27 juillet 2020
Français
Original : anglais

Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité
Vienne, 27-29 juillet 2020

Projet de rapport

Additif

II. Liste de recommandations et conclusions préliminaires (*suite*)

A. Coopération internationale

1. Conformément au plan de travail du Groupe d'experts, le présent paragraphe contient une compilation de propositions formulées à la réunion par les États Membres au titre du point 2 de l'ordre du jour, intitulé « Coopération internationale ». Ces recommandations et conclusions préliminaires ont été faites par les États Membres et leur inclusion ne signifie pas qu'elles ont l'aval du Groupe d'experts et leur ordre de présentation ne reflète pas leur degré d'importance :

1) En ce qui concerne la portée de la définition de la cybercriminalité aux fins de la coopération internationale, les pays devraient veiller à une incrimination suffisante des actes de cybercriminalité, qui englobent non seulement les infractions purement informatiques, mais aussi d'autres infractions fréquemment commises grâce à l'utilisation d'Internet et de moyens électroniques (infractions facilitées par Internet), tels que la cyberfraude, le vol électronique, l'extorsion, le blanchiment d'argent, le trafic de drogues et d'armes, la pédopornographie et les activités terroristes ;

2) En ce qui concerne les mécanismes de coopération internationale, les États sont encouragés à adhérer aux traités multilatéraux existants, tels que la Convention de Budapest et la Convention contre la criminalité organisée, qui constituent la base juridique de l'entraide judiciaire, ou à s'y référer en l'absence d'un traité bilatéral d'entraide judiciaire ; en l'absence de tout traité, les États peuvent demander à un autre État de coopérer sur la base du principe de réciprocité ; la Convention de Budapest devrait également être utilisée comme référence pour les activités de renforcement des capacités et d'assistance technique dans le monde entier et il convient d'attirer l'attention sur la négociation en cours du deuxième protocole additionnel à la Convention de Budapest visant à renforcer encore la coopération transfrontalière. Dans une autre intervention, il a été rappelé que la Convention de Budapest n'avait qu'une application limitée compte tenu de son caractère régional, de l'état des ratifications, de l'absence de démarche globale, de la non-prise compte des tendances actuelles en matière de cybercriminalité et du fait qu'elle ne convient pas pleinement aux pays en développement. L'attention a été appelée sur la

résolution 74/247 de l'Assemblée générale en date du 27 décembre 2019, dans laquelle l'Assemblée a décidé d'établir un comité intergouvernemental spécial d'experts à composition non limitée, représentatif de toutes les régions, ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. D'autres interventions ont en outre fait valoir qu'il ne faudrait pas que les nouveaux cadres ou instruments sur la cybercriminalité aillent à l'encontre des cadres ou instruments existants et que les États soient amenés à abandonner les traités actuels ou les engagements pris précédemment, ainsi que les accords déjà en place, ou à ne pas s'y conformer ;

3) Il est nécessaire d'avoir des partenaires stratégiques pour enquêter sur la cybercriminalité, tels que les membres d'organisations existantes, notamment l'Organisation des États américains, le G7 ou INTERPOL ;

4) Dans les enquêtes et les procédures judiciaires, il convient de respecter la souveraineté et la compétence des États. Aucune demande d'accès direct à des données situées dans d'autres pays ne doit être adressée à une entreprise ou à un particulier sans le consentement préalable des pays en question ;

5) L'efficacité de la coopération internationale devrait être améliorée en mettant en place des dispositifs de coopération internationale permettant d'intervenir rapidement ainsi que des voies de communication entre les autorités nationales par l'intermédiaire d'agents de liaison et de systèmes informatiques aux fins de la collecte transfrontalière de preuves et du transfert en ligne de preuves électroniques ;

6) Les États devraient continuer de renforcer la coopération pour protéger les infrastructures critiques et consolider les réseaux de collaboration entre les équipes d'intervention rapide dans le domaine informatique (CERT et CSIRT) ;

7) Les États devraient envisager la création de protocoles novateurs pour l'échange d'informations, y compris de renseignements et de preuves d'actes criminels, afin d'accélérer ces procédures ;

