autorités compétentes, comme on le verra plus loin.

Questions à examiner

22. La Commission souhaitera peut-être examiner plus avant les questions suivantes :

a) Quels enseignements peuvent être tirés de l'analyse de l'évolution des diverses formes de cybercriminalité ?

b) Quelle est la meilleure façon d'utiliser ces enseignements pour élaborer des mesures réglementaires et des stratégies politiques efficaces contre la cybercriminalité au niveau national ?

c) Quelle est l'incidence des différentes formes de cybercriminalité sur la capacité des États Membres à conserver de manière systématique les données relatives aux infractions et à échanger des renseignements aux fins de la détection et de la répression aux niveaux régional et international, y compris des renseignements concernant l'implication de groupes criminels organisés, leurs modes opératoires et les techniques employées pour détecter les diverses formes de cybercriminalité ?

d) Dans quelle mesure les définitions des termes « groupe criminel organisé » et « groupe structuré » figurant dans la Convention des Nations Unies contre la criminalité transnationale organisée s'appliquent-elles au cyberespace, notamment aux cas où les délinquants, souvent protégés par l'anonymat, interagissent sans connaître leur identité respective ?

B. Mesures juridiques contre la cybercriminalité : aspects relatifs à l'incrimination

Problèmes actuels

23. Lorsque l'on examine les problèmes rencontrés actuellement dans l'élaboration de mesures juridiques propres à combattre la cybercriminalité, il est utile d'avoir à l'esprit la manière dont ces problèmes sont apparus et se sont accentués au fil des ans. Dans le passé, les services informatiques et les technologies relatives à Internet ont fait naître de nouvelles formes de criminalité peu de temps après leur apparition. Le développement des réseaux d'ordinateurs dans les années 1970, suivi de près par le premier accès non autorisé à l'un de ces réseaux, en est un exemple. De même, les premières infractions liées à des logiciels sont apparues peu après l'arrivée des ordinateurs personnels dans les années 1980, alors que ceux-ci servaient à copier des produits logiciels. Vers la fin des années 1990, les réseaux étaient devenus des éléments essentiels de l'infrastructure des TIC, ce qui a suscité une préoccupation grandissante quant à la menace que représentaient pour eux certaines formes de cybercriminalité. Il en a résulté le recours à des mesures de cybersécurité et une tendance à incriminer spécifiquement certains types d'attaques contre les infrastructures critiques, ou à prévoir des peines aggravées pour ces attaques[5].

24. Outre l'apparition de nouvelles définitions et de nouveaux concepts du fait de l'évolution rapide des technologies, la question se pose toujours de savoir s'il convient de traiter la cybercriminalité comme un phénomène nouveau et donc de définir des infractions entièrement nouvelles, ou s'il vaut mieux essayer d'appliquer les définitions d'infractions qui existent déjà et, au besoin, élargir ou ajuster leur champ d'application. Ainsi, certains pays ont adopté de nouvelles lois traitant la « fraude informatique » comme une infraction à part entière, tandis que d'autres se sont contentés de compléter les définitions existantes d'infractions portant sur des biens corporels par des dispositions sur le fait de copier ou d'altérer des données, d'entraver l'accès aux données ou de les utiliser de manière abusive. Un autre exemple est celui de l'infraction d'usurpation d'identité créée dans certains pays.

25. Dans les pays qui ont préféré modifier les lois pénales préexistantes, le législatif est souvent aux prises avec de longues procédures visant à examiner et à mettre à jour la législation. Le principal problème est, de ce fait, le délai entre la détection de nouvelles formes de criminalité et l'entrée en vigueur des dispositions législatives adoptées pour y faire face. Ce problème est plus que jamais d'actualité, face à l'accélération de l'innovation technologique.

---

[5] Voir notamment Aunshul Rege-Patwardhan, « Cybercrimes against critical infrastructures: a study of online criminal organization and techniques », *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, vol. 22, n° 3 (2009), p. 261 ; éd. Luca Montanari et Leonardo Querzoni, *Critical Infrastructure Protection: Threats, Attacks and Countermeasures* (mars 2014) [publications en anglais]. Voir aussi la résolution 2341 (2017) du Conseil de sécurité sur les menaces contre la paix et la sécurité internationales résultant d'actes terroristes.

Réponses envisageables

26. Une législation pénale adéquate est le fondement des enquêtes et des poursuites en matière de cybercriminalité. De ce fait, les législateurs doivent être en mesure d'agir face à l'évolution des TIC et d'observer en permanence l'efficacité des dispositions juridiques existantes. Une analyse approfondie de la législation en vigueur est essentielle pour détecter ses éventuelles lacunes et surmonter les difficultés qui en découlent concernant le respect de l'exigence de double incrimination en matière de coopération internationale. Les législateurs peuvent également tirer parti des instruments multilatéraux contraignants et non contraignants.

27. Afin d'avoir un effet durable, les nouvelles lois et les modifications apportées aux lois existantes devront peut-être être rédigées de manière à assurer une marge de manœuvre et être neutres du point de vue technologique, tout en tenant compte du besoin de sécurité juridique et de précision. Elles devraient également prendre en considération la nécessité de garantir un accès rapide à l'information au-delà des frontières nationales. Finalement, les législateurs auront peut-être besoin d'une formation et de directives adéquates pour formuler des dispositions bien conçues et promulguer des lois efficaces.

