Nations Unies A/AC.291/4

Assemblée générale

Distr. générale
17 novembre 2021
Français
Original : anglais/arabe/chinois/
espagnol

Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

Compilation des commentaires communiqués par les États Membres sur le champ d'application, les objectifs et la structure (éléments) d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

Note du Secrétariat

Résumé

La présente note a été établie par le Secrétariat en vue de la première session du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, conformément aux instructions de la Présidente du Comité. Elle contient les commentaires reçus des États Membres sur le champ d'application, les objectifs et la structure (éléments) de la nouvelle convention.

V.21-08421 (F) 120122 130122

Merci de recycler

Table des matières

I. Introduction

1. Le 11 août 2021, la Présidente du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, M^me^ Faouzia Boumaiza Mebarki (Algérie), a invité les États Membres à présenter leurs commentaires sur le champ d'application, les objectifs et la structure (éléments) de la nouvelle convention en vue de la première session du Comité. Le délai de présentation de ces commentaires a été fixé au 29 octobre 2021, mais il a ensuite été prolongé jusqu'au 5 novembre 2021.

2. La Présidente a également chargé le secrétariat de rassembler les commentaires reçus et de les traduire dans les six langues officielles de l'ONU, afin qu'ils soient disponibles pour la première session du Comité spécial.

3. La présente note, qui a été établie par le secrétariat conformément aux instructions de la Présidente, contient les commentaires reçus des États Membres sur le champ d'application, les objectifs et la structure (éléments) de la nouvelle convention.

II. Commentaires reçus des États Membres

Australie

[Original : anglais]
[29 octobre 2021]

L'Australie se félicite de la possibilité qui lui est donnée de présenter ses commentaires sur le champ d'application, la structure et les objectifs d'une nouvelle convention internationale sur la cybercriminalité. Cette nouvelle convention offre une occasion unique d'obtenir un large consensus sur la coopération internationale en matière de lutte contre la cybercriminalité, permettant ainsi aux États de mieux combattre cette menace omniprésente et en constante évolution.

Une nouvelle convention n'aura de valeur que si elle peut susciter un large soutien de la majorité des États Membres, sur la base d'un accord consensuel obtenu à l'issue de discussions de bonne foi sous les auspices du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, créé en application des résolutions 74/247 et 75/282 de l'Assemblée générale. À cette fin, l'Australie est attachée à un processus ouvert, inclusif, transparent et multipartite, qui offre la meilleure chance de garantir aux États un résultat acceptable pour le plus grand nombre possible d'entre eux. Cela est conforme aux principes énoncés dans les observations que l'Australie a déjà communiquées au Comité spécial, ainsi que dans les observations conjointes auxquelles elle s'est associée. L'Australie saisit cette occasion pour rappeler les points soulevés dans ces observations.

La cybercriminalité menace tous les États, mais elle pose des problèmes particuliers aux petits États. Une coopération internationale efficace en matière de cybercriminalité est particulièrement importante pour les petits États insulaires en développement, afin de les aider à renforcer leur capacité nationale à lutter contre les activités de cybercriminalité transnationale. Il est impératif que ces États puissent participer de manière significative aux travaux du Comité spécial. L'Australie s'engage à veiller à ce que les pays insulaires du Pacifique aient des possibilités adéquates de participer aux travaux du Comité spécial. Elle se félicite de la décision d'appuyer la participation hybride (en présentiel et en ligne) aux sessions du Comité spécial et souligne l'importance de garantir aux plus petites délégations un temps de préparation et de participation suffisant.

Les entités du secteur privé jouent un rôle exceptionnel et inestimable dans la lutte contre la cybercriminalité. Pour aboutir, les travaux du Comité spécial doivent donc tenir compte des précieuses connaissances apportées par les parties prenantes de ce secteur. Les États devraient également être attentifs aux vastes connaissances et compétences que d'autres acteurs non étatiques, tels que les organisations de la société civile, les universités et les organismes intergouvernementaux, peuvent apporter au débat sur la meilleure façon de lutter contre la cybercriminalité. Pour garantir des débats éclairés et des résultats utiles, le Comité spécial doit donner à ces groupes toutes les occasions possibles de s'impliquer.

Champ d'application

Compte tenu de la brièveté du délai prévu pour les négociations, les États disposent d'un temps limité pour parvenir à un accord sur les nombreuses questions que comporte une nouvelle convention. Le champ d'application de la convention doit être clairement défini et devrait être étroitement axé sur la riposte de la justice pénale à la cybercriminalité. Il ne devrait pas englober des questions plus larges de cybersécurité qui sont traitées dans d'autres instances.

Pour accélérer nos travaux, les États devraient concentrer leur attention sur les domaines où des approches communes de la cybercriminalité sont nécessaires. Les travaux du Comité spécial devraient adopter une terminologie et des concepts relatifs à la cybercriminalité et à la coopération internationale en matière de justice pénale qui sont déjà bien compris par la communauté internationale. Nous n'avons pas besoin de « réinventer la roue » et nous ne souhaitons pas non plus créer d'ambiguïtés.

La nouvelle convention devrait donc largement mettre à profit la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention des Nations Unies contre la corruption, ainsi que d'autres concepts qui ont été adoptés par consensus lors des congrès des Nations Unies pour la prévention du crime et la justice pénale et dans d'autres instances des Nations Unies, le cas échéant. Elle devrait s'inspirer des instruments internationaux efficaces que les États ont déjà adoptés aux niveaux international et régional, tels que la Convention sur la cybercriminalité du Conseil de l'Europe, et elle doit éviter de porter atteinte aux normes existantes établies dans ces accords. Cela est conforme au mandat énoncé dans la résolution 74/247 de l'Assemblée générale, dans laquelle l'Assemblée a demandé que les travaux du Comité spécial tiennent pleinement compte des instruments internationaux existants et des initiatives prises aux niveaux national, régional et international.

En particulier, la convention devrait continuer d'utiliser le terme « cybercriminalité ». Ce terme, qui renvoie à un concept largement compris, a été employé dans d'innombrables documents de l'Organisation des Nations Unies, notamment les documents finals des douzième, treizième et quatorzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, ainsi que dans des résolutions de l'Assemblée générale (notamment la résolution 65/230) et de nombreuses autres résolutions et rapports de la Commission pour la prévention du crime et la justice pénale et du Conseil économique et social.

Éléments du traité (structure et objectifs)

Incrimination

La nouvelle convention offre la possibilité d'améliorer sensiblement la coopération internationale en matière de cybercriminalité. Grâce à des normes harmonisées visant un ensemble déterminé d'infractions de cybercriminalité, les États seront mieux à même de s'attaquer à la cybercriminalité aux niveaux mondial, régional et national.

À cette fin, l'Australie considère que la convention devrait adopter une approche ciblée des types d'actes criminels qui ont été fortement modifiés par la cybercriminalité. Les lois pénales nationales sont généralement plus que suffisantes pour définir les infractions courantes telles que la violation de domicile, le

vandalisme, le vol, les infractions liées aux stupéfiants et la criminalité violente. La convention n'a pas besoin de réinterpréter ces infractions simplement parce qu'un ordinateur ou un système d'information a été utilisé en vue de leur commission.

La nouvelle convention doit inclure de nouvelles normes pour l'incrimination des actes qui ne peuvent être commis qu'au moyen de systèmes d'information et de communication et dont on peut dire qu'il s'agit de « pure cybercriminalité » ou de « criminalité cyberdépendante ». Ces infractions n'existaient pas avant l'avènement des réseaux d'information et de communication, et les lois pénales nationales des États sont souvent insuffisantes ou manquent généralement d'uniformité lorsqu'on entend les appliquer à ces infractions. Dans ce domaine, des normes harmonisées en matière d'incrimination présenteront des avantages considérables pour les États, en ce qui concerne tant leurs propres mesures nationales de lutte contre la cybercriminalité que les mesures tendant à favoriser une plus grande coopération internationale.

De même, l'Australie considère qu'il existe certaines infractions « classiques » dont la portée, l'ampleur et la facilité de commission ont toutes été considérablement accrues par la rapidité, l'anonymat et le rayon d'action qu'offrent les réseaux d'information et de communication. On dit parfois qu'il s'agit d'infractions « facilitées par Internet ». La convention devrait aborder ces infractions de manière judicieuse, en élaborant un cadre clair permettant de déterminer pourquoi certaines infractions sont à ce point profondément modifiées par un « cyberélément » qu'elles nécessitent une nouvelle norme internationale harmonisée qui élève les actes en cause au-dessus des infractions « classiques ». La convention n'a pas besoin de créer de nouvelles catégories d'infractions pour chaque acte criminel existant susceptible d'incorporer un « cyberélément », en particulier lorsque la gravité ou la portée de l'acte incriminé n'est pas sensiblement modifiée par cet élément.

S'agissant de la catégorie des infractions « facilitées par Internet », l'Australie considère qu'il existe deux éléments qui devraient à l'évidence être pris en compte dans la convention : la grave menace posée par l'exploitation et l'abus sexuels des enfants en ligne, et l'augmentation importante et généralisée de la fraude et du vol facilités par Internet, y compris l'extorsion liée aux logiciels rançonneurs. L'Australie est prête à entendre les arguments en faveur de l'inclusion d'autres infractions facilitées par Internet, mais estime que, pour les raisons exposées ci-dessus, la convention devrait adopter une approche mesurée lorsqu'il s'agira d'inclure une nouvelle catégorie d'infractions.

La convention devrait également prendre dûment en considération les infractions principales et la responsabilité accessoire pour les infractions cyberdépendantes et les infractions facilitées par Internet. Elle devrait inclure les extensions habituelles de responsabilité pénale qui sont prévues dans des instruments tels que la Convention contre la criminalité organisée et la Convention contre la corruption. Compte tenu du rôle que joue la technologie dans la facilitation de la cybercriminalité, la convention devrait également prévoir une norme pénale harmonisée pour les infractions consistant à produire, procurer ou fournir des technologies et des logiciels adaptés uniquement ou principalement aux fins de la commission d'actes de cybercriminalité.

La cybercriminalité est un domaine qui évolue rapidement, et les cybercriminels cherchent constamment à déployer de nouvelles technologies et méthodologies pour étendre leurs activités et échapper aux services de détection et de répression. Pour remédier à cette situation, la convention doit faire en sorte que les normes d'incrimination soient rédigées de manière neutre d'un point de vue technologique et méthodologique, afin que le traité reste pertinent et efficace à l'avenir.

Mesures procédurales pour lutter contre la cybercriminalité

Le droit procédural est un élément essentiel des enquêtes et des poursuites en matière de cybercriminalité. La convention devrait fournir un cadre clair de mesures procédurales pour faire en sorte que les services de détection et de répression puissent

obtenir les preuves nécessaires à la lutte contre ce phénomène. Par son champ d'application, ce cadre de mesures procédurales devrait favoriser la mise en place de lois nationales claires et suffisamment solides pour permettre aux services de détection et de répression ou à d'autres autorités compétentes de lutter contre les problèmes que pose la cybercriminalité, notamment grâce à la détection des actes criminels, au démantèlement des opérations en cause, mais aussi à la prévention, aux enquêtes et aux poursuites.

Les mesures procédurales devraient également tenir compte de la nature des données électroniques, de sorte que les services de détection et de répression et d'autres autorités compétentes puissent obtenir ces données rapidement et efficacement et que les méthodologies et pratiques criminelles dans le cyberespace n'anéantissent pas les efforts de collecte des autorités concernées. Les types de mesures procédurales prévues pourraient inclure des pouvoirs de perquisition et de saisie, des pouvoirs liés à la production de données (tels que l'accès aux communications stockées et les activités d'interception), ainsi que des demandes ou des ordres de divulgation des données considérées en cas d'urgence. Les mesures procédurales doivent être étayées par des restrictions et des garanties solides qui protègent dûment les droits humains et l'état de droit.

Les États devront probablement examiner comment les pratiques nationales en matière de collecte de données électroniques entre les différents pays seront prises en compte dans une nouvelle convention.

Coopération internationale et assistance technique

La cybercriminalité est en très grande partie de nature transnationale. La coopération internationale, appuyée par des règles d'incrimination harmonisées, est essentielle pour que les États puissent enquêter sur les cybercriminels et les poursuivre avec efficacité.

Au cours des dernières décennies, la communauté internationale a fait des progrès considérables en matière de coopération internationale à l'appui de la justice pénale, en mettant au point des outils efficaces dans le cadre d'une série de traités internationaux en vigueur régissant l'entraide judiciaire, l'extradition et d'autres formes de coopération internationale. Les dispositions de la Convention contre la criminalité organisée et de la Convention contre la corruption, par exemple, constituent une excellente base pour une telle coopération, sachant qu'elles ont été presque universellement adoptées.

La nouvelle convention devrait s'inspirer autant que possible des dispositions similaires de la Convention contre la criminalité organisée et de la Convention contre la corruption en ce qui concerne l'entraide judiciaire, l'extradition, le transfèrement des détenus et le recouvrement du produit du crime. Ces dispositions se sont avérées efficaces et bénéficient d'un large soutien international. Conformément au mandat énoncé dans la résolution 74/247 de l'Assemblée générale, il convient également de veiller à ce que la nouvelle convention complète et ne compromette pas les autres mécanismes existants de coopération internationale en matière de justice pénale.

D'autres régimes internationaux et régionaux, assortis de restrictions et de garanties solides, offrent des cadres efficaces pour la coopération internationale en matière de lutte contre la cybercriminalité. La nouvelle convention devrait s'inspirer autant que possible de ces régimes. La Convention sur la cybercriminalité du Conseil de l'Europe, qui continue d'offrir une base utile pour la coopération internationale entre un grand nombre d'États de toutes les régions du monde, en est le principal exemple.

Outre la coopération internationale, la nouvelle convention devrait donner une impulsion appréciable aux efforts visant à améliorer la capacité internationale de lutte contre la cybercriminalité. Son libellé devrait réaffirmer le rôle primordial de l'Office des Nations Unies contre la drogue et le crime en matière d'assistance technique et

de renforcement des capacités, notamment en tant que responsable du Programme mondial contre la cybercriminalité.

Garanties visant à protéger et promouvoir les droits humains

L'accès des États aux données électroniques et de télécommunications des particuliers a, de par sa nature même, un impact sur les droits individuels. La convention doit réaffirmer la responsabilité qu'ont les États de promouvoir et protéger les droits humains des particuliers dans le cadre des efforts qu'ils déploient pour lutter contre la cybercriminalité, conformément au droit international des droits de l'homme.

Les droits des particuliers à la vie privée et à la liberté d'opinion, d'expression et d'association doivent tous rester dûment protégés, conformément aux normes internationales en vigueur. Parmi les autres droits qui doivent également être protégés figurent le droit à un procès équitable, y compris l'égalité devant la loi, ainsi que le droit de ne pas être soumis à la torture et à des peines ou traitements inhumains ou dégradants, à la détention arbitraire et à la discrimination. La communauté internationale a réaffirmé à plusieurs reprises que ces droits s'appliquaient aussi bien en ligne que hors ligne, et la convention devrait réitérer l'obligation qu'ont les États de faire respecter ces droits dans le cadre de leurs opérations de lutte contre la cybercriminalité.

Structure et méthode de travail

Dès lors que les États auront eu la possibilité de donner leur avis sur le champ d'application de la convention à la première session de négociation qui se tiendra en janvier 2022, l'Australie s'attend à ce qu'un consensus sur la structure de la convention se dégage rapidement.

Après que les États auront donné leur avis sur le champ d'application, la structure et les objectifs de la nouvelle convention, en janvier 2022, l'Australie suggère qu'ils soient invités à soumettre des propositions sur les dispositions à inclure dans chaque élément structurel de la nouvelle convention (par exemple, des propositions sur l'incrimination et la coopération internationale). La Présidente, agissant en consultation avec le Bureau, au besoin, devrait ensuite s'employer à synthétiser ces diverses propositions sous la forme d'un projet que les États pourraient alors négocier, chaque série de dispositions devant être examinée tour à tour selon un plan de travail établi par le Comité spécial lors de sa première réunion.

À l'issue des négociations préliminaires sur chaque élément de la structure, la convention pourrait être négociée plus avant dans son ensemble, toujours selon un plan de travail établi par le Comité spécial lors de sa première réunion et supervisé ensuite par la Présidente.

Brésil

[Original : anglais]
[29 octobre 2021]

Comme de nombreux pays, le Brésil est aux prises avec la cybercriminalité, phénomène qui gagne en fréquence et en complexité. Le déplacement de diverses infractions pénales vers des plateformes numériques exige des actions décisives pour adapter la réponse normative et répressive à apporter face aux menaces, y compris au niveau international. La portée géographique de ces infractions et leur rapidité d'exécution mettent à l'épreuve les mécanismes traditionnels de détection et de répression et de coopération juridique dans le monde entier.

Les difficultés sont immenses. Les fournisseurs d'accès à Internet, qui détiennent des informations importantes nécessaires aux enquêtes sur la cybercriminalité et à la collecte des éléments de preuve électroniques, ont souvent

leur siège physique dans un pays, mais ils offrent des services sur différents continents et sauvegardent les informations sur des serveurs hébergés encore ailleurs sur la planète. En pareil cas, les services de détection et de répression s'efforcent d'identifier et de contacter quiconque exerce une compétence sur les données et a un accès direct à celles-ci.

La cohésion et la coordination entre les pays au niveau international constituent une avancée indispensable pour engager des poursuites contre les auteurs d'actes de cybercriminalité. Une coopération accrue et améliorée est nécessaire. Des moyens de coopération réactifs et directs permettant aux services de détection et de répression d'échanger en temps voulu des éléments de preuve tirés de différentes affaires qui impliquent le même groupe criminel sont nécessaires pour assurer l'efficacité des mesures visant à démanteler ce type de groupes.

Le Brésil tient à s'impliquer pleinement dans la négociation d'une convention générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Il y a là une occasion unique d'établir des normes communes de coopération pour traiter une question aussi fondamentalement transnationale, en s'appuyant sur les meilleures traditions et pratiques en la matière.

Du point de vue du Brésil, pour être en mesure de faire face aux difficultés susmentionnées, une future convention doit inclure les éléments ci-après en termes d'objectifs, de champ d'application et de structure.

Objectifs

La convention devrait avoir pour principal objectif de fournir des outils spécifiques pour la coopération internationale, afin que les États parties aient accès en temps voulu aux preuves et aux autres informations qui contribuent aux enquêtes sur les actes de cybercriminalité et à la poursuite pénale de leurs auteurs. Malgré le mérite intrinsèque de cet objectif premier, elle devrait, dans l'idéal, en envisager également deux autres : a) l'établissement d'obligations minimales en matière d'incrimination (droit pénal matériel) dans le système juridique de chaque État partie ; et b) l'instauration d'obligations minimales dans le système juridique de chaque État partie pour permettre des interventions, des enquêtes et des poursuites rapides (droit pénal procédural).

Le Brésil soutient sans réserve l'idée d'une convention universelle. Nous sommes sensibles aux difficultés inhérentes à la négociation d'un instrument contenant des normes minimales en matière d'incrimination, compte tenu en particulier de la modernité et de la volatilité du phénomène. Cependant, des précédents ont déjà fait leurs preuves dans ce sens. Dans d'autres domaines liés à la criminalité, auxquels s'appliquent les conventions universelles sur la criminalité en vigueur, des négociations efficaces ont permis à la plupart des pays du monde d'adhérer à des normes minimales de fond. Les discussions ne doivent pas partir d'une antithèse présupposée entre la portée géographique et la portée des mesures d'incrimination, mais plutôt de l'idée que les négociations elles-mêmes seront la méthode la plus sûre pour dégager, dans toute la mesure possible, le meilleur consensus minimal sur le droit pénal matériel en matière de cybercriminalité. Aussi restreint soit-il, un consensus minimal sur les incriminations – fondé sur des concepts neutres et génériques – pourrait limiter le champ d'action géographique des cybercriminels, faciliter l'échange de données d'expérience et atténuer les disparités normatives entre les pays qui exigent l'application du principe de double incrimination pour coopérer.

La rapidité de la coopération internationale dépendra toujours des instruments procéduraux dont disposent les enquêteurs, les procureurs et les juges d'un pays à l'autre. Les instruments traditionnels de la coopération judiciaire, tels que la commission rogatoire et la reconnaissance des jugements étrangers, ne sont nulle part en mesure, à eux seuls, d'assurer une réaction appropriée face à la cybercriminalité. Du fait du caractère transnational et extrêmement volatile du phénomène, il faut procéder à une uniformisation des procédures, même si celle-ci doit être aussi souple

et générique que nécessaire pour tenir compte de toutes les spécificités des systèmes juridiques nationaux concernés. Cette uniformisation devrait toutefois pour l'essentiel porter sur certaines normes minimales afin de permettre la conservation rapide des preuves électroniques, qui serait déclenchée par un mécanisme international réactif et direct, faute de quoi il sera impossible d'identifier les criminels, notamment dans les cas de criminalité organisée.

Champ d'application

La convention devrait servir de base pour l'échange de preuves et de données concernant : a) les infractions contre les systèmes informatiques ; et b) toutes les infractions qui sont commises par des moyens électroniques. Dans l'idéal, les données électroniques relatives aux connexions, au contenu et aux abonnés devraient y être abordées.

La convention devrait également permettre aux parties de formuler des demandes de coopération internationale (pour la conservation rapide des données électroniques et l'entraide judiciaire) et de transmettre spontanément des informations à d'autres pays. Un chapitre devrait être consacré à la mise en place d'un réseau international de professionnels qui seraient chargés de répondre aux cas urgents. Ce type de mécanisme opérationnel renforce l'idée qu'une telle convention oblige à mettre sur pied un organe de décision pour le suivi et l'examen de son application.

En tant qu'instrument-cadre, le traité pourrait prévoir la possibilité de négocier des protocoles additionnels, qui permettraient d'approfondir la coopération sur des types particuliers de cybercriminalité.

La convention devrait donc être un instrument d'application pratique du droit pénal, sans s'appesantir sur les principes de paix et de sécurité internationales, sur la cyberdéfense ou sur des questions relatives à la structure ou à la gouvernance de l'Internet aux niveaux national, régional ou mondial.