8) Il est nécessaire de confirmer à nouveau l'engagement de tous les États Membres à assurer la sûreté et la sécurité des TIC par une utilisation exclusivement pacifique et à renforcer les efforts internationaux pour lutter contre toute activité malveillante dans le cyberespace en période de crise majeure aux niveaux mondial, régional et local ;

9) Les procédures de coopération internationale devraient être optimisées afin qu'une aide maximale soit fournie dans les limites des possibilités découlant du cadre juridique national pour les demandes de coopération internationale concernant la conservation des preuves électroniques, l'accès aux informations de journal et aux informations d'enregistrement des utilisateurs, qui ne portent pas atteinte aux droits humains et aux libertés fondamentales ou aux droits de propriété ;

10) Les pays sont invités à accorder une attention particulière à la nécessaire proportionnalité des mesures d'enquête, tout en respectant les libertés fondamentales et les régimes de protection des données à caractère personnel associés à la correspondance privée ;

11) La coopération internationale en matière de lutte contre la cybercriminalité devrait également tenir compte des spécificités liées au sexe et à l'âge ainsi que des besoins des groupes vulnérables ;

12) En ce qui concerne la portée de la coopération internationale, alors que l'entraide judiciaire ne devrait être fournie que par les autorités nationales, la coopération ne devrait pas se limiter aux services publics mais devrait également associer le secteur privé, notamment les fournisseurs d'accès à Internet (FAI). Dans ce contexte, il a été recommandé d'adopter des dispositions permettant la coopération directe avec les FAI d'autres pays s'agissant des demandes d'informations sur les abonnés et des demandes de conservation de données et des demandes urgentes ;

13) Les solutions visant à lutter contre la cybercriminalité et à protéger les sociétés doivent toujours assurer la protection des droits humains et des garanties constitutionnelles et promouvoir un cyberespace plus libre, plus ouvert, plus sûr et plus résilient pour tous ;

14) Les pays sont encouragés à rationaliser la coopération avec le secteur et à renforcer la collaboration entre les fournisseurs de services publics et les fournisseurs de services privés, en particulier pour relever les défis posés par les contenus criminels nuisibles sur Internet ;

15) Les entreprises privées, notamment les FAI, ont une responsabilité partagée dans la prévention et les enquêtes sur la cybercriminalité ; elles devraient accélérer et élargir leurs réponses aux demandes d'entraide judiciaire, les proposer dans les pays où elles se trouvent et s'assurer qu'elles disposent de canaux appropriés pour communiquer avec les autorités locales ;

16) Les partenariats public-privé doivent être renforcés ; là où de tels partenariats n'existent pas, ils doivent être créés ; les entreprises privées devraient participer à des groupes de travail (instances multilatérales) et prendre part aux discussions sur l'amélioration de la lutte contre la cybercriminalité ;

17) Les organisations non gouvernementales et les universités doivent également participer aux efforts de prévention et de lutte contre la cybercriminalité, car elles offrent une perspective inclusive, plurielle et globale, notamment pour garantir la protection des droits humains, en particulier la liberté d'expression et le respect de la vie privée ;

18) Les pays sont invités à rejoindre les réseaux autorisés de praticiens pour conserver et échanger des preuves électroniques recevables, à les utiliser plus largement et à les renforcer, y compris le réseau 24/7, les réseaux spécialisés dans la cybercriminalité et les canaux d'INTERPOL pour une coopération policière rapide, ainsi qu'à mettre en place des réseaux avec des partenaires stratégiquement alignés, en vue de partager des données sur les questions de cybercriminalité, d'intervenir rapidement et de minimiser la perte de preuves essentielles. Il a également été recommandé de recourir à la coopération entre les services de police et à d'autres méthodes de coopération informelle avant d'utiliser les canaux d'entraide judiciaire ;