Questions à examiner

28. La Commission souhaitera peut-être examiner plus avant les questions suivantes :

a) Quels sont les enseignements tirés des efforts déployés à l'échelle nationale pour élaborer et faire appliquer la législation contre la cybercriminalité et pour l'intégrer dans le cadre plus large d'une stratégie nationale de lutte contre la cybercriminalité ?

b) Les lois nationales constituent-elles un fondement juridique suffisant pour détecter les infractions liées à la cybercriminalité, enquêter à leur sujet et en poursuivre les auteurs de manière efficace ? Quelles sont les lacunes à combler ?

c) Quelle est l'incidence des instruments multilatéraux existants sur le champ d'application des cadres juridiques nationaux de lutte contre la cybercriminalité ? Les législations adoptées au niveau national sur la base de ces instruments convergent-elles ? Si oui, dans quelle mesure ?

d) Compte tenu de l'exigence de double incrimination, la diversité des conceptions nationales de l'incrimination des infractions relevant de la cybercriminalité influe-t-elle sur l'étendue de la coopération internationale ?

C. Pouvoirs procéduraux et preuves électroniques

Problèmes actuels

29. Les pouvoirs d'enquête nationaux jouent un rôle déterminant dans la collecte des preuves électroniques. Un examen de ces pouvoirs au niveau national révèle qu'il existe quantité de manières différentes d'envisager l'utilisation des preuves électroniques dans les enquêtes. Ces différentes interprétations déterminent dans quelle mesure les pouvoirs traditionnels peuvent être appliqués à des données constituant des éléments de preuve immatériels, ainsi que l'existence d'une autorisation légale pour adopter des mesures intrusives, comme les enquêtes de criminalistique informatique à distance. Bien que les pouvoirs juridiques varient, un corpus de mesures d'enquête devrait être mis à disposition en vue de la collecte de preuves électroniques. Ces mesures peuvent comprendre : 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 données relatives à l'abonné ; 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. Des exemples de lois nationales relatives aux mesures d'enquête figurent dans le Répertoire en ligne de l'ONUDC sur la cybercriminalité et

dans le portail de mise en commun de ressources électroniques et de lois contre la criminalité (SHERLOC). Les pouvoirs d'enquête doivent évoluer au rythme des nouvelles technologies. Ils devraient être appuyés par des cadres juridiques et institutionnels qui facilitent une coopération et une coordination efficaces et rapides entre le secteur privé et les organes gouvernementaux compétents, aux niveaux national, régional et international, tout en respectant les droits de l'homme. Il est impératif que ces cadres aient un volet consacré aux droits de l'homme, car les TIC touchent à des domaines tels que la protection de la vie privée et la liberté d'expression.

30. Théoriquement, les preuves électroniques sont admissibles devant les tribunaux. Cependant, l'importance croissante que prennent les éléments de preuve électroniques dans les procédures pénales soulève des questions qui ne se posaient pas auparavant. Par exemple, les preuves électroniques sont très fragiles et peuvent facilement être modifiées ou supprimées. En conséquence, l'un des objectifs fondamentaux de la criminalistique informatique est de protéger l'intégrité des données. Cette précaution est également nécessaire pour garantir la fiabilité et l'exactitude des éléments de preuve. En outre, pour être recevables, les preuves électroniques doivent être recueillies conformément aux procédures établies garantissant le respect des droits de l'homme.

31. Par ailleurs, pour enquêter efficacement sur la cybercriminalité et recueillir des preuves électroniques, 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 de services de communication jouent un rôle important en matière d'accès aux preuves électroniques. Les lois nationales relatives à la protection de la vie privée peuvent influer sur la capacité des fournisseurs à transmettre des renseignements aux services compétents dans le cadre d'une enquête.

Réponses envisageables

32. En raison de la nature transitoire des preuves électroniques, certaines normes et conditions sont nécessaires pour assurer le traitement des éléments de preuve et pour garantir leur authenticité et leur intégrité. Il s'agit de règles et de procédures générales, qui concernent notamment la tenue des dossiers, l'utilisation de technologies largement acceptées et la participation d'experts qualifiés aux enquêtes.

33. Un nombre croissant d'enquêtes sur la cybercriminalité, y compris dans des affaires relatives à la maltraitance et à l'exploitation des enfants, font intervenir des preuves électroniques détenues par des tiers. Par conséquent, il est crucial que les entreprises et les gouvernements collaborent pour mettre au point des mécanismes qui garantissent l'accès rapide des services de détection et de répression aux données en cas d'urgence. De tels mécanismes devraient être associés à des procédures judiciaires équitables et transparentes dans le cadre des enquêtes de routine.

34. Une réunion de groupe d'experts sur l'accès transfrontière licite aux données numériques, organisée conjointement par l'ONUDC et la Direction exécutive du Comité contre le terrorisme, en coopération avec l'Association internationale des procureurs et poursuivants, s'est tenue à Vienne les 12 et 13 février 2018. Cette réunion visait à jeter les bases de l'élaboration d'un guide pratique à l'intention des autorités centrales, des procureurs et des enquêteurs sur l'obtention de preuves électroniques auprès de juridictions étrangères dans le cadre des enquêtes transnationales relatives à la lutte contre le terrorisme et la criminalité organisée qui y est associée. La réunion a donné l'occasion de mettre en commun les lois et les directives nationales, ainsi que des exemples d'affaires réelles illustrant les bonnes pratiques et les enseignements tirés de l'obtention de preuves électroniques auprès de fournisseurs de services de communication situés à l'étranger.