Structure

Compte tenu des considérations déjà évoquées, le Brésil estime que la convention devrait avoir la structure suivante :

Chapitre I. Incrimination

Chapitre II. Règles de procédure pénale permettant des enquêtes et des poursuites rapides

Chapitre III. Coopération internationale

A. Conservation rapide des données électroniques

B. Entraide judiciaire

C. Échange spontané d'informations

Chapitre IV. Réseau de coopération

Chapitre V. Mécanisme de suivi et d'examen de l'application

Canada

[Original : anglais]
[1er novembre 2021]

La présente communication du Canada fait suite à l'invitation, en date du 11 août, que le secrétariat du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles a adressée aux États Membres pour les engager à soumettre leurs vues sur le champ d'application, les objectifs et la structure (éléments) de la nouvelle convention.

Pour l'élaboration des présentes observations, le Canada s'inspire de l'important travail sur la cybercriminalité réalisé depuis plus de 20 ans au sein de l'ONU sous les auspices de la Commission pour la prévention du crime et la justice pénale, en particulier par le Groupe intergouvernemental d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, l'Office des Nations Unies contre la drogue et le crime, par l'intermédiaire de son Programme mondial contre la cybercriminalité, et les congrès des Nations Unies pour la prévention du crime et la justice pénale. Ces initiatives ont préparé le terrain pour l'élaboration d'une convention des Nations Unies qui devrait se concentrer exclusivement sur la lutte contre la cybercriminalité et laisser de côté la cybersécurité, la cybergouvernance et d'autres questions connexes mieux traitées dans d'autres instances des Nations Unies.

Conformément à la résolution 75/282 de l'Assemblée générale et à ses communications antérieures au Comité spécial, le Canada tient à rappeler que la négociation de la nouvelle convention doit être un processus transparent et inclusif, offrant à la société civile et à d'autres parties prenantes une véritable occasion d'y participer.

Champ d'application

La nouvelle convention devrait fournir un cadre pour lutter contre la cybercriminalité et les infractions pénales graves fréquemment commises au moyen de systèmes informatiques, qui comprendrait les éléments suivants :

a) Des dispositions relatives aux infractions en matière de cybercriminalité proprement dites et aux enquêtes et poursuites visant la cybercriminalité ainsi que les infractions pénales graves fréquemment commises au moyen de systèmes informatiques ;

b) Des dispositions relatives à la coopération internationale en ce qui concerne ce qui précède, ainsi qu'à l'obtention de preuves électroniques d'autres infractions pénales ;

c) Des dispositions énonçant des mesures destinées à prévenir la cybercriminalité ; et

d) Des dispositions énonçant des mesures qui encouragent les États Membres et d'autres parties prenantes à entreprendre des activités suivies d'assistance technique et de renforcement des capacités.

Les éléments de la nouvelle convention doivent être conformes aux obligations internationales relatives aux droits humains, plus particulièrement en ce qui concerne les libertés d'expression, d'opinion et d'association, ainsi que le droit de ne pas subir d'immixtions illégales ou arbitraires dans sa vie privée.

Objectifs

Les objectifs de la nouvelle convention devraient être les suivants :

a) Partant d'une conception commune, établir des règles de base pour les infractions pénales proprement dites, les pouvoirs procéduraux et la coopération internationale visant à lutter contre la cybercriminalité ;

b) Veiller à ce que les dispositions soient rédigées de manière neutre sur le plan technologique pour éviter qu'elles ne deviennent obsolètes ou inapplicables à mesure que les technologies évoluent ;

c) Promouvoir et faciliter la coopération internationale visant à lutter conjointement contre la cybercriminalité ;

d) Établir le pouvoir de recueillir, d'obtenir et de communiquer les preuves électroniques d'autres infractions ;

e) Éliminer les refuges pour les cybercriminels ;

f) Respecter les obligations internationales relatives aux droits humains, en particulier en ce qui concerne les libertés d'expression, d'opinion et d'association, ainsi que le droit de ne pas subir d'immixtions illégales ou arbitraires dans sa vie privée ;

g) Être cohérente avec les traités des Nations Unies en vigueur dans le domaine de la prévention de la criminalité et de la justice pénale, en particulier la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention des Nations Unies contre la corruption, et tenir compte des instruments multilatéraux qui ont déjà prouvé leur utilité dans la lutte contre la cybercriminalité, notamment la Convention sur la cybercriminalité du Conseil de l'Europe ; et

h) Aider les États Membres à renforcer les moyens de lutte contre la cybercriminalité grâce à des activités d'assistance technique et de renforcement des capacités.

Structure

En ce qui concerne la structure de la nouvelle convention, outre des définitions claires et des dispositions finales, le Canada estime qu'il est important que la convention comprenne les cinq éléments suivants :

a) Des dispositions matérielles relatives aux infractions exigeant des États Membres qu'ils adoptent les mesures législatives et autres nécessaires pour :

i) Ériger en infraction pénale les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes, réseaux et données informatiques, ainsi que l'usage frauduleux de ceux-ci ; et

ii) Faire en sorte que certaines infractions classiques fréquemment commises par l'intermédiaire de systèmes informatiques soient couvertes de manière adéquate par leur droit pénal, par exemple la diffusion de pornographie mettant en scène des enfants ;

b) Des dispositions procédurales exigeant des États Membres qu'ils adoptent les mesures législatives et autres nécessaires pour établir le pouvoir de conserver et d'obtenir des preuves électroniques d'infractions pénales lorsque ces preuves sont stockées sur des systèmes informatiques se trouvant à l'étranger, dans plusieurs pays ou en lieu inconnu. Si des pouvoirs d'enquête plus généraux, tels que les pouvoirs de perquisition et de saisie et les injonctions de produire, devraient être inclus dans la nouvelle convention, des outils d'enquête plus spécialisés devraient aussi y figurer pour contrer la rapidité avec laquelle les infractions peuvent être commises et le caractère éphémère et volatile des preuves électroniques. Ces dispositions devraient faire l'objet de garanties afin que les activités des services de détection et de répression soient conformes aux obligations internationales relatives aux droits humains ;

c) La coopération internationale étant décisive dans la lutte contre la cybercriminalité, des mécanismes destinés à faciliter la coopération internationale formelle et informelle pour la détection des actes de cybercriminalité, les enquêtes à leur sujet et la poursuite de leurs auteurs, ainsi que pour l'obtention de preuves électroniques d'autres infractions pénales ;

d) Des mesures préventives similaires à celles prévues par la Convention contre la criminalité organisée et la Convention contre la corruption, par exemple, des dispositions relatives aux initiatives de sensibilisation et d'éducation. Les partenariats multipartites et la société civile peuvent jouer un rôle essentiel, dont ces dispositions devraient tenir compte ;

e) Des dispositions encourageant les États Membres à renforcer les moyens de lutte contre la cybercriminalité grâce à des activités d'assistance technique et de renforcement des capacités, et éventuellement des dispositions visant à :

i) Faciliter la participation multipartite ;

ii) Encourager la collaboration avec l'Office des Nations Unies contre la drogue et le crime et son Programme mondial contre la cybercriminalité pour renforcer les compétences des professionnels et des autorités centrales concernant l'utilisation de la technologie, le but étant de faciliter la coopération internationale visant à lutter contre la cybercriminalité ; et

iii) Mettre au point des programmes de formation à l'intention des enquêteurs et des procureurs et favoriser l'échange d'informations et de données d'expérience avec les parties prenantes concernées.

Chili

[Original : anglais]
[5 novembre 2021]

Le Gouvernement chilien a le plaisir de répondre à l'invitation faite aux États Membres de soumettre leurs vues sur le champ d'application, les objectifs et la structure (éléments) de la nouvelle convention, eu égard à l'application des résolutions 74/247 et 75/282 de l'Assemblée générale.

Le Chili estime que la nouvelle convention ne devrait pas être en contradiction avec d'autres traités ou accords préexistants sur la cybercriminalité. Elle devrait reposer sur la coopération internationale et l'assistance technique, qui constituent le fondement de l'approche multilatérale en matière de lutte contre la cybercriminalité. Les vues de tous les pays doivent être considérées comme d'égale importance, afin d'assurer un processus ouvert, inclusif, transparent et multipartite.

1. Aspects généraux

a) *Compétence*. La nouvelle convention donne une excellente occasion d'examiner cette question, qui est à la base de nombreux outils procéduraux susceptibles d'être abordés.

b) Il convient de veiller à ce que les définitions soient formulées de manière générale, afin d'en assurer la pertinence et l'applicabilité dans le contexte d'une évolution technologique rapide, et qu'elles visent entre autres, par exemple, les différents types de données.

2. Droit pénal matériel

a) *Incorporation de l'infraction pénale de recel de données informatiques*. Bien que certains pays aient une conception limitée de cette infraction, il semble approprié d'inclure dans la convention les actes illégaux de ce type lorsque les « biens » volés correspondent à des données informatiques et que la personne qui les stocke en connaît ou ne peut en ignorer l'origine douteuse ;

b) S'agissant des auteurs des infractions et des personnes qui participent à leur commission, il semble bon de traiter en particulier la collaboration offerte par le bénéficiaire de sommes d'argent ou de titres volés au moyen d'une utilisation frauduleuse de l'informatique. En effet, compte tenu des particularités que présente cette catégorie d'infractions et des difficultés qu'elle pose aux enquêteurs dans la grande majorité des cas, il est utile d'accorder un traitement spécial aux poursuites engagées contre ces personnes qui, en règle générale, constituent le premier maillon à cibler pour remonter la chaîne d'infractions ; il est donc approprié, du fait de leur participation, d'élever celles-ci au rang d'auteurs de la fraude, sans préjudice de la possibilité de leur proposer une réduction de peine si elles coopèrent effectivement à la capture des autres auteurs de l'infraction informatique.

3. Règles de droit procédural

a) Il convient de discuter des nouvelles idées et des nouveaux outils de travail dont les autorités pourraient se servir pour détecter les infractions qui sont en gestation ou qui sont destinées à être commises sur Internet, ainsi que de la manière la plus efficace d'y faire face.

b) Il semble opportun de discuter de l'équilibre à trouver entre la nécessaire protection des citoyens et des données personnelles, d'une part, et les enquêtes criminelles, d'autre part, étant donné qu'une protection excessive de ces informations pourrait avoir des conséquences sur la mise au point de procédures d'enquête permettant d'engager en temps voulu des poursuites pénales appropriées contre ce type d'infractions, qui bénéficient de l'anonymat, de la transnationalité et du manque de traçabilité associés aux actes en question.

4. Chapitre sur la coopération internationale

a) Il est important d'établir des principes sur l'entraide judiciaire en matière pénale.

b) Les pays devraient étudier des moyens qui permettraient aux enquêteurs et aux procureurs chargés de la lutte contre la cybercriminalité d'échanger entre eux des informations de manière rapide et sûre.

c) Les pays devraient coopérer étroitement, conformément à leurs systèmes juridiques et administratifs respectifs, en vue de renforcer l'efficacité de la détection et de la répression des infractions de cybercriminalité. Chaque pays devrait adopter des mesures efficaces pour établir des voies de communication entre ses autorités, organismes et services compétents afin de faciliter l'échange sûr et rapide d'informations concernant tous les aspects de la cybercriminalité.

d) Considérer la transmission électronique des échanges relatifs à l'entraide judiciaire comme une procédure valable à appliquer en permanence, et pas seulement en cas d'urgence.

e) Conserver et communiquer les données.

f) Analyser l'apport positif des réseaux fonctionnant 24 heures sur 24 et 7 jours sur 7 en tant que contribution innovante à la coopération internationale.

g) Réglementer les cas urgents.

h) Les pays devraient conjointement reconnaître l'existence d'une « fracture numérique », certains n'ayant pas les moyens de prévenir, de détecter et de combattre la cybercriminalité et étant plus vulnérables face aux défis qu'elle pose.

5. Outils spécialisés de coopération internationale

a) La communication de données par les fournisseurs d'accès à Internet et leur relation avec les États.

b) L'accès transfrontalier aux données.

c) Les techniques d'enquête spéciales : agents infiltrés en ligne, équipes communes d'enquête et enquêtes conjointes, entre autres.

6. Prévention

a) La prévention de la cybercriminalité requiert la participation de diverses parties prenantes, notamment des gouvernements, des services de détection et de répression, du secteur privé, des organisations internationales, des organisations non gouvernementales et du milieu universitaire.

b) Il convient de promouvoir des stratégies de prévention axées sur les victimes qui traiteront de cybercriminalité interpersonnelle.

c) Les pays devraient envisager de mettre en œuvre des mécanismes de coopération avec les entreprises, notamment en ce qui concerne le renvoi aux autorités nationales compétentes et le retrait de contenus illicites nuisibles, comme le retrait de contenus liés à l'exploitation sexuelle des enfants et d'autres contenus violents odieux.

7. Prise en compte des questions de genre dans le contexte d'une convention sur la cybercriminalité

a) Prendre en considération les questions de genre dans l'application des dispositions de la convention et l'évaluation de leur impact, et prévoir une analyse tenant compte des questions de genre lorsqu'il s'agit de l'utilisation des technologies de l'information et des communications, en particulier quand il est question des dimensions de genre liées à la cybercriminalité, afin de promouvoir l'égalité des genres et l'autonomisation des femmes en ligne et hors ligne.

b) S'attaquer à la cybercriminalité et prévenir et combattre la violence à l'égard des femmes et des enfants.

Chine

[Original : chinois]
[5 novembre 2021]

La Chine se félicite que la Présidente du Comité spécial des Nations Unies chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ait invité les États Membres à présenter leurs commentaires sur le champ d'application, les objectifs et la structure (éléments) de la convention. Conformément à la résolution 75/282 de l'Assemblée générale, le Comité spécial doit présenter un projet de convention à celle-ci à sa soixante-dix-huitième session. La Chine espère que des débats constructifs se tiendront sous la direction de la Présidente et permettront d'aboutir, conformément au calendrier prévu, à une nouvelle convention universelle, faisant autorité et acceptable pour toutes les parties, de manière à offrir un cadre juridique propre à renforcer la coopération dans la lutte contre la cybercriminalité au niveau mondial.

Les États Membres ont jusqu'à présent utilisé les mécanismes pertinents de l'Organisation des Nations Unies pour débattre en détail de la lutte contre la cybercriminalité et sont convenus de certaines conclusions et recommandations. L'un d'eux a également présenté un projet de convention générale, qui constitue une référence importante pour la négociation de la convention. La Chine salue les efforts déployés par la Présidente pour engager les États Membres à soumettre activement leurs commentaires et leurs propositions, et soutient les préparatifs qu'elle mène en vue de l'élaboration d'un avant-projet de convention fondé sur les soumissions des États Membres afin de commencer à négocier le texte de la convention dès que possible.

Afin d'appuyer les travaux de la Présidente et du Comité spécial, la Chine a formulé les commentaires ci-après sur le champ d'application, les objectifs et la structure (éléments) de la convention et se tient prête à prendre part à des négociations constructives avec l'ensemble des parties.

I. Objectifs

a) Promouvoir et renforcer les mesures visant à combattre et à prévenir de manière plus efficace l'utilisation des technologies de l'information et des communications à des fins criminelles, en vue de réaliser la vision d'un avenir commun dans le cyberespace.

b) Promouvoir, faciliter et appuyer la coopération internationale visant à prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles, en tenant compte des particularités de ces technologies et de la nécessité de combattre les activités criminelles connexes. Cette coopération internationale peut consister notamment à coordonner les normes d'incrimination entre les États Membres, à fournir des orientations pour régler les conflits de compétence et à mettre en place des arrangements institutionnels plus ciblés pour la coopération entre services de détection et de répression, l'entraide judiciaire, l'extradition et le recouvrement d'avoirs.

c) Améliorer la coopération en matière de renforcement des capacités et d'assistance technique et promouvoir l'échange d'informations dans ce domaine, conformément aux besoins de coopération internationale d'ordre plus général et aux intérêts des pays en développement.

II. Champ d'application

La convention devrait s'appliquer à la prévention, aux enquêtes et aux poursuites concernant l'utilisation des technologies de l'information et des communications à des fins criminelles par des personnes ou des groupes criminels, ainsi qu'au blocage, au gel, à la saisie, à la confiscation et à la restitution du produit de la criminalité informatique.

La notion d'utilisation des technologies de l'information et des communications à des fins criminelles devrait désigner, au minimum, les infractions commises contre des installations, des systèmes et des données informatiques ainsi que celles commises à l'aide desdites technologies.

III. Structure (éléments)

La convention pourrait être divisée en sept chapitres : dispositions générales ; prévention ; incrimination, détection et répression ; coopération internationale ; assistance technique et échange d'informations ; mécanisme d'application ; et dispositions finales.

Les suggestions préliminaires suivantes concernent les éléments de ces différents chapitres.

1. Dispositions générales

Outre les objectifs et le champ d'application, ce chapitre devrait comprendre les éléments ci-après :

a) *Protection de la souveraineté.* Le principe de l'égalité souveraine de tous les États consacré par la Charte des Nations Unies est la norme fondamentale des relations internationales modernes. Les États Membres sont largement favorables à ce que le principe de la souveraineté soit également appliqué au cyberespace. La convention devrait prévoir que les États parties doivent s'acquitter des obligations découlant de celle-ci dans le respect des principes de l'égalité souveraine de tous les États, de l'intégrité territoriale et de la non-ingérence dans les affaires intérieures d'autres États ;

b) *Terminologie.* Il convient de définir les termes clefs figurant dans la convention, tels que « preuve électronique », « informations personnelles », « infrastructures d'information critiques », « stockage en nuage », « fournisseur de services de réseau », « logiciel malveillant », « botnet », « information préjudiciable » et « cyberattaque ».

2. Prévention

Il convient de souligner l'importance que revêt la prévention de l'utilisation des technologies de l'information et des communications à des fins criminelles. Il faudrait, à titre de principe de base, « donner la priorité à la prévention, tout en luttant

contre la criminalité ». Le rôle des gouvernements et du secteur privé dans la prévention de la criminalité devrait être défini clairement, et les gouvernements devraient élaborer des mesures de prévention ciblées tout en encourageant la participation de la société et la coopération public-privé. Les points suivants devraient être inclus :

a) Les États Membres devraient être encouragés à désigner des institutions spécialisées chargées d'élaborer des politiques de prévention de l'utilisation des technologies de l'information et des communications à des fins criminelles et de procéder à des évaluations régulières. Ils devraient prendre des mesures pour sécuriser les infrastructures d'information critiques et mettre en place des systèmes de protection reposant sur différents niveaux de réseaux. Il faudrait adopter différentes technologies et mesures de gestion de la sécurité de l'information en fonction des installations de réseau afin de protéger les infrastructures d'information critiques contre les attaques de criminels ou de groupes criminels. Les moyens dont disposent les ministères compétents pour prévenir la criminalité devraient être renforcés ;

b) Les États Membres devraient améliorer leurs lois existantes ou en adopter de nouvelles pour préciser les obligations qui incombent au secteur privé, notamment aux fournisseurs de services de réseau, dans la prévention de l'utilisation des technologies de l'information et des communications à des fins criminelles. Ces obligations devraient inclure, entre autres, des mesures de sécurité (par exemple, la mise au point de plans d'urgence en cas d'atteintes à la sécurité de réseaux, le traitement rapide des faiblesses des systèmes et du matériel, des virus informatiques, des attaques de réseaux ou des intrusions dans un réseau, et la prise de mesures en temps réel lorsqu'il s'avère que les services desdits fournisseurs sont peut-être utilisés pour des activités criminelles) et la conservation des données de connexion (les gouvernements devraient préciser la norme concernant la teneur de ces données et la durée de leur conservation). Lors de la détermination des obligations des fournisseurs de services de réseau, il convient de prendre des dispositions adaptées à chaque niveau et conformes au principe de proportionnalité, en tenant pleinement compte des différences de capacité qui existent entre les fournisseurs en fonction de leur taille ;

c) Les gouvernements, le secteur privé et les collectivités devraient être encouragés à nouer diverses formes de coopération public-privé. Il faudrait notamment redoubler d'efforts pour sensibiliser le public à la prévention de la criminalité.

3. Incrimination, détection et répression

Les criminels et les groupes criminels détournent de plus en plus les technologies de l'information et des communications pour commettre des infractions, ce qui a conduit à l'apparition d'une « chaîne de production » obscure spécialisée dans le développement de ces technologies à des fins criminelles ainsi qu'à des opérations faisant intervenir ces technologies et les données qui y sont associées. La convention devrait établir un cadre de coordination en matière d'incrimination qui soit plus souple et davantage tourné vers l'avenir, de manière à répondre aux besoins découlant des évolutions actuelles et futures des technologies de l'information et des communications et à la nécessité de lutter contre la criminalité. Elle devrait aussi prévoir les mécanismes voulus en ce qui concerne la compétence, la détection et la répression et les preuves électroniques :

a) Les États Membres devraient être tenus d'incriminer l'intrusion dans les installations, les systèmes et les données informatiques ou dans les infrastructures d'information critiques, ainsi que leur destruction. Les actes incriminés pourraient inclure notamment l'accès illégal à des systèmes informatiques, l'atteinte illégale à l'intégrité de tels systèmes, l'acquisition illégale de données informatiques, l'atteinte illégale à l'intégrité de telles données et l'atteinte à des infrastructures d'information critiques ;

b) La convention pourrait énumérer, selon qu'il convient, les activités criminelles qui sont menées au moyen des technologies de l'information et des

communications et qui sont largement reconnues par la communauté internationale, telles que la cyberextorsion, la cyberfraude, la cyberpornographie (en particulier la pédopornographie), l'utilisation des technologies de l'information et des communications aux fins de violation du droit d'auteur et de droits connexes, et l'utilisation d'Internet aux fins de commission d'actes de terrorisme, d'incitation à leur commission ou de diffusion d'informations préjudiciables, entre autres ;

c) En ce qui concerne les autres infractions commises à l'aide des technologies de l'information et des communications, il convient d'insister sur le fait que les États Membres peuvent combattre et prévenir les infractions qui ne sont pas énumérées dans la convention et qu'ils peuvent coopérer au niveau international conformément à la convention, à d'autres conventions internationales et à leurs législations nationales applicables ;

d) Compte tenu de l'« industrialisation » croissante des infractions commises à l'aide des technologies de l'information et des communications, la « chaîne de production » obscure devrait entrer dans le champ d'application des mesures d'incrimination et des mesures plus strictes devraient être prévues pour réprimer la complicité ou les actes préparatoires en vue de la commission de ces infractions, y compris l'élaboration, la vente ou la diffusion de ces technologies ou de données à des fins criminelles ;

e) S'agissant de l'expression « preuve électronique », il convient de définir les règles permettant d'identifier ce type de preuves dans les procédures judiciaires pénales, et notamment de déterminer la manière d'en vérifier l'authenticité, l'intégrité, la légitimité et la pertinence ;

f) Les États Membres pourraient être tenus d'améliorer leurs lois existantes ou d'en adopter de nouvelles afin de préciser les obligations du secteur privé, telles que l'obligation pour les fournisseurs de services de réseau de coopérer avec les services de détection et de répression dans le cadre de la surveillance des infractions, des enquêtes menées à leur sujet et des mesures prises pour les combattre. Ces obligations devraient notamment comprendre la conservation des données de connexion, la conservation des données et des éléments de preuve conformément à des normes unifiées relatives à la teneur et à la durée et la coopération avec les services de détection et de répression. Lors de la détermination des obligations des fournisseurs de services de réseau, il convient de prendre des dispositions adaptées à chaque niveau et conformes au principe de proportionnalité, en tenant pleinement compte des différences de capacité qui existent entre les fournisseurs en fonction de leur taille. Si un fournisseur ne s'acquitte pas des obligations qui lui incombent, les États Membres devraient lui infliger des sanctions administratives et pénales efficaces, conformément à leur législation nationale ;

g) Il conviendrait de donner des orientations permettant de régler les conflits de compétence. Compte tenu des particularités du cyberespace et des technologies de l'information et des communications, des normes sur la façon de déterminer la compétence et d'éviter les conflits en la matière devraient être établies. La compétence devrait être fondée sur un lien « réel et suffisant » avec l'activité criminelle en question, la priorité étant donné au lieu où les conséquences de l'activité se produisent, au lieu de commission de l'infraction et au lieu où se trouve la personne ou le groupe qui l'a commise. S'il est difficile de formuler de telles normes, il conviendrait alors de proposer des normes d'exclusion ; par exemple, un État ne devrait pas pouvoir se déclarer compétent dans une affaire relative aux technologies de l'information et des communications au seul motif que les données ont transité par son territoire. En cas de conflit, la compétence devrait être déterminée au moyen de consultations, conformément aux principes du *forum conveniens* et de la facilitation du recouvrement d'avoirs ;

h) Des dispositions concernant, notamment, la complicité de commission d'une infraction, la préparation d'une infraction, la tentative de commission d'une infraction et la commission d'une infraction par une entité devraient aussi être prévues.