19) Chaque État doit mettre en place un véritable point de contact disponible 24 heures sur 24 et 7 jours sur 7, doté de ressources suffisantes, pour faciliter la conservation des données numériques ainsi que le traitement des demandes traditionnelles d'entraide judiciaire internationale en matière pénale, en s'inspirant du modèle réussi de gel des données prévu par la Convention du Conseil de l'Europe ;

20) Les pays devraient renforcer la collaboration interinstitutionnelle et améliorer l'interopérabilité grâce à la normalisation des demandes d'informations et des procédures d'authentification et l'adhésion des diverses parties prenantes ;

21) Les pays devraient améliorer l'application des législations nationales et renforcer la coordination et les synergies au niveau national dans le domaine de la collecte et du partage d'informations et de preuves à des fins de poursuites ;

22) Les États devraient renforcer les mesures de partage d'informations financières ou monétaires, de gel des comptes et de confiscation des avoirs afin de garantir que les criminels ne puissent pas profiter des gains provenant d'activités criminelles ;

23) Les États sont encouragés à créer des équipes d'enquête conjointes avec d'autres pays au niveau bilatéral, régional ou international afin de renforcer leurs capacités d'intervention ;

24) Les États devraient également favoriser le traitement efficace des preuves électroniques et leur recevabilité devant les tribunaux, y compris lorsqu'elles sont destinées à un pays étranger ou reçues de ce dernier. À cet égard, les pays sont encouragés à commencer ou à continuer à mettre en place des mesures de réforme de

la législation sur la cybercriminalité et les preuves électroniques, en s'inspirant des exemples positifs et des réformes mises en place de par le monde ;

25) Il est recommandé d'élaborer des cadres juridiques qui tiennent également compte de la compétence extraterritoriale à l'égard des actes de cybercriminalité ;

26) Les pays devraient affiner les mécanismes visant à atténuer les conflits et relever les défis que posent l'imputation de responsabilité et les capacités à enquêter sur les affaires de cybercriminalité ;

27) Les États devraient s'efforcer de normaliser et de diffuser des outils procéduraux pour accélérer la production de données et étendre les recherches (tels que les injonctions de produire, ainsi que les injonctions de conservation rapide ou d'accès transfrontalier, par exemple) afin de faciliter le travail des services répressifs et leur coopération directe avec les FAI et résoudre les problèmes liés au traçage des preuves électroniques et à leur utilisation appropriée ;

28) Les États devraient faciliter l'élaboration et l'harmonisation de normes techniques interopérables en matière de criminalistique numérique et de recherche transfrontalière de preuves électroniques ;

29) Il est recommandé d'investir dans une autorité centrale forte chargée de la coopération internationale en matière pénale afin de garantir l'efficacité des mécanismes de coopération visant également la cybercriminalité ; il est recommandé de créer des unités spécialisées chargées d'enquêter sur la cybercriminalité ; et de répondre en outre aux demandes de conservation des données d'un autre État par l'intermédiaire d'un réseau fonctionnant 24 heures sur 24 et 7 jours sur 7 (ou directement avec le fournisseur dans certaines circonstances) afin de conserver les données requises le plus rapidement possible. Une meilleure compréhension des informations nécessaires pour qu'une demande d'entraide judiciaire aboutisse pourrait favoriser l'obtention plus rapide des données ;

30) Pour que la coopération internationale soit efficace, il faut que la législation nationale établisse des procédures qui facilitent la coopération internationale. Ainsi, la législation nationale doit permettre la coopération internationale entre services de détection et de répression ;

31) Au-delà des lois nationales, la coopération internationale en matière de cybercriminalité repose à la fois sur la coopération formelle, fondée sur des traités, et sur l'assistance traditionnelle entre les services de police. Dans leurs discussions relatives à la création d'un nouvel instrument sur la cybercriminalité, il importe que les pays aient à l'esprit qu'il faudrait que cet instrument ne soit pas incompatible avec les instruments existants, qui permettent d'ores et déjà une coopération internationale en temps réel pour bon nombre d'entre eux. Ainsi, les pays devraient veiller à ce que tout nouvel instrument sur la cybercriminalité ne soit pas incompatible avec les traités existants ;