Questions à examiner

35. La Commission souhaitera peut-être examiner plus avant les questions suivantes :

a) Quelles sont les difficultés rencontrées par les autorités chargées des enquêtes lorsqu'elles essaient de se conformer aux exigences concernant l'utilisation de techniques d'enquête spéciales, la collecte et le partage des preuves électroniques pour détecter les actes de cybercriminalité, enquêter à leur sujet et en poursuivre les auteurs ? Quelles sont les bonnes pratiques permettant d'y remédier ?

b) Quelle expérience les États Membres ont-ils acquise en ce qui concerne l'admissibilité de ces preuves devant les tribunaux ?

c) Quelles ont été les conséquences de la collaboration établie avec le secteur financier pour la collecte de preuves électroniques sur les produits de la cybercriminalité (par exemple, sur les passeurs de fonds) ?

d) Du point de vue de l'état de droit et des droits de l'homme, quelles sont les principales difficultés que pose la mise en œuvre des techniques relatives aux enquêtes sur les infractions liées à la cybercriminalité et aux poursuites qui en découlent ?

e) Quels sont les enseignements tirés des mesures prises pour favoriser la coopération entre les services de détection et de répression et les fournisseurs de services de communication en vue de l'obtention de preuves électroniques dans le cadre de la détection des infractions relevant de la cybercriminalité et des enquêtes et des poursuites auxquelles elles donnent lieu ?

D. Questions de compétence

Problèmes actuels

36. Le droit international pose un certain nombre de règles relatives à la compétence sur les actes relevant de la cybercriminalité, fondées principalement sur le territoire et sur la nationalité. Certaines de ces règles figurent dans les instruments multilatéraux relatifs à la cybercriminalité. La compétence territoriale objective ou élargie repose désormais souvent sur la présence d'un élément constitutif de l'infraction ou des effets de celle-ci sur le territoire d'un État, ou de l'existence de tout autre lien important avec ce territoire. Les États doivent aussi établir quel pays est le plus à même de poursuivre les auteurs présumés de l'infraction sur la base de facteurs tels que la localisation des preuves ou des auteurs.

37. Du fait de la diversité des règles de compétence appliquées dans les différents États, il peut arriver que plusieurs pays fassent valoir leur compétence sur un même acte de cybercriminalité. Le risque que des conflits de compétence surviennent augmente encore lorsque le principe de territorialité est appliqué à des affaires dans le cadre desquelles seule l'infrastructure ayant servi à commettre l'infraction se trouve dans le pays compétent, mais que l'auteur ou la victime ne s'y trouvent pas.

38. L'informatique en nuage soulève plusieurs problèmes pour la justice pénale, en particulier en ce qui concerne le droit applicable et la juridiction compétente. Il n'est pas toujours évident pour les autorités de la justice pénale de savoir dans quel pays les données sont stockées ou de quel régime juridique elles relèvent. Un fournisseur de services peut avoir son siège dans un État, mais être soumis au régime juridique d'un autre État alors que les données sont stockées dans un troisième État. Les mêmes données peuvent être conservées dans plusieurs États grâce à la technique dite de la mise en miroir (« mirroring ») ou être déplacées d'un État à un autre, ce qui complique encore la situation.

39. En outre, il est souvent difficile de déterminer si un fournisseur de services d'informatique en nuage est chargé du « contrôle » ou du « traitement » des données d'un utilisateur et, de ce fait, de savoir quelles sont les règles applicables. Un autre facteur d'incertitude consiste à savoir si les données sont stockées ou si elles sont en transit et, partant, quelle règle de compétence s'applique face à des injonctions visant à

obtenir, à perquisitionner et à saisir, à intercepter ou à collecter en temps réel ces données. Par ailleurs, la nature non localisée de l'informatique en nuage pose des problèmes pour les enquêtes criminalistiques et les perquisitions en ligne du fait de l'architecture du nuage (mutualisation, distribution et séparation des données) et des questions juridiques relatives à l'intégrité et à la validité de la collecte de données, au contrôle des éléments de preuve, à la propriété des données et à la compétence[6].

Réponses envisageables

40. Dans bien des cas, plusieurs États peuvent établir leur compétence à l'égard d'actes de cybercriminalité et il est donc important de tenir des consultations afin de décider lequel devrait mener les poursuites. Cette décision peut faire intervenir des questions d'ordre juridique, diplomatique et pratique, telles que la question relative à la compétence et aux autres prétentions juridiques des États et celle de savoir si les auteurs des infractions peuvent être extradés vers l'État qui souhaite engager les poursuites, et des considérations pragmatiques relatives au coût et aux autres obstacles empêchant le transfert des éléments de preuve d'un État à un autre, leur admissibilité et leur présentation effective devant un tribunal. Lorsqu'ils surviennent, les conflits de compétence sont généralement réglés dans le cadre de consultations formelles et informelles entre les pays. Une fois qu'il est établi que l'un des États compétents mènerait les poursuites, la compétence des autres États peut effectivement lui être transférée. Le transfert des procédures pénales, forme distincte de coopération internationale, s'inscrit dans un contexte et un cadre bien définis[7].