4. Coopération internationale

L'utilisation des technologies de l'information et des communications à des fins criminelles présente un caractère fortement transnational et constitue un défi commun pour la communauté internationale. En outre, l'anonymat et la sophistication des activités criminelles ainsi que l'instabilité et le caractère périssable des preuves électroniques compromettent sérieusement les mécanismes de coopération internationale tels que l'entraide judiciaire dans le cadre juridique international existant. Les États Membres devraient coopérer entre eux dans toute la mesure possible pour combattre et prévenir l'utilisation des technologies de l'information et des communications à des fins criminelles, en observant le principe de réciprocité, en étudiant activement les possibilités d'innovation institutionnelle et en proposant de nouveaux mécanismes pour une coopération internationale plus ciblée :

a) La lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles doit passer par la collecte transfrontière de preuves électroniques, mais les États Membres devraient respecter la souveraineté de l'État où se trouvent les éléments de preuve. Les États Membres devraient également garantir le droit à une procédure régulière, respecter les droits légitimes des personnes et des entités et se garder d'employer des moyens techniques d'enquête intrusifs ou destructeurs dans le cadre de cette collecte. Ils ne devraient pas recueillir directement les données hébergées par des entreprises ou des particuliers dans des États étrangers ni recourir à des moyens techniques qui contournent les mesures de protection des réseaux si ces moyens contreviennent aux lois des États en question. Ils devraient envisager de nouveaux dispositifs institutionnels aux fins de la collecte de preuves électroniques auprès d'autres États, tels que l'authentification des preuves électroniques et la collecte d'éléments de preuve vidéo (ou audio) reposant sur la confiance mutuelle. Il faudrait, dans le cadre de ces dispositifs, fournir des orientations uniformes faisant autorité sur la collecte transfrontière de preuves électroniques, tout en conciliant les différents objectifs que sont le respect de la souveraineté nationale et la lutte contre la criminalité ;

b) Les États Membres devraient concevoir des mécanismes de coopération rapide entre les services de détection et de répression. Ils pourraient désigner des organismes chargés d'assurer la liaison, permettant ainsi le partage rapide d'indices, la fourniture de conseils techniques et d'autres formes de coopération en matière de détection et de répression en cas de besoins particuliers ;

c) Pour accroître l'efficacité de l'entraide judiciaire en matière pénale, les États Membres pourraient mettre en place un mécanisme d'échange rapide entre les autorités compétentes afin d'assurer une communication en temps réel en cas de besoin. Le transfert de documents juridiques et de preuves électroniques dans le cadre de la collecte transfrontière d'éléments de preuve pourrait se faire en ligne par des moyens techniques (tels que les signatures électroniques) s'inscrivant dans des systèmes nationaux de gestion de la sécurité en matière de transmission transfrontière des données. Des modalités d'entraide judiciaire en cas d'urgence pourraient également être prévues, notamment la conservation rapide des preuves électroniques ou la communication rapide des données conservées ;

d) Les législations nationales devant faire obligation au secteur privé, notamment aux fournisseurs de services de réseau, de coopérer avec les services de détection et de répression pour ce qui est de surveiller, détecter et combattre les activités criminelles, les États Membres, en particulier ceux qui disposent de ressources avancées en réseaux, devraient encore renforcer la coopération internationale. Si les installations, les systèmes ou les réseaux informatiques appartenant à un fournisseur de services de réseau d'un État A sont utilisés par un suspect dans un autre État pour commettre une infraction, dès lors que l'État A incrimine lui aussi l'acte en question, il devrait, de sa propre initiative ou à la demande de l'autre État, exiger du fournisseur qu'il emploie les mesures techniques et autres nécessaires pour apporter une réponse efficace à l'activité criminelle ;

e) Il conviendrait de renforcer les mesures permettant d'empêcher et de bloquer le transfert international du produit du crime et d'améliorer la coopération internationale en matière de recouvrement d'avoirs. Les États Membres devraient respecter le principe d'un recouvrement rapide et efficace des avoirs et ne devraient pas fixer de conditions préalables à ce recouvrement, hormis les procédures judiciaires.

5. Assistance technique et échange d'informations

Il est essentiel de fournir une assistance technique aux pays en développement et de renforcer l'échange d'informations avec eux afin de combattre et de prévenir efficacement l'utilisation des technologies de l'information et des communications à des fins criminelles :

a) L'assistance technique fournie aux pays en développement devrait notamment consister à :

i) Former le personnel des services de détection et de répression et le personnel judiciaire ;

ii) Former des équipes professionnelles dotées de compétences tant juridiques que techniques ;

iii) Renforcer les capacités dans le domaine de la collecte de preuves électroniques ;

iv) Fournir aux pays en développement le matériel et les technologies dont ils ont besoin pour renforcer leur capacité de lutte contre la criminalité ;

v) Inciter les organisations internationales telles que l'Office des Nations Unies contre la drogue et le crime, le secteur privé, les spécialistes et les universitaires à participer aux activités d'assistance technique et de renforcement des capacités ;

b) Les États Membres devraient être encouragés à faire part de leurs expériences en matière d'élaboration et d'application des lois et des politiques, et à échanger des données relatives à la lutte contre la criminalité et à sa prévention, ainsi qu'à ses tendances.

6. Mécanisme d'application

Afin de promouvoir l'application de la convention, une conférence des États parties et des groupes d'experts ou de travail appropriés, tels qu'un groupe de travail sur l'assistance technique et un groupe de travail sur la coopération internationale, devraient être institués. Les réunions de ces groupes pourraient également offrir aux États parties un cadre pour échanger des données d'expérience et promouvoir la coopération.

7. Dispositions finales

Aucun commentaire à ce stade.

Colombie

[Original : espagnol]
[5 novembre 2021]

Compte tenu de l'adoption de la résolution 74/247 de l'Assemblée générale, qui a porté création d'un comité intergouvernemental spécial d'experts à composition non limitée chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, et en réponse à l'invitation de la Présidente du Comité spécial, dans laquelle elle a engagé les États Membres à présenter leurs vues sur le champ

d'application, les objectifs et la structure que devrait revêtir la future convention sur la cybercriminalité, la Colombie souhaite soumettre les observations préliminaires suivantes.

Champ d'application

La nouvelle convention devrait s'attacher avant tout à offrir un outil de coopération juridique internationale permettant aux autorités nationales de prévenir les actes de cybercriminalité, d'enquêter sur eux et d'en poursuivre et sanctionner les auteurs. Elle devrait également traiter des questions relatives aux preuves électroniques. Par conséquent, il convient d'éviter les débats qui ne portent pas sur le problème juridique de la cybercriminalité ou sur la gestion des preuves électroniques.

Il convient aussi d'éviter de débattre de questions susceptibles d'être sensibles sur le plan politique ou qui n'ont pas directement trait au thème central de la convention.

Il est jugé essentiel que la nouvelle convention tienne compte des cadres et instruments juridiques internationaux existants, parmi lesquels figurent la Convention des Nations Unies contre la criminalité transnationale organisée, la Convention des Nations Unies contre la corruption et la Convention de Budapest sur la cybercriminalité, étant donné que la législation et les pratiques internes de la plupart des États sont alignées ou reposent sur les accords existants. Les futures normes doivent donc être compatibles avec eux. En outre, il convient de s'assurer que les nouvelles règles ne seront pas incompatibles, ni n'entreront en conflit avec d'autres obligations internationales contractées par les États.

À cet égard, la convention devrait adopter une approche complémentaire. En d'autres termes, les négociations devraient, en principe, tenir compte des travaux que la communauté internationale mène déjà depuis plusieurs années en matière de lutte contre la cybercriminalité et ne pas être incompatibles avec les obligations internationales contractées par les États dans ce domaine. Il convient donc de tirer parti du potentiel qu'offre la Convention des Nations Unies contre la criminalité transnationale organisée et des progrès qu'elle a permis de réaliser aux fins de l'élaboration de principes et d'outils en matière de coopération judiciaire.

Il devrait être tenu compte des cadres multilatéraux, régionaux et bilatéraux qui existent actuellement en matière d'entraide judiciaire, afin d'éviter tout risque de conflit normatif, de compléter et d'appliquer les instruments internationaux existants et de ne pas entraver leur mise en œuvre effective. Il est donc recommandé d'accorder une attention pleine et entière non seulement aux instruments multilatéraux existants, tels que la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention sur la cybercriminalité, mais aussi aux accords bilatéraux et régionaux, tels que la Convention interaméricaine sur l'entraide en matière pénale.

Il convient plus précisément de tenir compte de la Convention sur la cybercriminalité (Budapest, 2001), car elle traite de notions qui ont fait l'objet de discussions approfondies et compte à son actif 20 années de mise en application pratique à l'échelle internationale. S'en écarter reviendrait à courir le risque de s'engager sur une voie qui saperait les progrès accomplis jusqu'à présent dans la lutte contre la cybercriminalité.

Il conviendrait également de prendre en considération les résultats des travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, dans le cadre de l'Organisation des Nations Unies, et de s'appuyer sur la liste des conclusions et recommandations préliminaires formulées par les États Membres lors des réunions de ce Groupe d'experts.

Il importe que le processus d'élaboration de la nouvelle convention soit inclusif, transparent et, dans la mesure du possible, basé sur le consensus, comme l'ont été par le passé les travaux réalisés par les Nations Unies pour parvenir à l'adoption de la Convention contre la criminalité transnationale organisée et de la Convention contre la corruption, afin de prévenir l'apparition ultérieure de différends en la matière.

Objectif

La convention devrait avoir pour objectif général de déboucher sur l'adoption d'un cadre de coopération judiciaire internationale qui permette pleinement de prévenir l'utilisation des technologies de l'information et des communications à des fins criminelles et la cybercriminalité, ainsi que de mener des enquêtes et des poursuites dans ce domaine, et qui traite des questions relatives aux preuves électroniques.

Structure

- Définitions et termes techniques de base, qui seront uniformisés et qui resteront valables dans le temps.
- Règles matérielles (actes qui devront être incriminés dans les législations nationales).

À cet égard, la convention devrait incriminer divers actes qui portent atteinte aux systèmes et données informatiques.

Il semble raisonnable, tant sur le principe que d'un point de vue méthodologique, de se concentrer sur les infractions « essentielles » en matière de cybercriminalité, à savoir : l'accès numérique non autorisé à des réseaux ou systèmes informatiques, moyennant l'accès illicite à un système informatique ; l'espionnage informatique, qui recouvre tous les actes portant atteinte à la vie privée des personnes physiques ou morales au moyen de l'interception ou de l'obtention de données, de communications, de fichiers ou de bases de données stockés dans des systèmes informatiques ou transmis par l'intermédiaire des réseaux de communication et qui englobe les actes consistant à intercepter des données informatiques, à violer des données à caractère personnel et à usurper des sites Web en vue de dérober des données à caractère personnel ; et le sabotage informatique, qui vise à paralyser, endommager, rendre inutilisables, détruire ou perturber des systèmes informatiques, des bases de données ou des processus de traitement, de transfert et de transmission de données et qui englobe les actes visant à paralyser illégalement un système informatique ou un réseau de télécommunications.

En outre, l'instrument pourrait viser certains actes qui, parce qu'ils sont commis à l'aide de moyens informatiques, ont des répercussions à la fois étendues et graves et compliquent le travail d'enquête. Il serait ainsi suffisamment souple pour permettre de lutter contre les activités illégales liées à d'autres infractions :

- Principe de la double incrimination : ce mécanisme est important en ce qu'il facilite l'entraide judiciaire, que l'acte visé soit, ou non, passible de sanctions en vertu du droit de l'État requis, ce qui permet notamment d'éviter que les cybercriminels ne trouvent refuge dans certains pays en raison de l'absence de législation commune uniformisée ;
- Dispositions procédurales pour une coopération juridique efficace : il est impératif de renforcer la coopération internationale pour la conduite d'enquêtes sur les affaires de cybercriminalité, notamment en ce qui concerne la gestion des preuves numériques, la chaîne de conservation des preuves, la conservation des données et l'analyse criminalistique. Il est urgent de s'intéresser à la question de la transmission et du stockage des données, ainsi qu'à la conception de mécanismes qui permettent aux autorités de différents États de communiquer entre elles et de se répondre rapidement en utilisant des canaux numériques adaptés et sécurisés ;
- Circonstances aggravantes applicables aux actes qui portent atteinte au droit à la protection des informations et des données, notamment les actes consistant à dérober des données à caractère personnel à grande échelle, les violations des droits humains ou les actes ciblant les infrastructures critiques et les services essentiels ;

- Coopération judiciaire internationale : faciliter, élargir et accélérer l'entraide judiciaire, grâce à l'utilisation de moyens numériques, assortis des mesures de sécurité voulues et utilisant des formats standards ;
- Concevoir des mécanismes d'enquête spécialisés dans la collecte de preuves numériques, notamment lorsque les preuves sont conservées dans différents pays ;
- Il importe que les États Membres conviennent de mécanismes qui assurent aux données à caractère personnel un niveau de protection adéquat dans le cadre des échanges d'informations réalisés conformément à l'instrument international, non seulement du fait que la protection des données à caractère personnel a gagné en importance dans le contexte numérique, mais aussi pour éviter que les règles propres à chaque pays ne fassent éventuellement obstacle à l'échange d'informations entre États ;
- Promotion de l'assistance technique, de la diffusion de connaissances et de l'échange de bonnes pratiques en matière d'enquêtes, de poursuites et de sanctions. En outre, afin de réduire la fracture numérique, il est essentiel de prévoir le renforcement des capacités des services de détection et de répression et des autres autorités judiciaires nationales, notamment grâce à des programmes d'éducation et de formation comme autant d'outils de prévention ;
- Promouvoir la coopération technique à l'aide d'établissements régionaux de formation. Compte tenu de la complexité et de la particularité des enquêtes sur les infractions commises à l'aide de moyens informatiques, lesquels entravent d'ailleurs l'efficacité de ces enquêtes, il convient de proposer des formations spécialisées aux procureurs et aux enquêteurs de manière organisée et continue, en établissant préalablement des plans de travail qui définissent les résultats escomptés ;
- La promotion d'une coopération solide et fondée sur la confiance entre le secteur public et le secteur privé dans le domaine de la cybercriminalité est primordiale. Aussi est-il essentiel de parvenir à une position coordonnée sur la question et de faciliter la collecte de preuves numériques par les acteurs du domaine numérique, notamment les fournisseurs d'accès à Internet et les entreprises de communication ;
- Promouvoir et faciliter l'accès des autorités aux plateformes de collaboration aux fins du renforcement des capacités et de l'échange d'informations, ainsi qu'aux outils d'analyse et d'étude de contexte pour les enquêtes en la matière ;
- Prévoir des dispositions qui facilitent un accès rapide aux informations voulues en cas d'urgence ;
- Enfin, il est proposé de prévoir la création d'un réseau de points de contact accessibles 24 heures sur 24 et 7 jours sur 7 et chargés de traiter les demandes de coopération juridique internationale en matière de cybercriminalité. En outre, ce réseau pourrait être complété par un réseau de points de contact chargés des tâches suivantes : a) promouvoir la mise en commun des connaissances et des données d'expérience relatives à la cybercriminalité et aux infractions connexes ; b) définir des bonnes pratiques et les diffuser ; et c) optimiser et faciliter la coopération judiciaire internationale entre les pays.

Égypte

[Original : arabe]
[28 octobre 2021]

Désirant apporter une contribution utile aux efforts internationaux visant à établir, sous la houlette de l'Organisation des Nations Unies, une convention générale sur la lutte contre l'utilisation des technologies de l'information et des

communications à des fins criminelles, et respectant les engagements qu'elle a contractés en vertu des conventions et traités nationaux, régionaux et internationaux relatifs aux droits humains et à la lutte contre la criminalité transnationale, la République arabe d'Égypte a rédigé la présente proposition contenant des éléments qui pourraient être inclus dans le texte de la convention. Ce faisant, elle espère que les objectifs visés seront atteints par le renforcement de la coopération internationale et la formulation d'une politique commune de lutte contre la criminalité qui permette de combattre toutes les infractions liées aux technologies de l'information et des communications, de sorte à prévenir les risques que font peser ces infractions sur la sécurité et les intérêts des États et sur la sécurité des populations et des citoyennes et citoyens.

I. Objectifs

La convention devrait viser à renforcer la coopération entre les États Membres de l'Organisation des Nations Unies dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, afin de prévenir la commission de tout acte susceptible de porter atteinte à l'intégrité et à la confidentialité de ces technologies, de sanctionner leur utilisation à des fins illégales, ainsi que de faciliter la conduite d'enquêtes et l'engagement de poursuites contre celles et ceux qui s'en rendent coupables. Elle devrait également protéger des effets qui découlent des infractions liées à ces technologies, notamment en prévoyant la suspension des transactions qui portent sur le produit de l'un quelconque des actes illégaux visés dans ses dispositions, ainsi que la confiscation et la restitution d'un tel produit. Pour ce faire, elle devrait définir les pouvoirs nécessaires pour combattre efficacement les infractions liées aux technologies de l'information et des communications et, à cette fin, prévoir la mise en place d'accords de coopération internationale propices à la détection de ces infractions, à la conduite d'enquêtes en la matière et à l'engagement de poursuites et de procédures d'extradition contre leurs auteurs.

II. Champ d'application

1. Sauf disposition contraire, la convention devrait viser la prévention des infractions mentionnées dans son texte.

2. Chaque État partie devrait prendre toutes les mesures nécessaires pour établir sa compétence à l'égard des infractions pénales et des autres actes illicites définis dans la convention, lorsque l'infraction est :

a) Commise sur son territoire ; ou

b) Commise à bord d'un navire battant son pavillon ou à bord d'un aéronef immatriculé conformément à son droit interne au moment où ladite infraction est commise ; ou

c) De nature transnationale et qu'un groupe criminel organisé est impliqué dans sa commission. Toute infraction devrait être considérée comme étant de nature transnationale lorsqu'elle est commise : i) dans plus d'un pays ; ii) dans un seul pays, mais qu'elle est préparée, planifiée, dirigée ou supervisée dans un autre pays ; iii) dans un seul pays par un groupe criminel organisé qui a des activités criminelles dans plus d'un pays ; ou iv) dans un seul pays, mais qu'elle a de lourdes répercussions dans un autre pays.

3. Aux fins de l'application de la convention, il ne devrait pas être nécessaire que les infractions ou autres actes illégaux qui y sont visés causent un dommage matériel, sauf disposition contraire.

4. Les États parties devraient envisager de limiter les réserves qu'ils émettent, de sorte à permettre une large application des mesures susmentionnées.

III. Protection de la souveraineté

1. Chaque État partie devrait exécuter, conformément à sa législation interne et à ses principes constitutionnels, les obligations qui lui incombent au titre de la convention d'une manière compatible avec le principe de l'égalité souveraine des États et avec celui de la non-ingérence dans les affaires intérieures d'autres États.

2. La convention ne devrait pas autoriser les autorités compétentes d'un État partie à exercer sur le territoire d'un autre État partie une compétence et des fonctions qui sont exclusivement réservées aux autorités de cet autre État par son droit interne.

IV. Infractions qui pourraient être couvertes par la Convention

1. Chaque État partie devrait adopter les mesures législatives et autres nécessaires pour empêcher la commission des infractions visées par la convention ou de toute autre infraction liée aux technologies de l'information et des communications, notamment en prévoyant de bloquer et de supprimer les contenus ayant un lien avec ces infractions, de détecter les infractions, d'en poursuivre les auteurs, d'extrader les criminels et de faciliter les procédures applicables en matière de coopération internationale et de collecte d'éléments de preuve.

2. Chaque État partie devrait également adopter les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale aux actes suivants :

Article premier. L'utilisation illégale des services et technologies de l'information et des communications, y compris le fait de tirer un avantage illicite de services de télécommunications ou de canaux audio ou vidéo dont la transmission est assurée au moyen de réseaux informatiques ou d'un dispositif électronique, ou d'aider un tiers à obtenir un tel avantage.