32) Il convient d'accorder la priorité au renforcement durable des capacités et à l'assistance technique visant à accroître les capacités dans tous les domaines opérationnels et à améliorer les capacités des autorités nationales à lutter contre la cybercriminalité, y compris par la constitution de réseaux, l'organisation de réunions et de formations conjointes, le partage des meilleures pratiques, l'élaboration de supports de formation et de modèles de coopération. Ces activités de renforcement des capacités et de formation devraient inclure une formation hautement spécialisée à l'intention des praticiens, qui privilégie, en particulier, la participation de femmes expertes, et répondre davantage aux besoins des législateurs et des décideurs politiques pour mieux traiter les questions de conservation des données à des fins répressives ; aux besoins des autorités de détection et de répression, des enquêteurs et des analystes, pour améliorer leurs capacités dans le domaine de la criminalistique et de l'utilisation de données librement accessibles dans le cadre des enquêtes, de la chaîne de mise en sûreté des preuves électroniques ; et de la collecte et du partage de preuves électroniques à l'étranger ; et aux besoins des juges, des procureurs, des

autorités centrales et des avocats, pour qu'ils puissent juger et traiter efficacement les affaires pertinentes ;

33) Il est impératif d'élaborer des règles et des calendriers adéquats, et si possible uniformes, pour la collecte et la conservation des données, afin de garantir que les preuves électroniques puissent être conservées ou obtenues à l'appui d'autres demandes d'entraide judiciaire ;

34) Le Groupe des 77 et de la Chine reconnaît que la coopération internationale est importante pour la collecte et le partage des preuves électroniques dans le cadre d'enquêtes transfrontalières et qu'il est nécessaire de répondre rapidement et efficacement aux demandes d'entraide judiciaire liées à la conservation et à l'obtention de preuves électroniques. Le Groupe souligne également qu'il convient, dans ce contexte, de respecter les principes de souveraineté et de réciprocité ;

35) Le Groupe des 77 et de la Chine encourage également l'ONUDC à continuer d'offrir des programmes de formation et de renforcement des capacités en matière de lutte contre la cybercriminalité aux experts gouvernementaux nationaux, afin de renforcer les capacités de détection et d'enquête en matière de cybercriminalité. Ces activités de renforcement des capacités devraient tenir compte des besoins des pays en développement, mettre l'accent sur les vulnérabilités de chaque pays afin de fournir une assistance technique adaptée, et promouvoir l'échange de connaissances de pointe dans l'intérêt des praticiens et des parties prenantes ;

36) L'ONUDC a mis au point le « Rédacteur de requêtes d'entraide judiciaire » pour aider les praticiens de la justice pénale à rédiger des demandes d'entraide judiciaire. Il a également élaboré le « Guide pratique relatif aux demandes transfrontières de preuves électroniques », disponible sur demande pour les praticiens des États Membres. Ainsi, les pays peuvent tirer parti de l'utilisation de ces outils essentiels mis au point par l'ONUDC ;

37) La Commission pour la prévention du crime et la justice pénale devrait envisager de prolonger le plan de travail du Groupe d'experts au-delà de 2021 en tant que forum permettant aux praticiens d'échanger des informations sur la cybercriminalité ;

38) Certain(e)s intervenant(e)s ont recommandé que la négociation et l'adoption d'une convention des Nations Unies visant à promouvoir la coopération dans la lutte contre la cybercriminalité permettraient d'accroître l'efficacité de la coopération internationale dans ce domaine ;

39) Il a été recommandé que l'élaboration de toute nouvelle convention soit gérée par les experts de l'ONUDC à Vienne.

IV. Organisation de la réunion (*suite*)

C. Déclarations

2. Des déclarations ont été faites par les experts des États Membres et de l'État observateur non membre suivants : Algérie, Argentine, Arménie, Brésil, Canada, Chili, Colombie, Égypte, Équateur, État de Palestine, État de Palestine au nom du Groupe des 77 et de la Chine, États-Unis d'Amérique, Fédération de Russie, Inde, Liban, Mexique, Norvège, Pays-Bas, Portugal, Roumanie.