41. Des travaux visant à renforcer la coopération internationale et régionale aux fins de l'obtention de preuves électroniques ont également été menés au niveau multilatéral. En juin 2017, le Comité de la Convention sur la cybercriminalité (T-CY) du Conseil de l'Europe a approuvé l'élaboration d'un deuxième protocole à la Convention sur la cybercriminalité, qui vise à établir des règles précises et des procédures plus efficaces concernant la collecte de preuves électroniques « dans le nuage » dans le cadre de certaines enquêtes judiciaires. Le mandat a été approuvé le 8 juin 2017 et les négociations devraient se tenir de septembre 2017 à décembre 2019.

Questions à examiner

42. La Commission souhaitera peut-être examiner plus avant les questions suivantes :

a) Quelles sont les règles fixant la compétence en matière de poursuites pénales dans les affaires de cybercriminalité ? Comment ces règles sont-elles appliquées au cas de l'informatique en nuage où les données sont rarement stables ?

b) Quelle expérience a été acquise dans le cadre des consultations visant à régler les conflits de compétence à l'égard des infractions relevant de la cybercriminalité ? Quels sont les difficultés rencontrées, les bonnes pratiques adoptées et les enseignements tirés ?

E. Coordination et coopération interinstitutions au niveau national

Problèmes actuels

43. Les stratégies multipartites sont primordiales dans la lutte contre la cybercriminalité. Les problèmes juridiques, techniques et institutionnels posés par cette forme de criminalité sont vastes et ne peuvent être réglés qu'en suivant une stratégie cohérente, fondée sur les initiatives existantes et prenant en compte le rôle des

[6] Conseil de l'Europe, Comité de la Convention sur la cybercriminalité (T-CY), « Défis de l'accès de la justice pénale aux données stockées dans le nuage », document de réflexion préparé par le Groupe de travail sur les preuves dans le nuage, 26 mai 2015, document T-CY(2015)10, p. 10 à 15.

[7] Voir le document d'information établi par le Secrétariat intitulé « Considérations pratiques, bonnes pratiques et problèmes rencontrés dans le domaine du transfert de procédures pénales, forme distincte de coopération internationale en matière pénale » (CTOC/COP/WG.3/2017/2).

différentes parties prenantes. Pour être efficace, la lutte contre la cybercriminalité exige une structure organisationnelle sophistiquée qui évite les chevauchements, définit clairement les compétences et coordonne toutes les parties prenantes afin qu'elles puissent prendre des mesures concertées. En l'absence de telles structures, il sera particulièrement difficile de mettre en œuvre des politiques et des programmes viables.

44. En matière de cybercriminalité, la dissuasion fait également partie intégrante des stratégies nationales visant à assurer la cybersécurité et à protéger les infrastructures informatiques critiques. Il s'agit, en particulier, d'adopter des lois pour combattre le détournement des TIC à des fins criminelles ou autres, et pour lutter contre les activités visant à compromettre l'intégrité des infrastructures nationales critiques. La dissuasion est une responsabilité partagée entre les autorités nationales, le secteur privé et les citoyens, qui doivent mener une action coordonnée afin de prévenir les atteintes à la cybersécurité, de s'y préparer, d'y réagir et d'y remédier. L'élaboration et la mise en œuvre d'une stratégie nationale de lutte contre la cybercriminalité exigent une démarche globale, qui suppose la collaboration et la coordination des parties prenantes concernées au niveau institutionnel.

45. Toutefois, la coordination institutionnelle pose un certain nombre de difficultés, qui tiennent pour la plupart aux ressources et aux capacités dont dispose chaque pays. Il faut également tenir compte de plusieurs autres facteurs, tels que l'étendue de l'appui fourni par le secteur privé, notamment dans le cadre de partenariats public-privé, ou les mesures d'autoréglementation et d'autoprotection que celui-ci a mises en place.

Réponses envisageables

46. Sur le plan stratégique, l'établissement de partenariats interinstitutions est devenu une pratique courante pour combattre la cybercriminalité, notamment la criminalité assistée par les technologies informatiques visant les enfants. Pour relever les défis multiples que pose la lutte contre la cybercriminalité, les fournisseurs de service de communication et les institutions publiques telles que les services de détection et de répression et les services de justice pénale doivent former des partenariats public-privé, dans le cadre desquels un climat de confiance et des dialogues bilatéraux peuvent s'instaurer. D'une manière plus générale, les États doivent prendre des mesures réglementaires qui vont au-delà du droit pénal et inciter le secteur privé à participer activement à la prévention du crime. Une telle approche permettrait de créer un environnement sensible aux nouvelles menaces et apte à les contrer.

47. Des équipes spécialisées dans la lutte contre la criminalité organisée facilitée par Internet pourraient être des outils précieux pour mener une action concertée contre la cybercriminalité. Ces équipes devraient être capables de s'adapter à un environnement criminel en constante évolution et pourraient, par exemple, déboucher sur la création de groupes plus permanents d'échanges de renseignements et sur la conclusion d'arrangements plus adaptés aux besoins des opérations prévues, telles que le démantèlement de réseaux d'ordinateurs zombies (« botnets »). Dans tous les cas, les autorités doivent disposer d'une latitude suffisante pour faire participer les diverses parties prenantes, telles que les services de détection et de répression, le secteur privé, les universités et les groupes d'utilisateurs, et assurer une coordination efficace avec elles afin d'obtenir le résultat voulu.