Article 2. Tout accès illégal et/ou dépassant les limites du droit d'accès, notamment :

1. Le fait d'utiliser un privilège octroyé pour accéder à un site Web, à un compte privé ou à un système informatique d'une manière qui dépasse les limites dudit privilège, qu'il s'agisse de la durée de consultation ou du niveau d'accès.

2. Le fait d'accéder illégalement à la totalité ou à une partie d'un système informatique ou de communiquer illégalement avec la totalité ou une partie d'un tel système, et de prolonger un tel accès ou une telle communication.

3. Une telle infraction devrait être punie plus sévèrement lorsque l'accès ou la communication conduit à :

a) L'effacement, la modification, l'altération, la copie, le transfert ou la destruction de données sauvegardées, d'appareils et de systèmes électroniques ou de réseaux de communication, ou des dommages causés aux utilisateurs et aux bénéficiaires ;

b) La consultation d'informations confidentielles provenant de sources officielles.

Article 3. Le fait de porter atteinte à la conception d'un site Web en endommageant, en perturbant, en ralentissant, en altérant, en dissimulant ou en modifiant de façon illégale le site Web d'une entreprise, d'une institution, d'une installation ou d'une personne physique.

Article 4. L'interception délibérée et illégale d'un flux de données en recourant à un moyen technique quel qu'il soit ou en empêchant la transmission ou la réception de données informatiques.

Article 5. Le fait de porter atteinte à l'intégrité des données en détruisant, en effaçant, en entravant, en modifiant ou en bloquant des données informatiques de manière intentionnelle et illégale.

Article 6. L'utilisation abusive des technologies de l'information par la production, la vente, l'achat, l'importation, la distribution, la fourniture ou la détention d'outils ou de logiciels conçus ou adaptés à cette fin, de mots de passe ou d'informations analogues permettant d'accéder à un système informatique, dans l'intention de l'utiliser pour commettre l'une des infractions visées par la convention, ou la création de logiciels malveillants destinés à détruire, bloquer, modifier, copier ou diffuser des données numériques, ou à neutraliser les dispositifs de sécurité connexes, sauf dans le cadre de perquisitions légales.

Article 7. La falsification de données à l'aide des technologies de l'information en vue de les altérer d'une manière qui causerait un préjudice et dans l'intention de présenter les données ainsi altérées comme des informations valides.

Article 8. La fraude consistant à causer, de manière intentionnelle et illégale, un préjudice aux bénéficiaires et aux utilisateurs de sorte à procurer illégalement un intérêt ou un bénéfice à l'auteur de l'infraction ou à un tiers, y compris au moyen d'infractions électroniques liées aux monnaies virtuelles (numériques ou cryptées).

Article 9. Le recours à la menace ou à l'extorsion à l'aide des technologies de l'information et des communications ou de tout autre moyen technologique pour pousser autrui, par l'intimidation ou le chantage, à commettre un acte ou à s'en abstenir.

Article 10. La pornographie lorsque :

1. Les technologies de l'information et des communications sont utilisées pour produire, présenter, distribuer, fournir, publier, acheter, vendre ou importer des contenus pornographiques à des fins obscènes.

2. Les technologies de l'information et des communications sont utilisées pour produire, présenter, distribuer, fournir, publier, acheter, vendre ou importer des contenus pornographiques mettant en scène des enfants ou des mineurs, y compris la détention, grâce à ces technologies ou à quelque support de stockage informatique que ce soit, de ce type de contenu ou de tout contenu mettant en scène des enfants ou des mineurs dans des situations indécentes.

Article 11. Les autres infractions liées à la pornographie, dont l'exploitation ou le harcèlement sexuels, en particulier celles qui touchent les femmes, les enfants ou les mineurs.

Article 12. Le fait d'inciter ou de contraindre autrui, y compris une personne mineure, à se suicider, en exerçant des pressions psychologiques ou autres par l'intermédiaire des réseaux d'information et de communication, dont Internet, que ce soit au moyen d'interactions directes ou de technologies ou jeux électroniques prisés du public.

Article 13. L'utilisation des technologies de l'information et des communications pour impliquer des personnes mineures dans la commission d'actes illégaux qui mettent leur vie ou leur santé physique ou mentale en danger.

Article 14. L'utilisation des technologies de l'information et des communications pour porter atteinte à la vie privée d'autrui, y compris en créant une adresse électronique, un site Web ou un compte privé et en l'attribuant de manière trompeuse à une personne physique ou morale.

Article 15. L'utilisation des technologies de l'information pour commettre des infractions liées au terrorisme, notamment :

1. La diffusion des idées et des principes nourris par des groupes terroristes ou la justification du terrorisme.

2. Le financement d'opérations terroristes ou l'entraînement à de telles opérations, la facilitation de la communication entre les organisations terroristes ou la fourniture d'un appui logistique aux personnes qui mènent des opérations terroristes.

3. La diffusion d'informations relatives aux méthodes de fabrication d'explosifs, notamment aux fins de leur utilisation dans le cadre d'opérations terroristes.

4. L'incitation au fanatisme, à la sédition, à la haine ou au racisme.

5. Les États parties devraient prendre les mesures voulues pour interdire la diffusion de tels contenus à l'aide des technologies de l'information et des communications, notamment en bloquant et en supprimant les contenus ayant un lien avec les infractions susmentionnées.

Article 16. Les infractions financières, telles que le blanchiment d'argent, et notamment :

1. L'utilisation des technologies de l'information et des communications pour commettre des infractions financières ou l'utilisation abusive de monnaies virtuelles (numériques ou cryptées).

2. La conduite d'opérations de blanchiment d'argent, ainsi que la demande d'aide ou la diffusion de méthodes à cette fin.

Article 17. L'utilisation illicite d'instruments de paiement électronique, notamment :

1. Le fait de confectionner, de fabriquer ou de créer, par quelque moyen que ce soit, tout dispositif ou matériel facilitant la contrefaçon ou l'imitation de tout instrument de paiement électronique.

2. Le fait de se procurer les données relatives à un instrument de paiement, d'utiliser ces données, de les transmettre à un tiers ou de faciliter leur obtention pour le compte d'un tiers.

3. L'utilisation d'un réseau informatique ou d'une technologie de l'information pour obtenir, sans autorisation, accès au code ou aux données se rapportant à un instrument de paiement.

4. Le fait d'accepter sciemment un instrument de paiement contrefait.

Article 18. Les infractions liées à la criminalité organisée ou à la criminalité transnationale commises au moyen des technologies de l'information, notamment :

1. La commercialisation ou le trafic de stupéfiants ou de substances psychotropes.

2. La distribution illicite de médicaments ou produits médicaux contrefaits.

3. Le trafic illicite de personnes migrantes.

4. La traite des personnes.

5. Le trafic d'organes humains.

6. Le commerce illicite d'armes.

7. Le trafic de biens culturels.

Article 19. Les infractions liées à la violation des droits d'auteur et des droits voisins, notamment tels qu'ils sont définis dans la législation de l'État partie, si l'acte est commis intentionnellement.

Article 20. L'accès non autorisé aux infrastructures d'information critiques, notamment :

1. La création, la distribution ou l'utilisation de logiciels ou d'autres matériels numériques conçus pour permettre un accès non autorisé à une infrastructure d'information critique, notamment en vue de détruire, de bloquer, de modifier ou de copier les données qu'elle renferme ou de neutraliser ses dispositifs de sécurité.

2. La violation des règles d'exploitation applicables tant aux supports destinés au stockage, au traitement ou au transfert de données numériques protégées dans des infrastructures d'information ou systèmes informatiques critiques, ou d'informations protégées en vertu de la législation interne de l'État partie, qu'aux réseaux de communication qui font partie des infrastructures d'information critiques, ou la violation des règles d'accès à ces supports et réseaux, dès lors qu'une telle violation porte atteinte aux infrastructures d'information critiques.

Article 21. L'incitation à la commission d'actes subversifs, d'opérations armées ou d'autres infractions pénales, y compris les appels lancés au moyen des technologies de l'information et des communications en faveur d'actes subversifs ou d'opérations armées ciblant les autorités d'un autre État et susceptibles de porter atteinte à la sécurité et à la stabilité publiques, ou l'incitation à la commission d'infractions pénales passibles d'une peine d'emprisonnement d'au moins un an.

Article 22. Les infractions liées à l'extrémisme, notamment la distribution de matériels de nature à encourager ou à justifier la commission d'actes illégaux pour des motifs politiques, idéologiques, sociaux ou ethniques ou à inciter à la haine ou à l'hostilité ethnique ou religieuse en général, ou la fourniture d'un accès à de tels matériels.

Article 23. La tentative de commission de toute infraction visée par la convention, y compris le fait de s'en rendre complice et/ou le fait de l'organiser ou de donner des instructions à d'autres personnes pour qu'elles la commettent.

Article 24. Tous autres actes illégaux.

La convention ne devrait pas empêcher un État partie d'ériger en infraction tout autre acte illégal commis intentionnellement à l'aide des technologies de l'information et des communications et causant des dommages importants.

V. Responsabilité juridique, procédures pénales, détection et répression, et entraide judiciaire internationale

Article premier. Responsabilité des personnes morales

Sous réserve des dispositions de sa législation interne, chaque État partie devrait prévoir la responsabilité pénale des personnes morales en cas d'infraction commise par ses représentants en son nom ou pour son compte, sans préjudice des sanctions applicables aux personnes physiques (gestionnaire de site, par exemple) ayant commis l'infraction.

Article 2. Responsabilité des fournisseurs de services/gestionnaires de sites

Sans préjudice des dispositions de la convention, les fournisseurs de services/gestionnaires de sites et leurs subordonnés devraient être tenus aux obligations énoncées ci-après, et tout manquement devrait être érigé en infraction :

1. Sauvegarder et conserver le journal du système informatique ou le journal de tout outil informatique pour une durée à déterminer. Les données qu'il convient de préserver et de stocker devraient inclure :

a) Les données permettant d'identifier l'utilisateur du service ;

b) Les données relatives au contenu du système informatique du client dès lors qu'il est contrôlé par le fournisseur de services ;

c) Les données relatives au flux de communication ;

d) Les données relatives aux périphériques de communication ;

e) Toute autre donnée spécifiée par l'État aux fins de la mise en œuvre de la convention.

2. Garder confidentielles les données qui ont été sauvegardées et stockées, y compris les données à caractère personnel des utilisateurs des services, les données ou informations relatives aux sites ou aux comptes privés auxquels ces utilisateurs, ou les personnes ou entités avec lesquelles ils communiquent, ont accès, et ne les divulguer qu'à condition d'avoir reçu une instruction motivée en ce sens de la part d'une autorité compétente.

3. Sécuriser les données et informations de manière à les garder confidentielles et à les protéger contre toute violation et tout dommage.

4. Le fournisseur de services/gestionnaire de site devrait être tenu de communiquer aux utilisateurs et à toute autorité compétente les données et informations énoncées ci-après, sous une forme et d'une manière qui permettent d'y accéder facilement, directement et sans interruption :

a) Le nom et l'adresse du fournisseur de services ;

b) Les coordonnées du fournisseur de services, dont son adresse électronique ;

c) Les données relatives à l'autorisation d'activité qui permettent d'identifier le fournisseur de services et l'autorité compétente responsable de sa supervision.

5. Le fournisseur de services/gestionnaire de site devrait être tenu de mettre à la disposition des autorités compétentes désignées par l'État, lorsqu'elles le demandent, tous les moyens techniques voulus pour qu'elles puissent exercer leurs fonctions.

Article 3. Procédures pénales

1. Chaque État partie devrait prendre les mesures législatives et autres voulues afin d'établir les compétences et les procédures nécessaires pour prévenir toute infraction ou tout acte illégal, les identifier, les détecter, enquêter à leur sujet et engager des actions en justice.

2. Chaque État partie devrait établir les compétences et procédures susmentionnées à l'égard :

a) Des actes criminels et autres actes illégaux visés dans la convention ;

b) Des autres infractions pénales ou autres actes illégaux commis à l'aide des technologies de l'information et des communications ;

c) De la collecte électronique d'éléments de preuve relatifs aux infractions.

3. Les procédures pénales devraient prévoir :

a) La conservation rapide des données, y compris de celles relatives au trafic qui sont stockées à l'aide des technologies de l'information, en particulier lorsqu'on estime que ces données sont susceptibles d'être perdues ou modifiées, ordre étant donné à la personne concernée de protéger l'intégrité des informations en sa possession ou sous son contrôle pour permettre aux autorités compétentes de mener les perquisitions et les enquêtes voulues, en gardant secrète toute mesure prise à cet égard ;

b) La conservation rapide et la divulgation partielle des données relatives au trafic, que la transmission d'informations ait été assurée par un fournisseur de services ou par plusieurs, de telle sorte que les autorités compétentes divulguent rapidement une quantité de données suffisante pour permettre à l'État partie d'identifier le fournisseur de services et la voie par laquelle la transmission s'est faite ;

c) L'ordre de remettre des informations détenues par une personne se trouvant sur le territoire de l'État partie et stockées dans un système informatique ou sur un support de stockage, ou détenues par un fournisseur de services qui opère sur le territoire ou sous le contrôle de l'État partie ;

d) L'inspection des informations stockées dans un système informatique ou sur un support de stockage, ou l'accès à ces informations ;

e) La prise de contrôle, la copie et la conservation des informations stockées dans le cadre de procédures de perquisition ou d'accès à l'information ;

f) La collecte en temps réel de données relatives au trafic et l'obligation pour le fournisseur de services soumis à la juridiction de l'État de recueillir des informations, de les enregistrer et de les garder confidentielles ;

g) L'interception du contenu des communications de sorte à permettre aux autorités compétentes de recueillir et d'enregistrer en temps réel, à l'aide de moyens techniques, les informations transmises par l'intermédiaire des technologies de l'information et des communications ;

h) Chaque État partie devrait adopter les mesures législatives et autres nécessaires pour permettre à ses autorités compétentes d'empêcher la transmission ou la diffusion de tout contenu contraire aux dispositions de la convention.

4. Admissibilité des preuves numériques :

Les preuves numériques issues ou extraites de dispositifs, d'équipements, de supports électroniques, de systèmes ou programmes informatiques ou de toute autre technologie de l'information et des communications devraient avoir la même valeur et la même force probante que les preuves matérielles scientifiques dès lors qu'elles remplissent les conditions techniques imposées par la législation des États parties.

Article 4. Coopération juridique et judiciaire internationale

1. Les États parties devraient faciliter la coopération entre eux, conformément aux dispositions de la convention ou en application du principe de réciprocité, pour mettre en commun des informations en vue de prévenir la commission d'infractions liées aux technologies de l'information, de contribuer aux enquêtes sur ces infractions et d'en localiser les auteurs.

2. Les États Parties devraient coopérer dans toute la mesure possible conformément aux dispositions du présent article, aux dispositions des autres instruments internationaux relatifs à la coopération internationale en matière pénale, au principe de réciprocité et aux dispositions de la législation interne applicables en vue de prévenir les infractions liées aux technologies de l'information et des communications, de les réprimer et d'en identifier et poursuivre les auteurs.

3. Aux fins de l'extradition et de l'entraide judiciaire en matière pénale, aucune infraction visée par la convention ne devrait être considérée comme une infraction politique. En conséquence, une demande d'extradition ou d'entraide judiciaire en matière pénale qui porte sur une telle infraction ne peut être rejetée au motif qu'elle porte sur une infraction politique ou apparentée ou une infraction inspirée par des mobiles politiques.

5. Compétence :

Chaque État est tenu d'adopter les mesures nécessaires pour étendre sa compétence aux infractions susmentionnées, si :

a) L'infraction est commise en totalité ou en partie sur le territoire de l'État partie ;

b) L'infraction est commise en totalité ou en partie à bord d'un navire battant le pavillon de l'État partie ;

c) L'infraction est commise en totalité ou en partie à bord d'un aéronef immatriculé conformément au droit interne de l'État partie ;

d) L'infraction est commise en totalité ou en partie par un ressortissant d'un État partie et elle est passible de sanctions en vertu de la législation nationale applicable là où elle a été commise, ou elle a été commise en un lieu ne relevant de la juridiction d'aucun État ;

e) L'infraction porte atteinte aux intérêts supérieurs de l'État.

6. Extradition :

a) Les auteurs des infractions susmentionnées devaient pouvoir être extradés d'un État partie vers un autre dès lors que les infractions sont passibles de sanctions en vertu de la législation des États parties concernés. Lorsque sa législation le lui permet, un État partie peut donner suite à une demande d'extradition portant sur une infraction qui est visée par la convention mais qui n'est pas passible de sanctions en vertu de sa législation interne ;

b) Les infractions susmentionnées devraient pouvoir donner lieu à extradition en application des traités d'extradition conclus entre les États parties ;

c) Si un État partie qui subordonne l'extradition à l'existence d'un traité reçoit une demande d'extradition d'un État partie avec lequel il n'a pas conclu pareil traité, il peut considérer la convention comme la base légale de l'extradition ;

d) L'extradition devrait être subordonnée aux conditions prévues par la législation de l'État partie requis ou par les traités d'extradition applicables, notamment aux conditions concernant les motifs pour lesquels l'État partie peut refuser l'extradition ;

e) Tout État partie peut refuser d'extrader ses ressortissants, auquel cas il devrait, dans les limites de sa compétence, poursuivre ceux de ses ressortissants qui ont commis, dans tout autre État partie, une infraction passible d'une peine de privation de liberté en vertu de la législation des deux États parties, dès lors que l'autre État partie lui adresse une demande en ce sens, accompagnée des dossiers, documents, renseignements et éléments de preuve en sa possession. L'État partie requérant devrait être informé de la suite donnée à sa demande, et la question de savoir quelle était la nationalité de l'auteur au moment de la commission de l'infraction pour laquelle l'extradition est demandée devrait être tranchée ;

f) Les États parties devraient s'efforcer, sous réserve de leur législation interne, d'accélérer les procédures d'extradition et de simplifier les exigences en matière de preuve y relatives en ce qui concerne les infractions auxquelles s'applique le présent article ;

g) Sous réserve de sa législation interne et des traités d'extradition qu'il a conclus, l'État partie requis peut, à la demande de l'État partie requérant et s'il estime que les circonstances le justifient et qu'il y a urgence, placer en détention une personne présente sur son territoire dont

l'extradition est demandée ou prendre à son égard d'autres mesures appropriées pour assurer sa présence lors de la procédure d'extradition ;

h) Si l'extradition demandée aux fins d'exécution d'une décision de justice est refusée parce que la personne faisant l'objet de cette demande est un ressortissant de l'État partie requis, celui-ci devrait, si sa législation interne le lui permet, en conformité avec les dispositions applicables et à la demande de l'État partie requérant, envisager de faire exécuter lui-même la peine prononcée conformément à la législation interne de l'État partie requérant, ou le reliquat de cette peine ;

i) Toute personne faisant l'objet de poursuites en raison de l'une quelconque des infractions auxquelles le présent article s'applique devrait se voir garantir un traitement équitable à tous les stades de la procédure, y compris la jouissance de tous les droits et de toutes les garanties prévus par la législation interne de l'État partie sur le territoire duquel elle se trouve ;

j) Aucune disposition de la convention ne devrait être interprétée comme faisant obligation à l'État partie requis d'extrader s'il a de sérieuses raisons de penser que la demande d'extradition a été présentée aux fins de poursuivre ou de punir une personne en raison de son sexe, de sa race, de sa langue, de sa religion ou de sa nationalité, ou que donner suite à cette demande causerait un préjudice à cette personne pour l'une quelconque de ces raisons ;

k) Les États parties ne devraient pas pouvoir refuser une demande d'extradition au seul motif que l'infraction est liée à des questions financières ;

l) Avant de refuser l'extradition, l'État partie requis devrait, s'il y a lieu, consulter l'État partie requérant afin de lui donner toute possibilité de présenter ses vues et de fournir des informations tendant à attester les faits énoncés dans sa demande ;

m) Chaque État partie devrait, au moment du dépôt de son instrument de ratification ou d'adoption, être tenu de notifier à un organisme spécialisé, dont les parties doivent convenir, les coordonnées de l'autorité responsable du traitement des demandes d'extradition ou des procédures d'arrestation et d'actualiser périodiquement les informations communiquées.

7. Entraide :

a) Tous les États parties devraient se prêter l'entraide la plus large possible aux fins de la conduite des enquêtes, des procédures relatives aux infractions liées aux technologies de l'information et des communications ou de la collecte de preuves électroniques ;

b) Les demandes d'assistance bilatérale et les communications y afférentes devraient être soumises par écrit. Tout État partie peut, dans des circonstances impérieuses, présenter une demande urgente, y compris par courrier électronique, à condition que les communications soient raisonnablement sécurisées (par le recours à l'encodage, notamment) et répertoriées et, si l'État partie le demande, que leur bonne transmission soit confirmée ;

c) Sauf disposition contraire de la convention, l'assistance bilatérale devrait être soumise aux conditions fixées dans la législation de la partie requise ou dans les traités d'entraide applicables, y compris en ce qui concerne les motifs pour lesquels la partie requise peut refuser de coopérer ;

d) Lorsque l'État partie auquel la demande d'entraide est adressée ne peut prêter assistance qu'en cas de double incrimination, cette condition est considérée comme satisfaite que la législation de l'État partie requis classe l'infraction visée dans la même catégorie que la législation de l'État partie requérant ou non.

8. Communication spontanée d'informations :

Un État partie peut, conformément à sa législation interne et en l'absence de demande préalable d'un autre État partie, communiquer des informations obtenues dans le cadre de ses propres enquêtes lorsqu'il estime que la communication de ces informations pourrait aider cet autre État partie à engager ou à mener à bien des enquêtes au sujet d'infractions visées par la convention, ou pourrait aboutir à une demande de coopération formulée par cet État partie.