48. Internet a continué de modifier l'orientation des réglementations publiques des TIC. Les organismes chargés de réglementer le secteur des TIC participent déjà à de nombreuses activités de lutte contre la cybercriminalité. Cela est particulièrement vrai dans des domaines tels que la réglementation de contenu, la sécurité des réseaux et la protection des consommateurs, car les utilisateurs sont devenus vulnérables. Cette participation est due au fait que la cybercriminalité compromet le développement de l'industrie des TIC et des parties offrant des produits et services connexes. Les nouvelles obligations et responsabilités des organismes chargés de la réglementation des TIC dans la lutte contre la cybercriminalité s'inscrivent dans une tendance plus générale à la

conversion des modèles centralisés de réglementation de la cybercriminalité en des structures souples[8].

Questions à examiner

49. La Commission souhaitera peut-être examiner plus avant les questions suivantes :

a) Quelles sont les difficultés rencontrées au niveau national dans le renforcement des capacités institutionnelles et de la coordination interinstitutions contre la cybercriminalité ?

b) Les États ont-ils tiré une expérience de l'élaboration de cadres ou de lignes directrices types concernant la coopération à établir entre les parties prenantes intéressées à l'échelle nationale en vue de prévenir et de combattre la cybercriminalité ? Si oui, de quelle manière ces cadres ou lignes directrices ont-ils favorisé une réelle collaboration ?

F. Coopération internationale

Problèmes actuels

50. Outre l'incrimination des actes de cybercriminalité et l'octroi des pouvoirs procéduraux connexes, les instruments existants prévoient également des mécanismes de coopération internationale dans le cadre des enquêtes et des poursuites transnationales relatives à la cybercriminalité. La coopération internationale aux fins de la lutte contre la cybercriminalité se révèle de plus en plus complexe pour les autorités de la justice pénale et les services de détection et de répression. Si, en théorie, la localisation de données informatiques peut être déterminée à un instant précis, avec l'apparition de l'informatique en nuage, du chiffrement, du partage et du stockage des données de pair à pair, ces dernières peuvent désormais exister en plusieurs exemplaires, répartis entre divers appareils en divers lieux, et être transférées d'un lieu à un autre en quelques secondes[9].

51. En raison de la nature transitoire des preuves électroniques, la coopération internationale en matière de cybercriminalité exige une grande réactivité, notamment en ce qui concerne la conservation et la production des données par les fournisseurs de services, ainsi que la possibilité de demander que des enquêtes spécialisées soient ouvertes. L'un des obstacles fréquemment rencontrés dans le cadre des demandes adressées à d'autres pays pour obtenir ce genre de données réside dans les délais de réponse, qui dépassent souvent la période de conservation des données et peuvent permettre aux auteurs de détruire définitivement des preuves électroniques essentielles. D'autres obstacles fréquents sont le manque de volonté et d'esprit de conciliation des autorités sollicitées, leur capacité à fournir des preuves sous une forme qui peut être présentée aux juridictions, et les différences qui existent entre les États coopérants quant à la définition des infractions pénales[10].

52. Lors de la deuxième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue en 2013, la plupart des experts sont convenus qu'il serait nécessaire d'intensifier la coopération internationale pour faire face au problème de la cybercriminalité, d'autant plus que ce problème continuait de s'aggraver et que le recours aux technologies à des fins légitimes le rendait encore plus dangereux. Par ailleurs, divers points de vues ont été exprimés concernant la meilleure stratégie à adopter et les mesures à prendre en priorité pour s'attaquer aux problèmes liés à la

[8] Union internationale des télécommunications, *Comprendre la cybercriminalité : phénomène, difficultés et réponses juridiques* (Genève, 2012), p. 106 et 107.

[9] Document d'information sur l'atelier 3 relatif au 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. 32.

[10] Voir le document d'information établi par le Secrétariat sur la collecte et le partage de preuves électroniques (CTOC/COP/WG.3/2015/2), par. 19.

cybercriminalité[11]. Dans ce contexte, les avis ont divergé quant à savoir s'il fallait élaborer un nouvel instrument juridique universel contre la cybercriminalité qui aborderait, entre autres, les aspects relatifs à la coopération internationale à l'échelle mondiale, ou si la communauté internationale devrait plutôt continuer de recourir aux instruments multilatéraux existants, notamment la Convention sur la cybercriminalité du Conseil de l'Europe. À ce jour, la question continue de faire l'objet de débats sans qu'un consensus n'ait été atteint.

Réponses envisageables

53. On pourrait renforcer encore les mécanismes de coopération internationale en examinant la manière dont les procédures d'entraide judiciaire peuvent être accélérées. D'autres solutions consistent peut-être à renforcer la coopération en matière de détection et de répression, et à poursuivre le dialogue multilatéral sur l'accès transnational aux données informatiques. Par exemple, la mise en place d'un régime séparé pour l'accès aux données relatives aux abonnés telles que définies au paragraphe 3 de l'article 18 de la Convention sur la cybercriminalité du Conseil de l'Europe, qui établit une distinction entre les types de données recherchées, pourrait contribuer grandement à rendre l'entraide judiciaire en matière de cybercriminalité et de preuves électroniques plus efficace[12].

54. Des innovations telles que l'ajout d'un module sur les preuves électroniques dans la nouvelle version du Rédacteur de requêtes d'entraide judiciaire de l'ONUDC permettraient de rationaliser les procédures d'entraide judiciaire faisant intervenir des preuves électroniques. Parallèlement, toutefois, 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 pour l'innovation de l'Organisation internationale de police criminelle (INTERPOL) et le Centre européen de lutte contre la cybercriminalité de l'Office européen de police (Europol) participent à la coordination des enquêtes transnationales et y apportent leur soutien, notamment en facilitant l'échange de renseignements entre les services nationaux de détection et de répression, pourrait se révéler particulièrement important à cet égard.

55. Parmi les autres solutions possibles on peut mentionner les suivantes : mettre en place des unités spécialisées dans la lutte contre la cybercriminalité au sein des autorités centrales ; surveiller et examiner le traitement des dossiers d'entraide judiciaire pour assurer sa rapidité et son efficacité, notamment en recueillant des statistiques sur les demandes d'entraide judiciaire concernant des preuves électroniques ; recourir plus fréquemment à la coopération directe entre les services de police, complément utile à l'entraide judiciaire permettant de répondre plus rapidement aux demandes d'assistance urgentes ; dispenser des formations ciblées et plus intensives visant à renforcer l'entraide judiciaire, la coopération entre les services de police et les autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques ; améliorer l'échange d'informations et de données d'expérience entre des réseaux de points de contact accessibles en permanence ; allouer des ressources aux services nationaux chargés de traiter les demandes d'entraide judiciaire et renforcer la coordination de ces services avec les autorités centrales pour assurer des interventions rapides.

---

[11] Délibérations de la deuxième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 25 au 28 février 2013, Rapport succinct du Rapporteur, UNODC/CCPCJ/EG.4/2017/3, par. 25.

[12] Voir Conseil de l'Europe, Comité de la Convention sur la cybercriminalité (T-CY), Groupe de travail sur les preuves dans le nuage, « Accès de la justice pénale aux preuves électroniques dans le cloud : recommandations pour examen par le T-CY », document T-CY (2016)5, p. 16 et 17.

Questions à examiner

56. La Commission souhaitera peut-être examiner plus avant les questions suivantes :

a) Comment les procédures d'entraide judiciaire pourraient-elles être accélérées dans les affaires liées à la cybercriminalité et aux preuves électroniques ? Quelles sont les meilleures pratiques et les difficultés auxquelles donne lieu la coopération entre les services de police en vue du transfert de preuves électroniques à l'étranger ?

b) Quels exemples les États peuvent-ils donner pour illustrer la manière dont l'intensification de l'échange d'informations aux niveaux régional et international a amélioré leur capacité à détecter et à évaluer les risques, et à répondre aux demandes de manière efficace et rapide ?

c) De quelle manière les demandes internationales de conservation des preuves électroniques devraient-elles être établies, transmises et traitées ? Quelle est l'expérience acquise en matière de coopération entre les secteurs public et privé à cet égard ?

G. Prévention de la cybercriminalité

Problèmes actuels

57. Le coût et la complexité des enquêtes et des poursuites menées dans le cadre des affaires de cybercriminalité laissent penser que les avantages d'une action concertée en matière de prévention peuvent être considérables. Les partenariats public-privé, en particulier, jouent un rôle central dans la prévention de cette forme de criminalité. Les fournisseurs de services peuvent également y contribuer : a) en stockant les données d'utilisateurs que les agents des services de détection et de répression munis d'un mandat peuvent consulter en vue de leur utilisation dans des enquêtes sur la cybercriminalité ; et b) en filtrant activement les communications et les contenus en ligne pour prévenir les actes de cybercriminalité. Cependant, du point de vue de la liberté d'expression, ces deux mesures posent de nombreux problèmes.

58. S'agissant du rôle des fournisseurs de services dans la prévention de la cybercriminalité, il faudra peut-être tenir compte des limites qui découlent de leur statut d'entités du secteur privé. Premièrement, les politiques des fournisseurs de services sont souvent instables et manquent de prévisibilité tant pour les services de détection et de répression que pour les clients. Les fournisseurs de services peuvent modifier unilatéralement leurs politiques, à tout moment et sans en notifier préalablement les services de détection et de répression. À cela s'ajoute le fait que les politiques et les pratiques diffèrent non seulement considérablement d'un fournisseur à l'autre, mais aussi d'un État Membre à un autre. Un fournisseur peut répondre à de nombreuses demandes émanant d'un pays et à aucune ou à un petit nombre de demandes émanant d'un autre pays, tandis qu'un autre fournisseur peut faire exactement l'inverse[13].

59. Deuxièmement, les enquêtes policières sur la cybercriminalité peuvent être entravées par les garanties relatives à la protection des données, qui exigent que les données personnelles soient effacées lorsqu'elles ne sont plus utiles aux fins pour lesquelles elles ont été collectées. Par conséquent, si l'adoption de lois sur la conservation des données est une mesure pragmatique visant à faire en sorte que les fournisseurs de services de communication puissent jouer un plus grand rôle dans la prévention de la cybercriminalité en collaborant davantage avec les services de détection et de répression, il est important que l'application de ces lois soit accompagnée des garanties procédurales et des dispositions relatives à la protection de la vie privée qui s'imposent. Les normes et réglementations en matière de protection des données

[13] Ibid., « Accès de la justice pénale aux données stockées dans le cloud : la coopération avec des fournisseurs de services "étrangers" », document T-CY (2016)2, p. 24 et 25.

doivent être prises en compte, notamment le règlement général sur la protection des données de l'Union européenne[14].