9. Procédures relatives aux demandes de coopération et d'entraide :

a) Les alinéas du présent paragraphe devraient être appliqués en l'absence de traité ou de convention d'entraide ou de coopération conforme à la législation en vigueur entre l'État partie requérant et l'État partie requis. Ils ne devraient pas l'être dans le cas où un tel traité ou une telle convention existe, à moins que les parties concernées ne conviennent qu'ils le soient, en tout ou en partie ;

b) Chaque État partie devrait désigner une autorité centrale chargée de présenter les demandes d'entraide judiciaire, de les recevoir et d'y donner suite, ou de les transmettre à l'autorité compétente. Les coordonnées de l'autorité centrale devraient être mises à jour périodiquement ;

c) Les demandes d'entraide présentées en vertu du présent article devraient être traitées conformément aux procédures indiquées par l'État partie requérant, à condition que ces procédures ne soient pas contraires à la législation de l'État partie requis ;

d) L'État partie requis peut surseoir à l'exécution de la demande si une telle exécution est de nature à entraver des enquêtes judiciaires conduites par ses autorités ;

e) Avant de refuser ou d'ajourner son aide, l'État partie requis devrait examiner, après avoir consulté l'État partie requérant, s'il peut être fait droit à la demande partiellement ou sous réserve des conditions qu'il juge nécessaires ;

f) L'État partie requis devrait informer l'État partie requérant des résultats de l'exécution de la demande. Si l'entraide est refusée ou son exécution pleine et entière ajournée, l'État partie requis devrait être tenu d'informer l'État partie requérant des motifs de ce refus ou de tout ajournement notable ;

g) L'État partie requérant peut demander à l'État partie requis de garder la demande confidentielle dans la mesure où cela ne nuit pas à son exécution. Si l'État partie requis ne peut accéder à cette demande de confidentialité, il devrait en informer l'État partie requérant, qui devra alors déterminer la mesure dans laquelle la demande d'entraide peut être exécutée ;

h) En cas d'urgence, les demandes d'entraide peuvent être adressées directement aux autorités judiciaires de l'État partie requis par leurs homologues de l'État partie requérant. En pareil cas, une copie de la demande doit être envoyée simultanément par l'autorité centrale de l'État partie requérant à son homologue de l'État partie requis ;

i) Les demandes soumises en application de l'alinéa précédent et les communications y afférentes peuvent être présentées par l'intermédiaire de l'Organisation internationale de police criminelle (INTERPOL) ;

10. Refus d'entraide :

a) Un État partie requis peut refuser de donner suite à une demande d'entraide si, outre les motifs susmentionnés, il estime que l'exécution de cette demande pourrait porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à ses intérêts fondamentaux ;

b) Une demande d'entraide judiciaire qui porte sur une infraction visée par la convention ne devrait pas être rejetée au motif qu'elle porte sur une infraction politique ou apparentée.

11. Confidentialité et limites d'utilisation :

En l'absence de traité ou de convention d'entraide conforme à la législation en vigueur entre l'État partie requérant et l'État partie requis, le présent article doit être appliqué. Il ne devrait pas l'être dans le cas où une telle convention ou un tel traité existe, à moins que les États parties concernés ne conviennent qu'il le soit, en tout ou en partie.

12. Conservation rapide des informations stockées dans les systèmes informatiques :

a) Tout État partie peut demander à un autre État partie de conserver rapidement des informations qui sont stockées au moyen des technologies de l'information sur son territoire et au sujet desquelles l'État partie requérant souhaiterait présenter une demande d'entraide afin de perquisitionner, saisir, sécuriser ou divulguer lesdites informations ;

b) Un État partie requis peut refuser de donner suite à une demande de conservation d'informations s'il estime que l'exécution de cette demande pourrait porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à ses intérêts.

13. Lorsque, en exécutant une demande de conservation de données relatives au trafic en lien avec certaines communications, l'État partie requis découvre qu'un fournisseur de services d'un autre État a participé à la transmission de ces informations, il devrait communiquer à l'État partie requérant une quantité de données relatives au trafic telle qu'elle permette d'identifier ledit fournisseur de services et la voie par laquelle ont été transmises les informations dont la conservation est demandée.

14. Coopération et assistance bilatérales en matière d'accès aux données informatiques stockées :

a) Tout État partie peut demander à un autre État partie de perquisitionner, de consulter, de saisir, de sécuriser ou de divulguer des données informatiques stockées et situées sur le territoire de l'État partie requis, y compris des données qui y sont conservées ;

b) L'État partie requis devrait être tenu d'accéder à la demande de l'État partie requérant conformément aux dispositions de la convention ;

c) La demande devrait être exécutée dans les plus brefs délais si les données visées sont susceptibles d'être perdues ou modifiées.

15. Accès transfrontière aux données informatiques :

Tout État partie peut, sans obtenir l'autorisation d'un autre État partie, accéder à des données informatiques accessibles au public (domaine public), quel que soit le lieu géographique où se trouvent ces données.

16. Coopération et assistance bilatérales en matière de collecte en temps réel de données relatives au trafic :

a) Les États parties devraient se prêter une assistance bilatérale en matière de collecte en temps réel de données relatives au trafic qui sont en lien avec certaines communications ayant lieu sur leur territoire et qui sont transmises au moyen des technologies de l'information ;

b) Chaque État partie devrait fournir ce type d'assistance, au moins en rapport avec les infractions pour lesquelles la législation interne prévoit, dans des situations similaires, la collecte en temps réel de données relatives au trafic.

17. Coopération et assistance bilatérales concernant les données relatives au contenu :

Les États parties devraient être tenus de se prêter une assistance bilatérale aux fins de la collecte en temps réel de données relatives au contenu de communications spécifiques transmises au moyen des technologies de l'information, dans la mesure où les traités et la législation interne applicables le permettent.

18. Organisme spécialisé :

a) Chaque État partie devrait mettre en place, conformément aux principes fondamentaux de son système juridique, un organisme spécialisé chargé, 24 heures sur 24 et 7 jours sur 7, de fournir une assistance immédiate à l'appui des enquêtes et des procédures portant sur des infractions liées aux technologies de l'information ou de recueillir des preuves électroniques se rapportant à une infraction donnée. Une telle assistance devrait notamment consister à faciliter ou à assurer :

i) La prestation de conseils techniques ;

ii) La conservation de données, conformément aux dispositions pertinentes ;

iii) La collecte de preuves, l'apport d'informations à caractère juridique et la localisation des suspects ;

b) L'organisme spécialisé d'un État partie devrait pouvoir, en cas d'urgence, communiquer avec les organismes analogues d'autres États parties ;

c) Si l'organisme spécialisé désigné par un État partie n'est pas l'une des autorités chargées de l'assistance bilatérale internationale, il devrait être habilité à coordonner rapidement son action avec celle desdites autorités ;

d) Chaque État partie devrait s'assurer de la disponibilité de ressources humaines qualifiées de sorte à faciliter les travaux de l'organisme spécialisé.

VI. Assistance technique et formation

1. Principes généraux relatifs à l'assistance technique :

a) Les États parties devraient envisager, dans leurs plans et programmes nationaux de lutte contre la criminalité liée aux technologies de l'information et des communications, de s'accorder l'assistance technique la plus large possible, en particulier au profit des pays en développement, y compris un appui matériel et une formation dans les domaines mentionnés dans la convention, de même qu'une formation, une assistance, un transfert de technologies et de connaissances, et la mise en commun de données d'expérience pertinentes et de connaissances spécialisées, ce qui facilitera la coopération internationale entre États parties dans les domaines de l'extradition et de l'entraide judiciaire ;

b) Les États parties devraient renforcer les mesures prises pour optimiser l'efficacité des activités opérationnelles et de formation au sein des organisations internationales et régionales et dans le cadre des accords ou arrangements bilatéraux et multilatéraux pertinents ;

c) Les États parties devraient envisager de s'entraider, sur demande, pour mener des évaluations, des études et des recherches portant sur les types, les causes et les effets de la criminalité liée aux technologies de l'information et des communications sur leur territoire, en vue d'élaborer, avec la participation des autorités compétentes et des principaux acteurs, des stratégies et des plans d'action visant à combattre ce type de criminalité ;

d) Les États parties devraient envisager de créer des mécanismes de financement en vue d'appuyer, au moyen de programmes et de projets d'assistance technique, les efforts déployés par les pays en développement ;

e) Les États parties devraient envisager d'échanger des informations sur les avancées juridiques, politiques ou technologiques réalisées dans le domaine de la cybercriminalité, ainsi qu'en matière de collecte de preuves électroniques.

2. Formation et renforcement des capacités :

a) Chaque État partie devrait élaborer, mettre en œuvre ou améliorer, selon qu'il conviendra, des programmes de formation spécifiques à l'intention du personnel chargé de prévenir et de combattre la criminalité liée aux technologies de l'information et des communications. Ces programmes pourraient porter sur ce qui suit :

i) Mesures efficaces de prévention, de détection, d'enquête, de répression et de lutte ciblant la criminalité liée aux technologies de l'information et des communications, y compris l'utilisation des méthodes électroniques d'enquête et de collecte de preuves ;

ii) Prévention du transfert du produit d'infractions créées en application de la convention, et recouvrement de ce produit ;

iii) Détection et gel des transactions relatives au transfert du produit d'infractions créées en application de la convention ; surveillance du mouvement du produit d'infractions créées en application de la convention ; et surveillance des méthodes de transfert, de dissimulation ou de déguisement de ce produit ;

iv) Mise en place de mécanismes et de méthodes judiciaires et administratifs appropriés et efficaces pour faciliter la saisie et la confiscation du produit d'infractions créées en application de la convention ;

v) Méthodes employées pour assurer la protection des victimes et des témoins qui coopèrent avec les services de détection et de répression ;

vi) Élaboration et planification de politiques stratégiques de lutte contre les infractions liées aux technologies de l'information et des communications. Les pays devraient investir dans la mise en place et le renforcement de capacités en matière de criminalistique numérique, y compris dans l'offre de formations et de certifications sur les questions de sécurité, ainsi que dans les systèmes de gestion de la sécurité de l'information pour contribuer à l'efficacité des poursuites judiciaires visant la cybercriminalité par l'analyse des appareils électroniques afin de garantir une collecte rigoureuse des éléments de preuve ;

vii) Rédaction de demandes d'entraide judiciaire qui répondent aux conditions prévues par la convention ;

viii) Enquêtes sur la cybercriminalité, traitement des preuves électroniques, chaîne de garde de la preuve et analyse criminalistique ;

ix) Formation linguistique et professionnelle dans tous les domaines d'activité intéressant la lutte contre les infractions liées aux technologies de l'information et des communications, ainsi que la protection et l'accélération des

communications avec les organismes spécialisés en vue de détecter les infractions et de les réprimer ;

b) Les États parties dotés de capacités et d'infrastructures plus avancées dans le domaine de la cybercriminalité devraient assumer des responsabilités proportionnelles à ces capacités en offrant aux autres États, en particulier aux pays en développement, une assistance juridique, un appui et des conseils, ainsi qu'en leur transmettant des connaissances dans le domaine de la lutte contre la cybercriminalité.

États-Unis d'Amérique

[Original : anglais]
[28 octobre 2021]

C'est avec grand plaisir que le Gouvernement des États-Unis d'Amérique répond à l'invitation faite aux États Membres de communiquer leurs vues sur le champ d'application, les objectifs et la structure (éléments) de la nouvelle convention, dans le cadre de l'application des résolutions 74/247 et 75/282 de l'Assemblée générale. Les États-Unis se réjouissent de travailler avec d'autres États Membres et parties prenantes intéressées à l'élaboration d'un instrument mondial visant à améliorer les enquêtes et poursuites relatives à la cybercriminalité, dans le respect des droits et obligations existants et en s'appuyant sur ceux-ci. Nous réaffirmons l'importance d'assurer un processus ouvert, inclusif, transparent et multipartite, qui permettra à tous les États Membres de négocier de bonne foi pour trouver des solutions pratiques, éclairées et consensuelles, qui selon nous devraient favoriser une large adhésion au nouvel instrument mondial de lutte contre la cybercriminalité.

Alors que le calendrier des travaux proposé serait serré en temps normal, nous devons mener notre entreprise dans le contexte d'une pandémie mondiale. Dès lors, nous devons impérativement être concentrés et efficaces dans nos efforts pour négocier un instrument mondial de lutte contre la cybercriminalité. Malheureusement, alors que la plupart des pays se mobilisaient pour combattre la pandémie de maladie à coronavirus (COVID-19), les cybercriminels ont profité du changement mondial qui en a résulté et de notre dépendance aux technologies numériques. La cybercriminalité menace directement la sécurité et le bien-être des sociétés et des populations partout dans le monde. Une coopération de longue date nous a permis de renforcer notre capacité collective à lutter contre ce phénomène et nous pouvons nous en inspirer pour examiner attentivement des solutions pratiques. Compte tenu du caractère immédiat de la menace cybercriminelle, il est impératif que nous restions concentrés et déterminés dans nos efforts pour négocier un instrument mondial de lutte contre la cybercriminalité.

L'instrument de lutte contre la cybercriminalité devrait viser à renforcer la coopération internationale et à fournir aux services nationaux de détection et de répression des outils pratiques leur permettant de s'attaquer à la cybercriminalité, comme l'ont fait d'autres instruments des Nations Unies visant à combattre d'autres formes de criminalité transnationale, notamment la corruption, le trafic de stupéfiants, la traite des personnes et le trafic illicite de migrants. Il devrait également permettre aux autorités nationales de collecter et d'obtenir des preuves électroniques relatives à tout type d'infractions – pas seulement aux infractions cyberdépendantes – et promouvoir la coopération internationale dans ce type d'affaires. Comme pour tout instrument des Nations Unies sur la lutte contre la criminalité, ces outils devraient être assortis de limites et de garanties appropriées, dans le contexte des cadres nationaux existants, pour protéger la vie privée et les libertés civiles, tout en respectant pleinement les droits humains. L'instrument devrait aussi répondre au besoin croissant d'assistance technique et permettre aux États Membres de la demander.

Alors que les États Membres entament le processus de rédaction, il est essentiel d'admettre que notre démarche n'existe pas hors de tout contexte. S'il est important de définir le champ d'application de l'instrument, il est tout aussi important de reconnaître ce qui n'en relève pas. Des travaux utiles sur d'autres questions liées au cyberespace et dépassant le champ d'action de la cybercriminalité sont actuellement menés au sein des Nations Unies et dans d'autres instances intergouvernementales et multipartites. Il est important que nos travaux ne fassent pas double emploi avec ceux-ci et ne viennent pas les affaiblir, à la fois pour éviter les conflits en matière d'obligations et pour ne pas nous écarter de notre objectif, qui est de produire un instrument ciblé et pratique pour lutter contre la cybercriminalité. En voulant traiter toutes les questions liées au cyberespace dans cet instrument de justice pénale, nos négociations risqueraient de s'enliser dans des débats décousus et peu pertinents qui ne contribueraient guère à la lutte contre la cybercriminalité et ne feraient que ralentir notre progression vers un instrument utile.

En particulier, les États Membres ne devraient pas s'appesantir sur des sujets aussi vastes que la cybergouvernance ou la cybersécurité dans un instrument pénal voué à la lutte contre la cybercriminalité. Bien qu'elles soient souvent considérées comme les deux faces d'une même médaille, la lutte contre la cybercriminalité relève principalement de la responsabilité des gouvernements, tandis que la cybersécurité est du ressort d'une série d'acteurs publics et privés. Le mandat du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles porte essentiellement sur l'élaboration d'un instrument de justice pénale applicable dans les affaires pénales afin de faciliter une riposte internationale à la cybercriminalité, ce qui implique de définir et de prévoir des sanctions applicables aux comportements délictueux dans le cyberespace. Le Comité spécial n'est pas habilité à imposer des normes mondiales applicables aux comportements non délictueux en ligne. Intégrer des concepts de cybergouvernance et de cybersécurité dans un traité de lutte contre la cybercriminalité ne répondrait pas à l'objectif d'un instrument rationnel et efficace susceptible d'être largement soutenu par les États Membres.

Comme l'Assemblée générale l'a rappelé dans sa résolution 75/282, il est essentiel que les négociations relatives à un nouvel instrument de lutte contre la cybercriminalité ne fassent pas obstacle aux mécanismes existants, notamment les instruments multinationaux et régionaux qui offrent déjà un ensemble d'outils permettant de combattre efficacement la cybercriminalité. La meilleure façon de parvenir à un consensus sur ce nouvel instrument et d'éviter les questions politiques et les dissensions est de s'appuyer sur des instruments existants qui ont produit les résultats escomptés. Nous devrions nous inspirer des résultats obtenus dans la mise en œuvre d'autres traités de justice pénale des Nations Unies, tels que la Convention contre la criminalité transnationale organisée. Si cette convention s'est avérée très utile, c'est parce qu'elle vise les principaux types d'activités de la criminalité organisée, tout en prévoyant des dispositions générales sur la coopération internationale qui peuvent s'appliquer à tout type d'infractions graves commises à des fins lucratives au profit de trois personnes ou plus. De ce fait, les parties ont utilisé des milliers de fois la Convention contre la criminalité organisée avec succès, y compris pour lutter contre des infractions telles que les attaques de logiciels rançonneurs et l'exploitation sexuelle d'enfants.

Les États-Unis réaffirment de nouveau qu'il importe de garantir un processus ouvert, inclusif et transparent qui permettra à tous les États Membres et aux parties prenantes intéressées de négocier de bonne foi en vue de trouver des solutions pratiques, éclairées et consensuelles, ce qui, selon nous, est le meilleur moyen d'encourager une large adhésion au nouvel instrument mondial de lutte contre la cybercriminalité.

Incrimination des principaux actes de cybercriminalité

Avant toute chose, le nouvel instrument devrait conférer aux autorités nationales le pouvoir de collecter et d'obtenir des preuves électroniques pour tout type d'infractions. Ce pouvoir est impératif pour que les pays puissent enquêter efficacement sur tous les types d'infractions ou presque et en poursuivre les auteurs, car très peu d'infractions sont aujourd'hui totalement commises en dehors du monde numérique. Il devrait également autoriser la coopération internationale en matière de partage des preuves électroniques pour tout type d'infractions, sous réserve d'une disposition souple concernant la double incrimination, telle qu'elle figure dans la Convention contre la criminalité organisée et dans la Convention des Nations Unies contre la corruption[1].

Par ailleurs, une coopération internationale efficace implique qu'une législation nationale adaptée incriminant les principaux actes de cybercriminalité soit en place dans les États Membres. Afin de ne pas créer des sanctuaires pour les cybercriminels, il est essentiel que les États Membres aient une définition commune des principales infractions et des pouvoirs procéduraux correspondants. Des études de l'Office des Nations Unies contre la drogue et le crime (ONUDC) montrent que les pays s'accordent généralement sur les principaux comportements que des lois spécifiques sur la cybercriminalité devraient ériger en infractions pénales et qu'un grand nombre d'accords multinationaux et de lois pénales nationales ont des dispositions communes. De même, il existe entre les pays une entente sur les différents types de pouvoirs procéduraux légaux nécessaires pour soutenir des enquêtes efficaces sur la cybercriminalité. De ce fait, les praticiens disposent d'une vaste expérience en matière d'enquête dans ce domaine, accumulée depuis deux décennies, qui atteste que les types de pouvoirs matériels et procéduraux communément adoptés pour enquêter sur la cybercriminalité restent viables.

Le nouvel instrument de lutte contre la cybercriminalité devrait définir et viser la criminalité cyberdépendante – soit le déploiement d'une activité criminelle dont des ordinateurs ou des données sont les cibles –, ainsi que certaines infractions facilitées par Internet – soit des infractions pénales dont la commission est facilitée par l'utilisation d'un ordinateur. Cette première grande catégorie que le nouvel instrument devrait définir comprend les infractions qui ne peuvent être commises sans utiliser des ordinateurs ou des réseaux informatiques à des fins abusives et qui n'existaient donc pas en tant que telles avant l'arrivée des premiers systèmes informatiques. Les infractions cyberdépendantes peuvent être perpétrées entièrement dans le domaine numérique. S'agissant des principales infractions pénales cyberdépendantes, telles que les attaques par déni de service ou les dommages causés aux ordinateurs et aux données, des lois spécifiques à la cybercriminalité sont nécessaires, car, dans la plupart des pays, le droit pénal est interprété strictement et les lois classiques – applicables à des notions bien connues telles que la violation de domicile et le vandalisme – sont souvent inadaptées et ne peuvent être appliquées à la cybercriminalité. De plus, certaines dispositions pénales applicables aux infractions commises sans réseau informatique peuvent ne pas être facilement applicables aux agissements commis au moyen d'ordinateurs.

Nous devrions cependant nous garder de traiter les infractions classiques comme des « cyberinfractions » simplement parce qu'elles ont été planifiées ou exécutées à l'aide d'un ordinateur. Quand bien même un ordinateur a été utilisé à des fins abusives pour commettre une infraction, certains comportements coupables peuvent être couverts par les lois générales, dans la mesure où l'utilisation d'un système informatique associée à ce comportement n'a rien de particulier ou de spécial. En revanche, certaines infractions facilitées par Internet peuvent être visées à raison par

[1] Voir l'article 18, paragraphe 9, de la Convention des Nations Unies contre la criminalité transnationale organisée et l'article 46, paragraphe 9, de la Convention des Nations Unies contre la corruption. Malgré de légères différences entre les dispositions des deux conventions, elles offrent toutes deux une grande latitude aux États parties requis pour fournir une assistance concernant, en particulier, les mesures coercitives.

un instrument de lutte contre la cybercriminalité, par exemple si l'utilisation d'un ordinateur accroît :

a) La portée de l'infraction, par exemple si celle-ci fait des milliers de victimes ou permet de voler des millions de données de paiement enregistrées ;

b) La rapidité de l'attaque, car un ordinateur augmente de façon exponentielle la capacité à perpétrer l'infraction ;

c) L'ampleur des dommages ou des préjudices causés aux victimes ; ou

d) L'anonymat de l'auteur de l'infraction.

Partant de ces principes, on peut raisonnablement estimer que certaines infractions pénales classiques comme la fraude et l'exploitation d'enfants peuvent aussi entrer dans le champ de cette négociation. Les États Membres devraient toutefois faire preuve de discernement concernant le spectre des infractions facilitées par Internet qu'ils s'efforcent de combattre s'ils ne veulent pas fausser des notions de justice pénale établies de longue date. Des lois et instruments pénaux en vigueur depuis longtemps ne deviennent pas inapplicables simplement parce qu'une infraction comporte un élément « cyber ».

L'instrument mondial de lutte contre la cybercriminalité devrait également inviter les parties à adopter une législation qui incrimine les principaux actes cybercriminels d'une manière technologiquement neutre, tout en prévoyant des garanties procédurales. En incriminant les actes d'une manière technologiquement neutre – autrement dit, en incriminant l'activité qui compromet la confidentialité, l'intégrité et la disponibilité des données informatiques et non pas la forme ou la méthode particulière utilisée, comme l'hameçonnage ou un logiciel rançonneur –, nous nous assurons que les dispositions pénales matérielles couvriront les technologies et techniques criminelles d'aujourd'hui et celles de demain. Les technologies se développent rapidement, la preuve en est que même la version préliminaire de l'étude approfondie sur la cybercriminalité de 2013, qui pourtant se voulait explicitement exhaustive, manquait d'informations détaillées sur les technologies et techniques dont l'usage n'était pas très répandu, ou qui, au moment de l'étude, venaient tout juste de faire leur apparition, comme les logiciels rançonneurs, l'Internet des objets, les cryptomonnaies, ainsi que le développement rapide et la prédominance de la technologie mobile. Aussi, l'une des conclusions et recommandations approuvées par les États Membres lors de la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité observait-elle que les États Membres devraient s'assurer que leurs dispositions législatives résistent à l'épreuve du temps en ce qui concerne de futurs progrès technologiques, en adoptant à cet effet des lois aux formulations technologiquement neutres qui incriminent l'activité jugée illicite et non les moyens employés [2]. Cela est particulièrement important, car nous nous efforçons de rédiger un instrument pérenne qui puisse s'appliquer de manière adéquate aux technologies de demain et répondre aux besoins actuels et futurs des praticiens des services de détection et de répression.

Compte tenu de ces principes, un instrument mondial de lutte contre la cybercriminalité devrait incriminer, entre autres, les agissements suivants :

a) L'accès illégal, soit l'accès à un ordinateur ou à un système informatique sans autorisation ;

b) L'interception illégale, soit l'interception illégale en temps réel du contenu des communications ou des données relatives au trafic liées aux communications ;

c) L'atteinte à l'intégrité des données ou des systèmes, soit l'utilisation de logiciels malveillants, les attaques par déni de service, les logiciels rançonneurs, et la suppression ou la modification de données ;

[2] Voir le rapport sur la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 6 au 8 avril 2021(UNODC/CCPCJ/EG.4/2021/2).

d) L'utilisation abusive de dispositifs, soit le trafic ou l'utilisation de données de cartes de crédit, de mots de passe et d'informations personnelles permettant d'accéder à des ressources ;

e) Les infractions liées à des contenus montrant des violences sexuelles sur enfant ;

f) Les infractions liées à la fraude facilitée par ordinateur, soit la manipulation de systèmes ou de données informatiques à des fins frauduleuses telles que l'hameçonnage, la compromission de courriers électroniques professionnels et la fraude aux enchères ;

g) Les infractions liées à la violation du droit d'auteur et des droits connexes ;

h) La tentative, la complicité et l'entente délictueuse.

Par ailleurs, le blanchiment du produit de la cybercriminalité devrait aussi être érigé en infraction pénale. Enfin, les personnes morales devraient se voir imposer des sanctions pénales ou civiles et administratives si elles sont impliquées dans les cyberinfractions que l'instrument proscrit.

Pouvoirs procéduraux pour la collecte et le partage de preuves électroniques

Outre l'incrimination des infractions proprement dites, l'instrument mondial de lutte contre la cybercriminalité devrait également prendre en compte la nécessité pour les autorités judiciaires nationales de préserver, de collecter et de partager les preuves électroniques, dans le respect des garanties d'une procédure régulière et de la protection des droits humains et des libertés fondamentales. Plusieurs États Membres ont observé que les sources traditionnelles des pouvoirs procéduraux prévus dans leur droit interne n'étaient pas forcément applicables aux données intangibles ou n'autorisaient pas une collecte suffisamment rapide des preuves électroniques volatiles. Comme toujours, des lois obsolètes ne suffiront pas pour relever les nombreux défis rencontrés dans le cadre des enquêtes sur les infractions électroniques, notamment face aux nouvelles technologies comme le chiffrement généralisé et les services d'informatique en nuage. En matière de pouvoirs procéduraux, des sources spécialisées sont donc essentielles pour collecter des preuves électroniques. Ces lois devraient être rédigées en tenant compte des notions techniques applicables et des besoins concrets des enquêteurs. Plus précisément, ces sources de pouvoirs procéduraux devraient autoriser :

a) Une conservation rapide des données informatiques stockées ;

b) Des ordonnances demandant la production de données informatiques ;

c) Les perquisitions et les saisies de données informatiques stockées ;

d) La collecte en temps réel de données relatives au trafic ; et

e) La collecte en temps réel de données relatives au contenu en cas d'infraction grave.

Le nouvel instrument devrait en outre autoriser la coopération en matière de collecte et d'obtention de preuves électroniques pour tout type d'infractions, pas seulement en cas de cyberinfractions. Presque toutes les infractions pénales graves impliquent de recueillir des preuves électroniques, qu'il s'agisse des données de téléphones mobiles, de courriers électroniques, de données transactionnelles ou d'autres données, qui sont à prendre en considération dans les enquêtes et les poursuites. Au niveau national, les États Membres ont besoin d'un cadre juridique moderne en matière de preuve qui permette l'admission des preuves électroniques dans les enquêtes et les poursuites pénales, y compris le partage de preuves électroniques avec les partenaires des services répressifs au niveau international.

Coopération internationale

Au-delà des lois nationales, une coopération internationale efficace en matière de cybercriminalité repose à la fois sur la coopération formelle, fondée sur des traités, comme l'entraide judiciaire, et sur d'autres moyens, comme la coopération traditionnelle et autorisée entre les services de police. Le nouvel instrument devrait s'appuyer sur des outils efficaces de renforcement de la coopération internationale prévus dans les traités existants et veiller à ne pas affaiblir les instruments en vigueur et la coopération internationale déjà en place dans la lutte mondiale contre la cybercriminalité. Les dispositions relatives à la coopération internationale – notamment sur l'entraide judiciaire, l'extradition, le transfert des poursuites, la confiscation du produit, y compris les monnaies virtuelles, et la restitution aux victimes des avoirs confisqués, le principe de la double incrimination et la coopération entre les services de détection et de répression – devraient être très largement inspirées de celles prévues dans la Convention contre la criminalité organisée et dans la Convention contre la corruption, y compris les garanties et protections appropriées qu'elles contiennent et qui ont été mises en œuvre avec succès par la très grande majorité des États Membres. Par ailleurs, la disposition sur l'entraide judiciaire devrait prévoir une large assistance concernant l'obtention d'éléments de preuve électroniques relatifs à une infraction pénale, que celle-ci ait été commise ou non à l'aide d'un système informatique.

Assistance technique et renforcement des capacités

Les études de l'ONUDC indiquent que plus de 75 % des pays ont mis en place une unité spécialisée dans les questions liées à la cybercriminalité au sein de leurs services de détection et de répression, et que 15 % environ disposent d'un service spécialisé dédié à la cybercriminalité, ce qui montre bien le caractère pointu des enquêtes dans ce domaine et la nécessité de dispenser une formation spécialisée. De plus, les cyberinfractions et les éléments électroniques ou numériques des infractions classiques ont considérablement gagné en complexité, de sorte que la demande de formation et de maintien en poste d'enquêteurs et d'experts techniques hautement qualifiés augmente.

Le plus souvent, le manque de moyens internes explique pourquoi les pays ne sont pas en mesure de coopérer efficacement au niveau international. Pour la plupart des pays, si la coopération internationale échoue, ce n'est pas à cause d'un manque de volonté, mais en raison des limites de leur législation nationale ou de l'expertise limitée de leurs services de détection et de répression. Beaucoup d'États Membres ne sont pas dotés de ressources suffisantes pour que leurs services de détection et de répression puissent combattre la cybercriminalité ou traiter les éléments de preuve électroniques. Ainsi, compte tenu des priorités nationales actuelles, certains ont du mal à former des enquêteurs qualifiés et des analystes en criminalistique et à les retenir, ainsi qu'à composer avec leurs pénuries d'équipements et de logiciels. Il est par conséquent généralement admis, au niveau international, que l'assistance technique et le renforcement des capacités des services de détection et de répression, notamment des enquêteurs, des procureurs et des juges, restent des priorités absolues pour organiser une riposte internationale efficace à la cybercriminalité. De plus, les preuves électroniques faisant de plus en plus partie intégrante des enquêtes sur tous les types d'infractions ou presque, même les agents des services de détection et de répression non spécialisés devront avoir des notions de base en matière d'enquêtes informatiques.

Les dispositions de l'instrument de lutte contre la cybercriminalité relatives à l'assistance technique et aux capacités devraient prévoir :

a) Que les États Membres prennent des mesures pour élaborer, développer ou améliorer les programmes de formation destinés au personnel chargé de prévenir et de combattre la cybercriminalité ;

b) Que les États Membres envisagent, dans leurs plans et programmes nationaux de lutte contre la cybercriminalité, selon leurs capacités, de s'accorder l'assistance technique la plus étendue, en particulier au profit des pays en

développement et des pays qui peuvent être confrontés de manière disproportionnée à des menaces de cybercriminalité ;

c) Que soient établis des mécanismes permettant aux États Membres de verser des contributions volontaires pour soutenir l'application de l'instrument de lutte contre la cybercriminalité ;

d) Que les États Membres envisagent de verser des contributions volontaires au Programme mondial de l'ONUDC contre la cybercriminalité et à ses programmes connexes de renforcement des capacités de la justice pénale.

Participation de la société, d'entités et d'organisations

Il est impossible de lutter de façon compartimentée contre la cybercriminalité, vu la complexité et la nature multidimensionnelle du phénomène. Un instrument de lutte contre la cybercriminalité devrait tenir compte de l'importance d'une participation active de personnes et de groupes, dans le respect de la parité femmes-hommes, notamment d'organisations non gouvernementales, d'organisations de la société civile, d'établissements universitaires et du secteur privé, à la prévention de la cybercriminalité. Cette participation contribuera à sensibiliser le public aux menaces que représente la cybercriminalité, à garantir la transparence de l'action des États Membres et la prise en compte de questions de fond liées à la vie privée, aux libertés civiles et aux droits humains. L'efficacité de l'instrument dépend aussi des contributions de personnes et d'entités ayant des compétences en matière de cybercriminalité. Une forte participation d'experts dans ce domaine est essentielle à la mise en œuvre d'un instrument pratique et efficace de lutte contre la cybercriminalité.

Mécanismes d'application

Il est encore trop tôt pour savoir si un processus distinct sera nécessaire pour examiner l'application future de l'instrument et, dans l'affirmative, quelle forme il devrait prendre. Plusieurs modèles ont fait leurs preuves. Compte tenu de l'insuffisance des ressources disponibles pour l'assistance technique, des méthodes reposant sur des solutions abordables devraient être envisagées pour optimiser les contributions des donateurs au titre de l'assistance technique. L'une de ces méthodes consisterait à habiliter la Commission pour la prévention du crime et la justice pénale, créée par la résolution 1992/1 du Conseil économique et social, à examiner toutes les questions ayant trait aux objectifs de l'instrument de lutte contre la cybercriminalité. La Commission des stupéfiants, qui supervise l'application des trois traités internationaux relatifs au contrôle des drogues, est un exemple positif à cet égard. Comme indiqué plus haut, il est essentiel qu'une forte participation de la société, des entités et des organisations publiques soit envisagée lors de la mise en œuvre de tout axe de travail émanant d'un instrument. Toutefois, la discussion sur les mécanismes d'application devrait être reportée jusqu'à ce que la définition du champ d'application de l'instrument soit plus précise.

Fédération de Russie

Note du Secrétariat : Les observations de la Fédération de Russie figurent dans le document A/75/980, intitulé « Lettre datée du 30 juillet 2021, adressée au Secrétaire général par le Chargé d'affaires par intérim de la Fédération de Russie auprès de l'Organisation des Nations Unies », et dans l'annexe à cette lettre, intitulée « Projet de convention des Nations Unies sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles », dont l'Assemblée générale a été saisie à sa soixante-quinzième session. Le document a été communiqué au Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles en même temps que les commentaires des États Membres sur le champ d'application, les objectifs et la structure (éléments) de la nouvelle convention, conformément à l'invitation de la Présidente du Comité spécial.

Indonésie

[Original : anglais]
[28 octobre 2021]

Contexte général et objectifs

L'Indonésie, qui est l'un des plus grands utilisateurs d'Internet au monde, a bien conscience de l'importance des technologies de l'information et des communications (TIC) pour la société. Toutefois, les progrès des TIC ont été exploités pour induire des comportements irresponsables, notamment la cybercriminalité et le cyberterrorisme, ce qui compromet l'utilisation de ces technologies en faveur du développement politique, économique et social.

La cybercriminalité, comme d'autres formes de criminalité transnationale, a porté préjudice à la communauté internationale, en raison de la nature exceptionnelle de la technologie et du cyberespace qui ne connaissent pas de frontières. La coopération internationale est donc essentielle. L'Indonésie salue l'adoption de la résolution 74/247 de l'Assemblée générale, dans laquelle l'Assemblée a décidé d'établir un comité intergouvernemental spécial d'experts à composition non limitée chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

L'Indonésie estime qu'il est particulièrement opportun et essentiel de débattre d'une convention traitant expressément de la cybercriminalité dans le cadre du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, et espère que les États profiteront de l'élan ainsi imprimé pour examiner et négocier un instrument international capable de répondre aux défis de la cybercriminalité, de manière inclusive et transparente.

Au cours de la dernière décennie, des progrès importants ont été réalisés dans le cadre de l'examen et de l'élaboration d'instruments internationaux visant à déterminer les méthodes les plus efficaces de prévenir la cybercriminalité. Par conséquent, pour élaborer un futur instrument de lutte contre la cybercriminalité, les États devraient prendre en considération tous les outils et cadres existants, y compris les travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité et la Convention des Nations Unies contre la criminalité transnationale organisée.

Les débats consacrés à la convention sur la cybercriminalité devraient viser principalement à renforcer et à promouvoir la coopération internationale à l'appui des efforts de lutte menés à l'échelle nationale, régionale et internationale contre l'utilisation des TIC à des fins criminelles, notamment en fournissant une assistance technique pour améliorer les législations et les cadres nationaux des États Membres et renforcer la capacité des autorités nationales à s'attaquer à ce type de criminalité.

En outre, la convention devrait prévoir des mesures appropriées et efficaces applicables entre et parmi les États ainsi que, le cas échéant, en collaboration avec les organisations internationales et régionales compétentes.

Principes

Comme pour de nombreuses conventions internationales, notre examen doit tenir compte des obligations contractées par les États Membres conformément aux principes d'égalité souveraine et d'intégrité territoriale des États, ainsi que de non-ingérence dans les affaires intérieures des autres États. En outre, les États devraient respecter les droits souverains des autres États lorsqu'ils élaborent des politiques et des législations pour lutter contre la cybercriminalité, conformément à leurs situation et besoins nationaux.

Le futur instrument doit prendre en considération l'impact sur la sécurité et les conséquences socioéconomiques et humanitaires de l'utilisation des TIC à des fins criminelles. Dans le même temps, la convention doit faire en sorte que les mesures de

lutte contre la cybercriminalité soient axées sur le comportement criminel et ne compromettent pas le développement des TIC, y compris la recherche-développement et le transfert de technologies.

Il est dans l'intérêt de tous et essentiel pour le bien commun de promouvoir l'utilisation des TIC à des fins pacifiques. Le respect de la souveraineté, des droits humains et des libertés fondamentales, ainsi que le développement durable et numérique, restent au cœur des efforts déployés dans ce contexte.

L'Indonésie est également consciente de l'intérêt qu'il y a à veiller à ce que les procédures pénales soient établies, mises en œuvre et appliquées conformément au droit interne de chaque nation, tout en reconnaissant la nécessité de remédier aux difficultés que soulèvent les différences entre les procédures pénales des États, ainsi que les obligations contractées par chaque État en vertu des instruments internationaux pertinents, tels que la Convention contre la criminalité organisée et les instruments relatifs au droit international des droits de l'homme, aux droits de propriété intellectuelle, à l'extradition bilatérale et à l'entraide judiciaire.

En outre, les États Membres doivent souligner qu'il est nécessaire de maintenir un processus multipartite ouvert et transparent qui leur permette à tous de négocier de bonne foi en vue de trouver des solutions éclairées, consensuelles et réalistes.

Champ d'application

Le champ d'application de la convention doit permettre de relever les défis actuels et futurs posés par l'utilisation abusive des TIC à des fins criminelles, de protéger les utilisateurs des TIC, ainsi que d'atténuer et de prévenir les dommages causés aux personnes, aux données, aux systèmes, aux services et aux infrastructures.

La convention devrait également pouvoir garantir que les États Membres sont en mesure d'adopter les mesures législatives et autres nécessaires pour incriminer le fait d'entreprendre des activités interdites par elle, notamment les délits informatiques et les délits liés à l'utilisation des réseaux informatiques, ainsi que d'autres activités menées à des fins illégales.

L'Indonésie estime que la future convention devrait couvrir toute une série d'infractions principales liées à la cybercriminalité. Il devrait s'agir, entre autres :

a) Du fait d'accéder illégalement à des systèmes informatiques ou de les pirater ;

b) De l'interception illégale de données informatiques et de systèmes ;

c) De la fraude ;

d) De l'utilisation abusive de données et de systèmes informatiques à des fins criminelles ;

e) De la violation des droits d'auteur et des droits voisins ;

f) De la manipulation de données et de systèmes informatiques ;

g) De la distribution et de la transmission de contenus et de supports illégaux, concernant, par exemple, la pornographie, la pédopornographie, la désinformation, les thèses conspirationnistes et les canulars, ainsi que de supports diffusant des éléments hostiles en rapport avec la race, la nationalité, la religion ou la politique.

Les États Membres devraient envisager d'adopter les mesures nécessaires pour mener à bien les procédures pénales décrites dans la convention, y compris, mais sans s'y limiter :

a) La conservation des données et des systèmes et la conservation des données relatives au trafic stockées par un ou plusieurs fournisseurs de services, étant entendu que le délai de conservation des données et la classification des données stockées sur leur territoire sont régis par le droit international et national ;

b) La soumission ou le transfert de données informatiques stockées par des personnes physiques ou morales, et la mise en place de mesures adéquates pour contraindre les fournisseurs de services de systèmes en ligne à soumettre ou transférer

les données informatiques stockées, y compris les données liées au type de services fournis ;

c) La recherche et la saisie de données et de systèmes informatiques, la création et la conservation de copies de données informatiques, ainsi que la modification et le transfert de données stockées ;

d) La collecte et l'enregistrement de données relatives au trafic en temps réel, ainsi que l'obtention de données relatives au trafic auprès de fournisseurs de services et/ou de systèmes en ligne.

Compte tenu de ce qui précède, les États Membres devraient veiller à ce que le processus d'enquête sur la cybercriminalité soit mené conformément aux principes de protection de la vie privée, de confidentialité, de durabilité du service public, de maintien de la continuité des services publics et de défense de l'intérêt public, ainsi que d'intégration des données.

Coopération

La cybercriminalité et les infractions facilitées par l'utilisation des TIC devraient faire l'objet d'enquêtes efficaces aux niveaux national et transnational. Ainsi, la convention devrait servir de mécanisme efficace pour la coopération internationale dans la lutte contre l'utilisation des TIC à des fins criminelles. Cette coopération devrait être mise en œuvre sur la base de l'avantage mutuel et de la réciprocité, conformément à la législation nationale, compte tenu des instruments existants et des mécanismes et cadres en vigueur.

Eu égard à l'importance des approches multipartites de la prévention, de la détection et de l'éradication de la cybercriminalité, le débat devrait également porter sur la promotion d'une solide coopération avec les entités chargées de lutter contre la cybercriminalité, y compris la coopération entre les services de détection et de répression et les fournisseurs de services informatiques. Dans ce contexte, la collaboration avec les entreprises privées, renforcée par des partenariats public-privé lorsque cela est possible, est essentielle pour améliorer les connaissances et accroître l'efficacité des moyens de répression de la cybercriminalité. Les États Membres devraient également mener des actions de sensibilisation à la cybercriminalité dans les secteurs public et privé.

Nos délibérations devraient également mettre en évidence les mesures permettant aux autorités de mener des enquêtes dans lesquelles des données peuvent être recueillies et confisquées par le biais de mécanismes d'entraide judiciaire, et les États Membres pourraient envisager d'utiliser leurs cadres juridiques existants à cet égard.

S'agissant de l'entraide judiciaire, nos délibérations devraient tenir compte, dans toute la mesure possible, des lois, traités et accords pertinents en ce qui concerne les enquêtes, les poursuites et les procédures judiciaires. Les États Membres sont encouragés, entre autres, à débattre des dispositions tendant à accélérer la collecte de preuves électroniques, ou des mécanismes d'échange d'informations entre les autorités compétentes.

Les dispositions de cette convention relatives à la coopération internationale doivent fournir un cadre juridique essentiel pour remédier aux problèmes de procédure, aux lacunes et à l'insuffisance des mécanismes de coopération internationale, notamment en ce qui concerne les enquêtes, le partage d'informations, la collecte de données et de preuves électroniques, et les poursuites, ainsi que pour faciliter l'extradition entre les États. Les États Membres sont également encouragés à désigner des points de contact ou des autorités spécialisées pour accélérer la mise en œuvre des dispositions de la convention relatives à la coopération internationale.

En outre, les États Membres pourraient envisager de développer leur capacité nationale à mettre en évidence l'utilisation des TIC à des fins criminelles, à enquêter à ce sujet et à prendre des mesures de lutte contre ce phénomène, grâce à des activités de renforcement des capacités et d'assistance technique contribuant à accroître leur résilience. Ces mesures de renforcement des capacités devraient être fondées sur la

confiance mutuelle, être motivées par une demande correspondant aux besoins recensés au niveau national et reconnaître pleinement que les pays conservent la maîtrise du processus.