60. Le milieu universitaire a la lourde tâche de combler les nombreuses lacunes qui existent et qui continuent d'apparaître dans les connaissances sur la cybercriminalité, en particulier en ce qui concerne la maltraitance et l'exploitation sexuelles des enfants au moyen des TIC. Sous réserve d'un financement durable, ce qui est un problème considérable pour de nombreux pays, les établissements universitaires peuvent jouer divers rôles dans la prévention de la cybercriminalité, notamment en dispensant des enseignements et des formations aux professionnels, en élaborant des lois et des politiques, et en participant à la mise au point de normes et de solutions techniques.

Réponses envisageables

61. Les bonnes pratiques en matière de prévention de la cybercriminalité comprennent la promulgation de textes législatifs, l'exercice efficace de l'autorité, le renforcement des capacités de la justice pénale et des services de détection et de répression, la constitution d'une solide base de connaissances et la coopération entre les pouvoirs publics, les collectivités, le secteur privé et les États. Il est de la plus haute importance d'aider à l'élaboration et au renforcement des techniques de prévention, de diffuser les enseignements tirés et les meilleures pratiques adoptées, ainsi que les informations nécessaires à la mise au point de techniques de prévention efficaces.

62. Les campagnes et les initiatives de sensibilisation et d'éducation, y compris celles ayant trait aux nouvelles menaces et celles destinées à un public particulier tel que les enfants, ont été présentées comme un élément important des politiques de prévention de la cybercriminalité[15]. L'initiative sur l'éducation pour la justice, une initiative clef du Programme mondial de l'ONUDC pour la mise en œuvre de la Déclaration de Doha, prévoit l'élaboration et la diffusion de matériel sur la lutte contre la cybercriminalité à l'intention des enfants et des jeunes de l'enseignement primaire, secondaire et tertiaire.

63. La société civile peut jouer un rôle déterminant en aidant les enfants à comprendre et à gérer les risques de l'utilisation d'Internet, apportant ainsi une contribution de poids à la prévention de la maltraitance et de l'exploitation des enfants facilitées par les TIC. L'éducation et les méthodes de prévention psychosociales sont considérées comme indispensables pour protéger les enfants contre ce type de maltraitance et d'exploitation. Des initiatives éducatives permettent aux enfants, aux familles et aux autres personnes aidantes d'appréhender et d'évaluer correctement les risques associés à ces technologies[16].

64. Il existe un certain nombre de modèles de partenariats public-privé favorisant la prévention de la cybercriminalité, notamment de partenariats entre les services de détection et de répression et les fournisseurs de services de communication. Nombre d'entre eux sont fondés sur un partage d'informations reposant sur des règles claires, la confiance, un nombre de membres restreint, des bénéfices mutuels et la rapidité de réaction. En outre, le rôle du secteur privé, notamment dans la détection et le blocage de contenus en ligne liés à la maltraitance sexuelle des enfants avant que les clients puissent y accéder, continuera de s'élargir[17].

65. Une stratégie prospective évidente pour les gouvernements consiste à collaborer avec ceux qui exerceront à l'avenir une influence sur l'environnement commercial et opérationnel, afin que toutes les parties concernées puissent mieux anticiper l'évolution

[14] Règlement (EU) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (*Journal officiel de l'Union européenne*, L 119/1, 4 mai 2016, p. 1 à 88).

[15] Voir ONUDC, « Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children », New York, 2015, p. 54 [publication en anglais].

[16] Ibid, p. 54.

[17] Voir, par exemple, *The Netclean Report 2017*, disponible (en anglais) à l'adresse suivante : https://www.netclean.com/netclean-report-2017.

des comportements criminels et des utilisations abusives des technologies. Dans ce contexte, il importera de continuer d'améliorer la compréhension des comportements des cyberdélinquants contemporains au moyen de l'analyse du renseignement, de la recherche criminologique et des techniques de profilage, de manière à affecter plus efficacement les ressources existantes et à détecter activement les aspects des futures technologies de communication susceptibles d'être exploitées à des fins criminelles.

Questions à examiner

66. La Commission souhaitera peut-être examiner plus avant les questions suivantes :

a) Quels exemples les États peuvent-ils donner pour illustrer les stratégies de prévention efficaces que les parties prenantes compétentes ont adoptées pour lutter contre la cybercriminalité ? Comment peut-on définir et mesurer leur succès ?

b) De quelle manière les établissements universitaires, le secteur privé et les organisations non gouvernementales peuvent-ils contribuer au mieux à l'approfondissement et à la diffusion des connaissances ainsi qu'à l'élaboration de lois et de politiques dans le domaine de la cybercriminalité ?

c) Quelle expérience les États Membres ont-ils acquise concernant l'équilibre à trouver entre la protection des données et l'efficacité des enquêtes sur la cybercriminalité ?

H. Renforcement des capacités et assistance technique

Problèmes actuels

67. Le renforcement des capacités nationales dans les domaines de la détection et de la répression et de la justice pénale est 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 preuves électroniques, mais souvent, ces structures manquent de ressources et de capacités. Les preuves électroniques jouant un rôle essentiel dans les enquêtes sur la cybercriminalité, 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 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.

68. Dans l'ensemble, il est clair que le renforcement des capacités des agents de détection et de répression et de la justice pénale aux fins de la lutte contre la cybercriminalité est une entreprise qu'il faudra mener sans relâche, car la technologie et l'innovation en matière criminelle évoluent rapidement.