La collaboration en matière de prévention et d'éradication de la cybercriminalité restant une priorité dans nos débats, le futur instrument devrait, pour le moins, inclure une liste d'activités tendant à améliorer la coopération par le biais des mesures suivantes :

a) Échanger des informations sur les menaces liées à la cybercriminalité ;

b) Favoriser la coopération et la coordination entre les services de détection et de répression, les procureurs et les autorités judiciaires ;

c) Mettre en commun les meilleures pratiques et les données d'expérience relatives aux enquêtes transnationales sur la cybercriminalité ;

d) Établir des partenariats public-privé avec les fournisseurs de services afin de définir des modalités de coopération en matière de détection et de répression, d'enquêtes sur la cybercriminalité et de collecte de preuves ;

e) Élaborer des lignes directrices à l'intention des fournisseurs de services informatiques pour aider les services de détection et de répression dans le cadre des enquêtes sur la cybercriminalité, notamment en ce qui concerne le format et la durée de conservation des preuves et informations numériques ;

f) Développer les compétences et les ressources humaines dans le cadre des politiques permettant aux États Membres d'accroître leur capacité d'adaptation aux technologies numériques ;

g) Renforcer les capacités techniques et juridiques des services de détection et de répression, des juges et des procureurs au moyen de programmes de développement des compétences.

Grâce à ce mécanisme, les États Membres devraient également continuer d'améliorer l'efficacité de la coordination et des synergies interinstitutions au niveau national, y compris en ce qui concerne l'échange d'informations et la collaboration avec les organisations régionales, le secteur privé, les équipes d'intervention en cas d'urgence informatique et les équipes d'intervention en cas d'incident de sécurité informatique, les organisations de la société civile et les autres parties prenantes, afin de favoriser la mise en place d'une coopération internationale efficace.

Le débat devrait également porter sur un mécanisme d'examen de l'application ou de la mise en œuvre de tous les engagements et obligations contractés au titre du futur instrument.

Jamaïque

[Original : anglais]
[29 octobre 2021]

Les vues énoncées ci-après sont communiquées en réponse à la demande que le secrétariat du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles a adressée aux États pour qu'ils formulent des observations sur le champ d'application, les objectifs et la structure d'une convention internationale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

La Jamaïque attend avec intérêt de contribuer aux travaux entrepris en vue de la rédaction d'une convention sur la cybercriminalité en coopération avec les autres États Membres. Elle table sur une convention qui répondra aux besoins de la communauté mondiale en ayant pour objectif de protéger les citoyens contre les cybermenaces ou autres attaques criminelles et qui sera universellement acceptée et

ratifiée. Elle se félicite de la participation d'experts de la société civile dans ce domaine pour enrichir nos délibérations.

La Jamaïque considère que le processus d'élaboration d'une convention sur la lutte contre l'utilisation criminelle des technologies de l'information et des communications (TIC) apporte une contribution décisive aux mesures envisagées par la communauté mondiale pour parer aux problèmes que rencontrent les États en raison de cette menace. L'objectif d'une telle convention a été décrit avec justesse dans le rapport de consensus élaboré en 2015 par le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, qui prévoyait, à l'alinéa d) du paragraphe 13, que ceux-ci devraient réfléchir à la meilleure façon de coopérer pour échanger des informations, s'entraider, engager des poursuites en cas d'utilisation criminelle des TIC et appliquer d'autres mesures collectives afin de parer à ces risques[3].

Coopérer à l'échange d'informations afin d'aider les États à combattre et à poursuivre l'utilisation criminelle des TIC devrait être l'objectif général de la convention. Vient ensuite celui consistant à faire mieux connaitre aux États les différentes perspectives en matière de cybercriminalité. Il faut espérer que s'ensuivra une harmonisation des approches, socle d'un cadre international valable pour tous. Cet objectif ne pourra néanmoins être atteint que si l'on suit un processus durant lequel seront prises en considération, de manière équilibrée, équitable, transparente et inclusive, les positions de tous les États, y compris des petits États insulaires en développement.

Il conviendra de tenir compte d'autres processus qui peuvent contribuer, sans les retarder indûment, aux travaux d'élaboration d'une convention. Il serait bon de respecter les délais impartis pour les négociations et l'achèvement du projet de convention afin de prouver à quel point nous prenons au sérieux la lutte contre la cybercriminalité.

Il va de soi que la définition des termes constitue le point de départ des négociations. Les termes fixent le champ d'application de la convention et sont importants pour atteindre les objectifs communs des participants. Les définitions doivent donc être claires, bien réfléchies et soigneusement élaborées de sorte qu'elles ne soient pas excessivement restrictives ou larges, mais soient adaptées au contexte et aux objectifs de la convention.

La lutte contre l'utilisation des TIC à des fins criminelles est une mission ambitieuse. Il faut donc inscrire dans la durée les infractions, qui devraient être définies de manière à ne pas être limitées aux technologies existantes mais, au contraire, à pouvoir être interprétées au gré de l'évolution des technologies futures et de celle, constante, de l'environnement des TIC.

La convention devrait prévoir des mesures contre les infractions qui renforcent les outils dont disposent les pays pour cibler la cybercriminalité et qui ne portent pas atteinte aux droits et libertés fondamentaux de la personne mais visent à promouvoir l'observation et le respect de ces droits. Il conviendra donc de prendre en considération les traités internationaux relatifs aux droits humains.

Les dispositions d'une nouvelle convention devraient tenir dûment compte du principe de la souveraineté des États, ainsi que d'autres principes énoncés dans la Charte des Nations Unies et le droit international, en matière de procédure pénale, de détection et de répression, et de coopération internationale.

La Jamaïque estime que la convention doit traiter comme il convient la question de la coopération internationale pour faciliter une meilleure collaboration dans le cadre de la lutte mondiale contre la cybercriminalité. Lorsque des États ne sont pas liés par un traité d'entraide judiciaire, elle devrait leur montrer la voie à suivre pour

[3] A/70/174.

déposer une demande ou y répondre, sans oublier certains points comme la prise en charge des coûts.

La convention doit tenir compte des diverses capacités des États, qui elles-mêmes ont une incidence sur l'aptitude de ces derniers à coopérer aussi largement que nécessaire pour obtenir les meilleurs résultats. Il est donc crucial qu'une assistance technique soit mise à la disposition des États pour qu'ils soient à même de contribuer davantage au cadre mondial de la lutte contre la cybercriminalité. À cet égard, le renforcement des capacités devrait s'inscrire dans la durée, avoir un but clairement défini, correspondre aux besoins nationaux et répondre à l'objectif de mise en valeur des ressources humaines dans ce domaine spécialisé. Il faudrait aussi envisager de mettre en place un mécanisme de financement qui viendrait l'appuyer en vue de l'application de la convention sur la cybercriminalité.

Japon

[Original : anglais]
[29 octobre 2021]

En tant qu'État Membre qui attache de l'importance au déroulement d'un processus inclusif, transparent et équitable en vue de la rédaction de la future convention des Nations Unies sur la cybercriminalité, le Japon a le plaisir d'apporter sa propre contribution à cet effet avant le début des travaux officiels de rédaction et remercie la Présidence de lui en offrir la possibilité.

Bien que les États ne soient pas confrontés aux mêmes problèmes en matière de cybercriminalité, le Japon considère que celle-ci constitue pour tous une menace grave qui ne cesse d'évoluer. Afin de lutter contre la cybercriminalité, fléau qui ne s'arrête pas aux frontières nationales, il est essentiel de veiller à ce que tous les États Membres coopèrent les uns avec les autres. Le Japon estime donc que nous devrions aspirer à rechercher les moyens de garantir un cyberespace libre, équitable et sûr et de renforcer notre capacité à prévenir et à combattre la cybercriminalité dans le monde entier en faisant en sorte que la nouvelle convention internationale ait une portée universelle et que tous les États Membres souscrivent à ses dispositions.

La présente contribution expose les vues du Japon sur le champ d'application, les objectifs et la structure de la nouvelle convention, afin de favoriser les délibérations au sein du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, créé conformément à la résolution 74/247 de l'Assemblée générale.

Champ d'application

Pour renforcer les mesures mondiales de lutte contre la cybercriminalité et établir un cadre international universel, la communauté internationale devrait, en premier lieu, élaborer un cadre solide, en se concentrant sur les dispositions fondamentales et essentielles relatives aux infractions pénales et à la procédure pénale, ainsi qu'à l'entraide judiciaire et aux autres formes de coopération internationale dans ce domaine.

Les actes que la nouvelle convention érigera en infractions devraient être limités à la cybercriminalité ; les infractions créées par la nouvelle convention devraient avant tout couvrir celles qui sont purement informatiques, et les infractions facilitées par les TIC ne devraient être visées qu'en cas de besoin et s'il existe un large consensus à leur sujet parmi les États Membres.

La nouvelle convention devrait reposer fermement sur les délibérations menées antérieurement et actuellement dans les cadres existants de la lutte contre la cybercriminalité, tout en tenant compte des débats et travaux engagés dans d'autres

instances auxquels sont associées des réflexions sur la cybercriminalité, afin d'éviter les doubles emplois ou de ne pas remettre en cause les travaux.

Afin d'établir un cadre international universel qui soit généralement applicable à toutes formes d'utilisation des technologies de l'information et des communications, indépendamment des disparités existant entre les États, et de pouvoir suivre l'évolution future des technologies, il conviendra d'employer des formulations neutres sur le plan technologique pour la rédaction des dispositions de la nouvelle convention.

Quelle que soit l'importance de la lutte contre la cybercriminalité, les mesures prises pour la combattre ne doivent pas porter atteinte au droit à une procédure régulière, ni imposer des restrictions injustifiables aux droits humains. Ces garanties étant des conditions préalables à une coopération internationale fructueuse, la nouvelle convention devrait inclure des dispositions concrètes visant à garantir le respect des procédures régulières et des droits humains.

Objectif

L'objectif premier de la nouvelle convention devrait être de contribuer à la sûreté et à la sécurité de toutes les personnes associées aux technologies de l'information et des communications qui devraient être protégées, ainsi qu'à la protection de leurs intérêts. À cette fin, il faut intensifier les mesures de lutte contre la cybercriminalité au niveau mondial en établissant un cadre international universel qui s'appliquerait le plus largement possible à la cybercriminalité sous ses diverses formes transnationales et en favorisant une coopération bilatérale ou multilatérale efficace en matière d'enquêtes et de poursuites pénales.

Pour atteindre cet objectif, la nouvelle convention devrait comporter des dispositions fondamentales et essentielles qui puissent être observées et mises en œuvre par le plus grand nombre possible d'États Membres, de sorte à perfectionner, à l'échelle mondiale, les mesures visant à lutter contre la cybercriminalité et à renforcer les cadres existants.

Structure

Le Japon estime que la nouvelle convention pourrait s'articuler utilement autour de la structure de base présentée ci-après, mais il est prêt à se prononcer en faveur d'une structure plus détaillée lors des négociations à venir :

a) Définition des termes :

b) Liste des mesures que les États Membres devraient adopter à l'échelle nationale :

i) Incrimination :

a. Infractions classées dans la catégorie des infractions purement informatiques ;

b. Infractions classées parmi celles facilitées par les TIC qui devraient être incriminées ;

ii) Dispositions procédurales concernant la conservation, la divulgation et la production de données ;

iii) Garanties destinées à assurer les droits humains et autres droits ;

c) Coopération internationale en matière d'extradition, d'entraide judiciaire et autres formes de coopération ;

d) Dispositions finales.

Jordanie

[Original : arabe]
[28 octobre 2021]

Champ d'application

La convention devrait couvrir les infractions concernant :

- Le caractère confidentiel, l'intégrité et la disponibilité des services électroniques ;
- L'accès non autorisé à un réseau d'information, à un système d'information ou à une quelconque partie de ceux-ci ;
- La dégradation d'infrastructures critiques ;
- L'intention de saboter des réseaux d'information ou des systèmes d'information ;
- L'espionnage du flux de données sur un réseau d'information ou un système d'information ;
- La fraude, l'usage de faux et l'usurpation d'identité ;
- L'interception de données ou d'informations tirées de systèmes financiers ;
- La violation de la vie privée et de la propriété intellectuelle ;
- Le matériel, les logiciels de déchiffrement et les codes d'accès ;
- La fraude aux noms de domaine ;
- La pornographie ;
- L'exploitation et la maltraitance d'enfants ;
- La diffusion d'informations fallacieuses ;
- La discrimination raciale ;
- L'exploitation des femmes et les violences à leur encontre ;
- La sédition, l'incitation à la haine ou la diffusion de discours de haine ;
- Le trafic illégal via des réseaux d'information ou des sites Web ;
- La diffusion ou la promotion d'une idéologie terroriste ou le soutien apporté à une telle idéologie ;
- L'utilisation des technologies de l'information et des communications (TIC) à des fins terroristes ;
- Les atteintes portées aux religions, aux pays et aux symboles ;
- Les chaînes d'approvisionnement ;
- Les logiciels rançonneurs ;
- Le hameçonnage par voie électronique ;
- Le piratage de logiciels ;
- L'utilisation non autorisée de données par les prestataires de services.

Objectifs

Les objectifs de la présente Convention devraient être les suivants :

- Renforcer la coopération et la coordination à l'échelle internationale pour lutter contre l'utilisation des TIC à des fins criminelles ;

- Élaborer une législation internationale pour lutter contre l'utilisation des TIC à des fins criminelles ;
- Souligner l'importance de la protection des infrastructures critiques en instituant des mesures de lutte contre l'utilisation des TIC à des fins criminelles ;
- Promouvoir l'importance de mettre sur pied des capacités nationales et internationales et de les améliorer et mieux sensibiliser les personnes et les sociétés à la lutte contre l'utilisation des TIC à des fins criminelles.

Structure

- Introduction.
- Définitions.
- Objectifs.
- Champ d'application.
- Devoirs et responsabilités.
- Coopération internationale.
- Renforcement des capacités et sensibilisation.
- Mécanisme d'application.
- Mise à jour permanente de la convention en fonction des éléments nouveaux.

La convention devrait avoir un champ d'application étendu pour couvrir le plus grand nombre possible de pays dans le monde, en mettant l'accent sur ceux qui sont de grands terrains d'expérimentation de technologies.

Elle devrait intégrer des concepts approuvés à l'échelon international s'appliquant à la commission d'infractions liées aux technologies de l'information contre des personnes ou des fonds.

L'accent devrait être mis sur la création de moyens qui permettraient aux services de détection et de répression des États parties d'échanger des informations et sur la mise en place de mécanismes pour le suivi des fonds provenant d'infractions relevant de la fraude électronique et pour l'identification de leurs auteurs, dans le respect de la législation nationale et de la vie privée.

Des points de contact permanents devraient être établis dans les États parties pour intervenir immédiatement en cas d'actes de terrorisme ou d'exploitation sexuelle des enfants, entre autres. Il est également nécessaire de créer des mécanismes propres à promouvoir la coopération avec les médias sociaux de portée internationale de sorte à pouvoir communiquer les informations techniques nécessaires pour lutter contre ce type d'infractions.

Il conviendrait d'encourager la coopération internationale pour renforcer les capacités du personnel des services de lutte contre la cybercriminalité dans les États parties au moyen de cours de formation, d'ateliers et d'échanges de données d'expérience.

Koweït

[Original : arabe]
17 novembre 2021

1. De manière générale, le projet de convention devrait souligner que cet instrument a pour objectif d'améliorer et de renforcer la coopération destinée à combattre et à réduire les risques d'infractions liées aux technologies de l'information, sur la base des principes de l'égalité souveraine des États et de la non-ingérence dans leurs affaires intérieures, qui englobent les procédures liées à

l'exercice de la compétence, au respect de l'état de droit, au maintien de l'ordre et de la sécurité publics et au respect des valeurs sociales.

2. Il devrait être tenu compte dans le champ d'application de la convention des instruments internationaux destinés à prévenir les actes terroristes ainsi que de la Convention des Nations Unies contre la criminalité transnationale organisée et de ses protocoles, de sorte à couvrir les infractions commises dans plus d'un pays, celles qui sont préparées, planifiées, dirigées ou supervisées dans d'autres pays, celles commises dans d'autres pays, ou encore celles commises dans un pays mais ayant de graves conséquences dans un autre.

3. Les actes à incriminer en vertu de la convention devraient être établis en fonction des nouvelles formes de criminalité liées aux technologies de l'information et des communications (TIC) définies comme des infractions principales dans la législation interne des États parties, et plus particulièrement celles liées au contenu, aux discours de haine et à la violence.

4. Il faudrait établir des cadres pour les éléments suivants : la coopération juridique et judiciaire, l'extradition des criminels, l'échange d'informations, la possibilité de communiquer des informations sans demande préalable si l'État partie estime que leur divulgation pourrait contribuer à l'ouverture d'enquêtes sur des infractions, la coopération en matière de divulgation et de conservation urgentes d'informations stockées au moyen de technologies de l'information, l'accès aux technologies de l'information de portée internationale, la coopération et l'assistance bilatérales concernant la collecte en temps réel de données relatives au trafic, l'établissement d'éléments de confidentialité et les limites de l'utilisation des données figurant dans les demandes d'entraide judiciaire.

5. Des cadres devraient également être établis pour l'évaluation de l'application de la convention selon les mécanismes utilisés par les États parties. Des institutions compétentes et des points de contact devraient être désignés dans les États parties, et il faudrait s'employer à tirer parti des réseaux d'information existants au sein de l'Office des Nations Unies contre la drogue et le crime.

Liechtenstein

[Original : anglais]
[28 octobre 2021]

Le Liechtenstein tient à remercier le secrétariat du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et sa présidente, S. E. M^me^ Faouzia Boumaiza, d'avoir sollicité l'avis des États Membres sur le champ d'application, les objectifs et la structure (éléments) de la nouvelle convention. La position générale du Liechtenstein est la suivante.

Un objectif majeur du Liechtenstein est de veiller à ce qu'une nouvelle convention sur la cybercriminalité soit conforme aux instruments internationaux et régionaux existants, notamment la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention du Conseil de l'Europe sur la cybercriminalité, et qu'elle soit étayée par le droit international, y compris le droit des droits humains.

Le Liechtenstein s'oriente donc vers une convention courte et fonctionnelle qui se concentre sur les infractions propres au cyberespace, telles que l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données et des systèmes, l'utilisation abusive de dispositifs, le faux et l'usage de faux en informatique, la fraude informatique, les infractions qui supposent une violation du droit d'auteur et celles liées à la pornographie mettant en scène des enfants. L'incrimination à grande échelle d'infractions autres que celles commises dans le cyberespace devrait être couverte par d'autres conventions et instances et n'a donc pas sa place ici. En outre, le

Liechtenstein est contre la répétition inutile d'infractions couvertes par d'autres traités particuliers.

Du fait de l'évolution rapide de l'environnement dans le cyberespace, le Liechtenstein œuvre en faveur d'une convention rédigée dans un langage neutre sur le plan technique afin que les infractions pénales proprement dites puissent s'appliquer tant aux technologies actuelles concernées qu'aux futures. Il conviendra d'éviter d'employer dans la convention des définitions techniques précises de certaines formes de cybercriminalité susceptibles de devenir obsolètes à l'avenir.

Un autre aspect crucial pour le Liechtenstein est celui des dispositions relatives à la protection des données et aux droits humains, qui doivent occuper une place importante dans la convention. Il est primordial que les normes en la matière soient pleinement respectées.

Une position plus détaillée du Liechtenstein sera présentée lors des négociations relatives à la nouvelle convention sur la cybercriminalité.

Mexique

[Original : espagnol]
[21 octobre 2021]

Pour le Gouvernement mexicain, les technologies de l'information et des communications, les plateformes numériques et le cyberespace offrent des possibilités majeures de consolider le développement, de remédier aux inégalités et de promouvoir l'inclusion, le bien-être, la justice et les droits.

Le Mexique est néanmoins conscient que la commission d'infractions au moyen de ces technologies, outre que celles-ci favorisent le développement d'un marché illicite, préoccupe de plus en plus les gouvernements, les entreprises, les organisations sociales et tous les individus.

La coopération internationale et les mécanismes d'entraide judiciaire et d'échange de renseignements sont plus que jamais une nécessité. Le Mexique est attaché au multilatéralisme, et en particulier au rôle de l'ONU dans la définition de mesures globales et utiles face à ce problème mondial.

Le Mexique estime que le mandat établi par l'Assemblée générale afin que soit élaborée une convention générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles offre une occasion idéale d'engager un processus approfondi, résolu, pluriel, inclusif et transparent, en tenant compte des enseignements d'autres processus des Nations Unies menés sur le sujet et d'autres données d'expérience régionales recueillies dans ce domaine.

On trouvera ci-après les aspects que le Gouvernement mexicain souhaiterait voir abordés dans le processus d'élaboration de la convention future ainsi que dans son contenu.

Objectifs, portée et caractéristiques de la convention

La convention devrait constituer un instrument juridique complet et contraignant, couvrant les questions de droit matériel et procédural et définissant des modalités pour la coopération internationale et l'échange de renseignements, de données d'expérience, de compétences techniques et de bonnes pratiques.

Le Mexique souhaite que la convention aide à promouvoir des normes pour faciliter les enquêtes, l'action préventive et les poursuites. Nonobstant le fait que la convention n'exclut pas la possibilité d'adhérer à d'autres instruments en la matière, il en attend également un cadre de référence uniformisé qui permette de réprimer plus efficacement la cybercriminalité.

Devraient figurer dans la convention les éléments suivants :

- Définitions générales, typologies de base et indication des acteurs compétents ;
- Mesures procédurales de base que les États devraient adopter pour pouvoir mener des enquêtes et des poursuites efficaces concernant les actes de cybercriminalité ;
- Qualifications pénales générales à prévoir dans les lois nationales ;
- Mécanismes pour l'accès à l'information et la promotion d'une collaboration efficace.

La convention future devrait aussi ménager la possibilité de formuler des réserves et des déclarations interprétatives et prévoir une procédure d'amendement souple, pour en faciliter l'actualisation, et fixer des mécanismes de règlement des différends. Il conviendrait d'en subordonner l'entrée en vigueur au dépôt de 50 instruments de ratification.

Une fois arrêté le contenu de la convention, il serait bon de s'accorder sur un mécanisme efficace, universel et peu onéreux pour l'examen de son application par des pairs.

Pertinence des autres instruments internationaux

Pour le Gouvernement mexicain, il importe que la convention parte du principe que le droit international est applicable au cyberespace et que, dès lors, un certain nombre d'instruments juridiques internationaux en vigueur soient pris en considération, parmi lesquels :

- La Convention des Nations Unies contre la criminalité transnationale organisée et les trois protocoles y relatifs ;
- Le Statut de la Cour internationale de Justice ;
- La Convention du Conseil de l'Europe sur la cybercriminalité ;
- Les traités relatifs à la protection des données à caractère personnel et aux flux internationaux de ces données ;
- Les traités internationaux relatifs aux droits humains et les traités protégeant les garanties reconnues aux personnes visées par des procédures judiciaires ;
- Les traités applicables à la propriété intellectuelle ;
- Les traités bilatéraux sur l'extradition, l'entraide judiciaire en matière pénale et d'autres formes de coopération internationale dans le domaine judiciaire.