Réponses envisageables

69. L'assistance et la coopération techniques sont importantes pour la diffusion de bonnes pratiques d'enquête, de données d'expérience et de nouvelles techniques. Les États Membres pourraient souhaiter améliorer la diffusion des nouvelles méthodes d'enquête sur les fraudes financières complexes commises sur Internet, sur le trafic de drogues en ligne ou sur l'utilisation de monnaies virtuelles à des fins de blanchiment d'argent, ce qui permettrait aux services de détection et de répression de plusieurs pays d'acquérir rapidement les compétences requises pour contrer les nouvelles menaces relatives à la cybercriminalité.

70. 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 mettre au point des techniques d'enquête spécialisées, de collecter et d'analyser les preuves électroniques utiles 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 enquêtes et cibler les formes de cybercriminalité susceptibles d'être particulièrement préoccupantes pour les pouvoirs publics.

71. Conformément à la résolution 65/230 de l'Assemblée générale et aux résolutions 22/7 et 22/8 de la Commission pour la prévention du crime et la justice pénale, l'ONUDC est chargé, dans le cadre de son Programme mondial contre la cybercriminalité, d'aider les États Membres à lutter contre la cybercriminalité grâce au renforcement de leurs capacités et à une assistance technique. Au titre de ce programme, il fournit une assistance technique ciblée axée sur le renforcement des capacités, la prévention et la sensibilisation, la coopération internationale et l'analyse en matière de cybercriminalité, en particulier dans les pays en développement. Il fournit également, sur demande et dans les limites de son mandat, une assistance législative aux États Membres qui en ont besoin.

72. Par exemple, l'ONUDC a mis au point un cours de formation de formateurs sur les enquêtes concernant les cybermonnaies et dispensé des formations à ce sujet dans diverses régions. Ces formations visent à renforcer les capacités des agents des services de détection et de répression, des analystes, des procureurs et des juges en ce qui concerne les cybermonnaies, la localisation des bitcoins dans les enquêtes financières, la localisation des sources d'informations et la collaboration dans les affaires internationales.

Questions à examiner

73. La Commission souhaitera peut-être examiner plus avant les questions suivantes :

a) Quels sont les aspects des mesures et des stratégies de lutte contre la cybercriminalité les plus importants pour l'assistance technique et le renforcement des capacités, en particulier compte tenu de l'évolution de la cybercriminalité et des nouvelles menaces qui y sont associées ?

b) Quels enseignements ont été tirés de la diffusion des bonnes pratiques d'enquête, des données d'expérience et des nouvelles techniques dans le cadre de la coopération en matière d'assistance technique ?

c) Comment dégager et promouvoir des synergies et des alliances entre les différentes organisations internationales apportant une assistance technique dans le domaine de la cybercriminalité afin de fournir aux États Membres qui ont besoin d'aide des services concrets et durables de renforcement des capacités ?

IV. Combler les lacunes : la voie à suivre

74. La communauté internationale continue d'intensifier l'action qu'elle mène pour mieux comprendre et combattre les menaces que représente la cybercriminalité. Cela étant, il est urgent d'en faire davantage, étant donné qu'il reste des défis de taille à relever pour pouvoir élaborer et mettre en œuvre une action globale, coordonnée, durable et efficace face à la cybercriminalité.

75. À sa vingt-septième session, la Commission facilitera le débat thématique et, durant l'examen du point de l'ordre du jour correspondant, donnera aux participants l'occasion d'échanger des informations, leurs meilleures pratiques et des enseignements tirés de leur expérience, pour l'élaboration de mesures efficaces et la promotion des normes ou des instruments internationaux pertinents aux fins de la lutte contre la cybercriminalité.

76. Lorsqu'elle examinera les activités qui pourraient être entreprises pour relever les défis posés par la cybercriminalité et la voie qui pourrait être suivie pour mener une action appropriée, la Commission voudra peut-être faire porter les débats sur les aspects des cadres juridiques et institutionnels en place qui semblent présenter les plus grands

risques, ainsi que sur les domaines d'activité prioritaires dans lesquels les États Membres rencontrent les plus grandes difficultés.

77. La Commission pourrait envisager de recommander aux États Membres d'intensifier leurs efforts de renforcement des capacités et de consolider leurs cadres juridiques, en particulier lorsqu'ils examinent les politiques, les lois et les cadres institutionnels nationaux existants pour déterminer quelles lois, nouvelles ou modifiées, quels cadres institutionnels et quelles pratiques pourraient leur donner plus de moyens pour faire face aux menaces présentes et futures liées à la cybercriminalité.

78. La Commission pourrait déterminer et hiérarchiser les domaines dans lesquels l'ONUDC pourrait fournir une assistance technique, en étroite collaboration et coordination avec d'autres acteurs concernés, conformément aux mandats qui leur ont été confiés, afin d'aider plus efficacement les États Membres à mettre en œuvre les politiques et lois nationales et à se doter des capacités institutionnelles nécessaires pour faire face aux problèmes que pose aujourd'hui la cybercriminalité et à ceux qu'elle posera demain.

79. La Commission voudra peut-être aussi inviter l'ONUDC à l'aider à poursuivre la communication avec d'autres organismes intergouvernementaux chargés de la lutte contre la cybercriminalité et de l'élaboration de mesures de justice pénale propres à la prévenir et à la combattre, notamment avec la Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée et son Groupe de travail sur la coopération internationale, dans le cadre de leurs mandats respectifs et selon qu'il convient.