En outre, le processus de négociation pourrait utilement s'inspirer de certains documents adoptés sous l'égide de l'ONU et d'autres instances internationales compétentes, dont principalement les suivants :

- La compilation des conclusions et recommandations issues des réunions tenues par le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité en 2018, 2019 et 2020 ;
- Le rapport final du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace, portant sur la période 2019-2021, et ses rapports antérieurs de 2013 et de 2015 ;
- Le rapport final du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, portant sur la période 2019-2021 ;
- Le projet de lignes directrices relatives à l'utilisation du Programme mondial cybersécurité, établi par l'Union internationale des télécommunications ;
- Les résolutions de l'Assemblée générale sur le droit au respect de la vie privée à l'ère du numérique ;

- Les résolutions du Conseil des droits de l'homme sur la promotion, la protection et l'exercice des droits humains sur Internet.

Actes de cybercriminalité/comportements criminels à prendre en considération

Le Gouvernement mexicain est d'avis que la convention devrait accorder une large place aux actes que le droit international considère comme illicites (selon les termes des autres instruments adoptés sous l'égide de l'ONU) et qui sont commis par des moyens électroniques.

Si l'on ne s'attend pas que la convention comporte une liste exhaustive d'infractions, ni que toutes les typologies soient compatibles avec les différents systèmes juridiques, il est souhaitable qu'un dialogue soit engagé dans le cadre du processus de rédaction pour servir de référence générale sur les aspects suivants :

- Vol et usurpation d'identité ;
- Fraude et extorsion ;
- Utilisation de logiciels rançonneurs ;
- Logiciels malveillants et comportements criminels liés à la production, au stockage, à la distribution, à la vente et à l'exécution de codes malveillants ;
- Divulgation au détriment de leurs propriétaires de renseignements à caractère privé ou institutionnel ;
- Infractions liées à la traite des personnes, à la pédopornographie et à la violation de l'intimité sexuelle ;
- Sollicitation d'enfants sur Internet à des fins sexuelles (« grooming ») et harcèlement en ligne ;
- Violence numérique, y compris la violence sexiste et la violence fondée sur la haine, la race, la nationalité, la religion ou l'hostilité politique ;
- Méthodes d'attaque (hameçonnage, notamment par courriel, téléphone, message vocal ou SMS, ou encore technique du dévoiement) ;
- Atteintes à la souveraineté nationale, dont le terrorisme, le sabotage, l'espionnage et l'intrusion dans des systèmes contenant des renseignements classés pour des raisons de sécurité nationale ;
- Actes criminels visant les infrastructures d'information critiques, et la confidentialité, l'intégrité et l'accessibilité des informations ;
- Délits contre les enfants et les adolescents ;
- Atteintes à la liberté d'expression ;
- Atteintes à la propriété intellectuelle ;
- Délits contre le système financier ;
- Vente illicite d'armes, d'animaux, de médicaments placés sous contrôle et de médicaments ne bénéficiant pas d'autorisation de mise sur le marché ;
- Contrefaçon de monnaie et falsification de documents officiels ;
- Utilisation de cryptomonnaies et de biens à double usage à des fins criminelles ;
- Modification illicite de sites Internet (« défiguration ») ;
- Responsabilité des personnes morales.

Il serait aussi opportun d'examiner, au moment de rédiger la convention, si la tentative doit être sanctionnée et si certains éléments doivent être considérés comme des circonstances aggravantes donnant lieu à des peines plus lourdes.

Aspects concernant la souveraineté et la compétence

- Réaffirmer les principes de respect de la souveraineté nationale et de non-ingérence dans les affaires intérieures des États.
- Établir d'après quelles règles générales la compétence sera déterminée, en s'inspirant des dispositions analogues d'autres instruments juridiques et processus.
- Formuler des mesures communes pour l'obtention des données de trafic et de contenu, visant également à prévenir l'interception ou le blocage illicites des données.
- Favoriser des mécanismes permettant de garantir l'obtention, l'enregistrement et la conservation des preuves numériques, ainsi que leur communication.
- Apporter des précisions s'agissant de mesures d'enquête comme la citation à comparaître ou l'arrestation.
- Définir des spécifications en ce qui concerne la communication des données techniques et des données de contenu dans le cadre des enquêtes criminelles, et la divulgation rapide des données informatiques.
- Aborder la question des obligations légales qui incombent aux opérateurs technologiques et aux prestataires de services et de contenu sur Internet en ce qui concerne la communication de renseignements aux autorités compétentes pendant une enquête indépendamment du lieu où ils se trouvent.

Aspects concernant l'échange de renseignements et la coopération internationale

Le Gouvernement mexicain est d'avis qu'un des objectifs principaux de la convention devrait être de créer un cadre sûr pour l'échange de renseignements et la coopération internationale et d'établir des procédures efficaces à cette fin. Il compte que les questions ci-après seront notamment abordées :

- Entraide judiciaire ;
- Extradition ;
- Mécanismes communs pour la demande, l'envoi, la réception et l'échange d'informations dans le cadre d'enquêtes ou pour les besoins du renseignement.
- Procédures de contrôle judiciaire propres à assurer une collaboration souple et efficace dans les enquêtes ;
- Coopération dans la conduite des enquêtes de police et l'obtention de témoignages aux fins de procédures judiciaires, en tenant compte de la possibilité d'utiliser aussi les technologies de l'information et des communications à cette fin ;
- Élaboration de guides, de normes, de méthodes et de bonnes pratiques pour la prévention des actes de cybercriminalité et la conduite d'enquêtes sur ceux-ci ;
- Promotion, dans un but de prévention de la cybercriminalité, de la collaboration entre les équipes nationales d'intervention informatique d'urgence ou d'intervention en cas d'atteinte à la sécurité informatique ;
- Coordination des enquêtes ;
- Recommandation d'un cadre commun minimum de protection de l'information et de transparence, de sorte que l'échange des données sur les enquêtes et les procédures judiciaires soit possible, malgré les différences entre les politiques de chaque État ;
- Fixation de délais minimums pour la conservation des données et la préservation des preuves numériques ;

- Recommandation de règles et de conditions auxquelles devront se conformer l'interception des communications privées et la géolocalisation en temps réel ;
- Définition de critères généraux concernant l'observation et la réglementation des politiques de respect de la vie privée ;
- Promotion de l'uniformisation des statistiques locales, régionales et mondiales.

Aspects relatifs à la protection et à l'exercice des droits humains

Toutes les mesures découlant de la future convention devront être compatibles avec les obligations consacrées par les instruments internationaux relatifs aux droits humains. Les dispositions de la convention devront être compatibles également avec les normes relatives à la liberté d'expression.

Le Gouvernement mexicain compte que les points ci-après seront abordés pendant le processus d'élaboration :

- Question des entreprises et des droits humains ;
- Importance de privilégier les enquêtes, poursuites et sanctions en rapport avec la violence sexiste et les délits contre les enfants et les adolescents sur Internet ;
- Importance de promouvoir les enquêtes, poursuites et sanctions en rapport avec les comportements racistes qui incitent à la violence, à l'exclusion ou à la ségrégation ;
- Éléments communs minimums sur la neutralité d'Internet ;
- Recommandation de mécanismes concernant la protection de l'information par les entreprises de services sur Internet.

Éléments relatifs au renforcement des capacités et à l'assistance technique

Le Gouvernement mexicain estime que pour appliquer efficacement la convention future, il sera nécessaire de prévoir des dispositions qui favorisent le renforcement des capacités, en ce qui concerne tant la prévention de la cybercriminalité que sa répression. Il serait souhaitable :

- De promouvoir des initiatives de formation, d'assistance technique et d'échange de bonnes pratiques, ainsi que des procédures normalisées pour la conduite des enquêtes de criminalistique informatique et l'obtention de preuves numériques valables ;
- De promouvoir des initiatives éducatives axées sur la prévention et des campagnes transposables de sensibilisation du public ;
- De promouvoir aussi la création d'équipes d'intervention informatique d'urgence dans les secteurs notamment financier, universitaire, commercial et énergétique, ou le renforcement de ces équipes quand elles existent ;
- D'élaborer des guides, lignes directrices ou recommandations pour inciter à adopter des bonnes pratiques ;
- Élargir la gamme des activités de formation pour l'adapter aux différents publics concernés : enquêteurs, procureurs, juges, diplomates, parlementaires et acteurs non étatiques.

Aspects intéressant la participation des acteurs non étatiques concernés (société civile, secteur privé, milieux universitaires)

Le Gouvernement mexicain juge souhaitable que l'on prévoie, dès l'étape de l'élaboration de la convention, des mécanismes destinés à faciliter la participation et la contribution des organisations de la société civile, du secteur privé, des prestataires de services, et des milieux universitaires et de recherche. Il serait souhaitable de tenir compte des aspects suivants :

- Le rôle possible de ces acteurs dans la prévention de la cybercriminalité et la lutte contre ce phénomène ;
- La promotion de cadres de collaboration avec des équipes privées d'intervention informatique d'urgence, des opérateurs et diverses entreprises de télécommunications ;
- Le dialogue avec les entreprises privées qui exploitent des infrastructures d'information critiques ou sont présentes dans des secteurs stratégiques, ainsi qu'avec les entreprises assurant des services Internet gratuits comme le courrier électronique, la messagerie instantanée, les microblogs et les services de transport en ligne ;
- L'appui à des mesures d'autorégulation et de sensibilisation de la société, ainsi que la promotion de la question des entreprises et des droits humains.

Nigéria

[Original : anglais]
[5 novembre 2021]

Le Nigéria estime que, pour répondre efficacement à l'évolution rapide des menaces liées à la cybercriminalité, il est urgent de définir et de sanctionner les actes criminels commis dans le cyberespace, d'améliorer la synergie entre les moyens de répression au niveau transnational, d'améliorer les outils de procédure et de réformer et/ou renforcer la coopération internationale, dans le respect des droits humains. Ainsi, l'élaboration d'une convention des Nations Unies sur le sujet doit se centrer pour le moment sur la lutte contre la cybercriminalité, et ne pas tenter de couvrir la cybersécurité et d'autres questions liées au cyberespace qui sont politiquement sensibles et qu'il est préférable de traiter dans d'autres instances de l'ONU. Il est impératif que la négociation soit un processus transparent, inclusif et consensuel, qui favorise une plus large acceptation et/ou adoption de la convention qui en résultera.

Champ d'application

La nouvelle convention devrait établir un cadre juridique et institutionnel de lutte contre la cybercriminalité comportant les éléments suivants :

a) Des dispositions matérielles pour incriminer les actes commis dans le cyberespace : définir les infractions cyberdépendantes, soit celles qui ciblent des ordinateurs ou des données, certaines infractions facilitées par Internet, ainsi que le blanchiment du produit de la cybercriminalité, et prévoir les sanctions correspondantes ;

b) Des dispositions sur les pouvoirs procéduraux pour les enquêtes et les poursuites visant les infractions ainsi établies, ainsi que pour l'obtention et la communication de preuves électroniques concernant d'autres infractions pénales ;

c) Des dispositions ou des mesures permettant d'assurer durablement un renforcement des capacités et une assistance technique ;

d) Des dispositions ou des mesures pour le recouvrement du produit de la cybercriminalité, et la restitution de celui-ci ;

e) Des dispositions ou des mesures tendant à améliorer la collaboration et la coordination entre les services de détection et de répression et le secteur privé ;

f) Des dispositions ou des mesures visant à renforcer la coopération internationale en ce qui concerne les questions précitées, y compris la coopération directe avec les fournisseurs de services Internet ; et

g) Des dispositions ou des mesures visant à prévenir la cybercriminalité et à renforcer la sensibilisation, y compris en coopérant avec les organisations de la

société civile, le secteur privé, les fournisseurs de services, les universités et les centres de recherche.

Objectifs

La nouvelle convention devrait avoir les objectifs suivants :

a) Parvenir à une communauté de vues sur les règles de base à établir en ce qui concerne les infractions de cybercriminalité proprement dites, les pouvoirs procéduraux et la coopération internationale en matière de lutte contre la cybercriminalité ;

b) Promouvoir une incrimination technologiquement neutre des actes en question, de sorte que les dispositions de droit pénal matériel ne couvrent pas seulement les technologies et les procédés criminels d'aujourd'hui, mais aussi ceux qui pourraient être utilisés à l'avenir ;

c) Mettre en place les autorités et les capacités nécessaires à la collecte, l'obtention et la communication des preuves électroniques des actes de cybercriminalité et autres infractions, de façon compatible avec les garanties d'une procédure régulière et la protection des droits humains et des libertés fondamentales ;

d) Promouvoir et faciliter la coopération internationale en matière de lutte contre la cybercriminalité et priver les cybercriminels de tout sanctuaire ;

e) Promouvoir le renforcement des capacités et l'assistance technique afin de doter les services de détection et de répression de moyens plus importants pour lutter contre la cybercriminalité, ainsi que l'utilisation de moyens institutionnels existants, tels que les bases de données de l'Organisation internationale de police criminelle (INTERPOL) ;

f) Encourager les États Membres à utiliser des instruments multilatéraux qui ont déjà fait leurs preuves en matière de lutte contre la cybercriminalité, tels que la Convention du Conseil de l'Europe sur la cybercriminalité, et tenir compte des liens avec les traités des Nations Unies existant dans le domaine de la prévention du crime et de la justice pénale, en particulier la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention des Nations Unies contre la corruption ;

g) Promouvoir, au niveau des praticiens, des processus intergouvernementaux et multipartites pour la mise en commun de renseignements fiables afin de dégager les tendances et menaces futures, et les mesures d'atténuation possibles, en matière de cybercriminalité ; et

h) Établir un mécanisme pour suivre et/ou faciliter l'utilisation et l'application efficaces de la convention, pour promouvoir l'échange de renseignements et pour examiner d'éventuels révisions et/ou amendements futurs.

Structure

Il serait important que la structure de la nouvelle convention, outre le préambule, des définitions précises et des dispositions finales appropriées, comporte les éléments ci-après :

a) Des dispositions générales et/ou des objectifs et leurs modalités d'application ;

b) Des mesures de prévention de la cybercriminalité, analogues à celles qui figurent dans la Convention contre la criminalité organisée et la Convention contre la corruption, par exemple des dispositions portant sur des initiatives de sensibilisation et d'éducation ;

c) Des dispositions de droit pénal matériel concernant les infractions de cybercriminalité et les peines correspondantes ;

d) Des dispositions de droit procédural et des pouvoirs d'enquête généraux ;

e) Des garanties pour veiller à ce que, dans leurs activités, les services de détection et de répression observent les normes internationales relatives aux droits humains ;

f) Des dispositions sur la coopération internationale en matière de lutte contre la cybercriminalité, notamment la coopération internationale de caractère formel ou informel pour ce qui est de détecter la cybercriminalité, d'enquêter sur celle-ci et d'en poursuivre les auteurs, ainsi que d'obtenir les preuves électroniques d'autres infractions pénales ;

g) Des dispositions concernant le renforcement des capacités et l'assistance technique afin d'améliorer les compétences des praticiens et de renforcer les moyens de lutte contre la cybercriminalité ;

h) Des dispositions concernant la collaboration multipartite au niveau des praticiens pour l'échange de renseignements et de données d'expérience fiables avec les acteurs concernés ;

i) Des dispositions instituant un mécanisme pour suivre et/ou faciliter l'utilisation et l'application efficaces de la convention, pour promouvoir l'échange de renseignements et pour examiner d'éventuels révisions et/ou amendements futurs.

Norvège

[Original : anglais]
[3 novembre 2021]

Le Gouvernement du Royaume de Norvège est heureux de répondre à l'invitation faite aux États Membres de présenter leurs vues sur le champ d'application, les objectifs et la structure de la nouvelle convention sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, eu égard aux résolutions 74/247 et 75/282 de l'Assemblée générale. La coopération internationale est indispensable pour répondre à la menace toujours grandissante que représente la cybercriminalité, et le Gouvernement norvégien se réjouit à la perspective de participer à des négociations sur une convention générale en la matière.

Champ d'application

Dans sa résolution 74/247, l'Assemblée générale 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. Comme la résolution vise clairement les comportements criminels, l'incrimination des principaux actes commis dans le cyberespace devrait occuper une place centrale dans la convention.

Les questions de cybersécurité et de cybergouvernance n'entrent pas dans le cadre du mandat défini par l'Assemblée générale et ne devraient pas être le sujet de la convention. Ces questions relèvent d'autres instances et processus du système des Nations Unies. Il sera plus difficile d'élaborer un instrument capable de susciter une large adhésion si l'on tente d'y faire figurer des dispositions relatives à la cybersécurité et à la cybergouvernance.

Voici déjà plusieurs décennies que la cybercriminalité est une menace ; et le fait que ceux qui s'y livrent aient souvent une longueur d'avance sur les services nationaux de détection et de répression est un problème persistant. La cybercriminalité de demain ne sera pas identique à celle d'aujourd'hui, et la révolution numérique actuelle place la communauté internationale des États devant une tâche immense. À cet égard, il est de la plus haute importance que l'on tente de parvenir à une liste moderne et actuelle d'infractions qui soit à l'épreuve du temps.

Si la cybercriminalité évolue chaque jour, les autorités nationales et internationales sont parvenues à dégager des types fondamentaux et récurrents de comportement. Ces comportements sont déjà incriminés dans de nombreux États Membres à l'heure actuelle. À cet égard, le Gouvernement du Royaume de Norvège souhaiterait recommander de prendre en considération, au minimum, les infractions cyberdépendantes et infractions facilitées par Internet ci-après :

a) L'accès illégal, soit le fait d'accéder à un ordinateur ou un système informatique sans autorisation ;

b) L'interception illégale, soit le fait d'intercepter illégalement en temps réel le contenu de communications ou des données de trafic liées à des communications ;

c) Les atteintes à l'intégrité de données ou de systèmes, soit les logiciels malveillants, les attaques par déni de service, les logiciels rançonneurs, et la suppression ou la modification de données ;

d) L'abus de dispositifs, soit le trafic ou l'utilisation de données de cartes de crédit, de mots de passe et de données à caractère personnel permettant l'accès à certaines ressources ;

e) Les infractions liées aux contenus montrant des actes d'abus sexuels sur enfants ;

f) Les infractions liées à la fraude facilitée par l'informatique, soit le fait de manipuler des systèmes ou des données informatiques dans un but frauduleux tel que l'hameçonnage, la compromission de courriers électroniques professionnels et la fraude aux enchères ;

g) Les infractions liées aux atteintes au droit d'auteur et aux droits voisins.

La convention devrait également inclure des dispositions sur la tentative, la complicité et l'entente délictueuse, le blanchiment du produit de la cybercriminalité, et la responsabilité des sociétés et autres personnes morales.

Étant donné que la cybercriminalité ne cesse d'évoluer, il importe que le Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles centre son attention sur les rapports les plus récents que publient les services nationaux de détection et de répression, et les rapports équivalents émanant des organisations régionales et internationales. L'étude approfondie que l'Office des Nations Unies contre la drogue et le crime consacre à la cybercriminalité est importante. Le Gouvernement du Royaume de Norvège souhaite aussi attirer l'attention sur l'évaluation annuelle de la menace que représente la criminalité organisée sur Internet, publiée par l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), qui constitue une source importante de renseignements concernant les principaux types de cybercriminalité.

Outre les dispositions sur l'incrimination, la convention devrait aussi prévoir des dispositions sur les pouvoirs procéduraux, en particulier des dispositions sur la collecte et la communication des preuves électroniques. Il est important que ces dispositions soient compatibles avec les garanties d'une procédure régulière et la protection des droits humains et des libertés fondamentales.

Face au problème de la cybercriminalité moderne, la convention devrait exiger des États Membres qu'ils prévoient des dispositions nationales concernant spécifiquement les preuves électroniques, telles que des règles pour la conservation rapide de données informatiques stockées, la perquisition et la saisie de données informatiques stockées et la collecte en temps réel de données informatiques de trafic et de contenu dans le cas d'infractions graves. En outre, la convention devrait permettre la coopération pour la collecte et l'obtention de preuves électroniques pour tout type d'infractions, et non pas uniquement pour les actes de cybercriminalité.

En particulier, le Comité spécial devrait envisager des dispositions concernant l'obtention de preuves électroniques dans ce qu'il est convenu d'appeler le « nuage ».

Ces dix dernières années, le stockage de données informatiques dans le nuage a régulièrement posé des difficultés aux services nationaux de détection et de répression, en particulier du fait de questions de compétence et de la dépendance à l'égard d'autres États. Une convention moderne et à jour sur la cybercriminalité devrait donc indiquer de quelle façon les États Membres peuvent coopérer s'agissant de l'obtention des preuves stockées sur le nuage dans d'autres États.

Il est nécessaire également de prévoir dans la convention des dispositions sur la coopération internationale. À cet égard, le Comité spécial devrait s'inspirer de l'expérience de traités existants, en particulier la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention des Nations Unies contre la corruption. Les dispositions en matière d'extradition et d'entraide seraient à prendre en considération.

Il est aussi important que la convention tienne compte des moyens différents dont les États Membres disposent pour se conformer aux dispositions envisagées, en particulier celles qui concernent les infrastructures et capacités techniques. Ainsi, la convention devrait établir des instruments pour le renforcement des capacités et définir les moyens par lesquels les États Membres peuvent demander cette assistance.

Enfin, la convention devrait mentionner comment les citoyens, les entreprises, les organisations et d'autres parties prenantes peuvent collaborer avec les gouvernements pour se protéger eux-mêmes et protéger la collectivité face à la cybercriminalité. Bien que la cybersécurité ne relève pas du champ d'application de la convention, la prévention de la cybercriminalité joue naturellement un rôle et devrait être prise en considération.

Objectifs

Le Comité spécial devrait aspirer à créer une convention robuste qui demande aux États Membres d'adopter des lois nationales visant à améliorer la prévention et le traitement de la cybercriminalité à l'échelle mondiale. Des dispositions nationales sur l'incrimination de certains types d'actes commis dans le cyberespace, ainsi que des dispositions sur les pouvoirs procéduraux et la coopération internationale, auront un rôle particulièrement important à jouer.

Le processus de rédaction à venir devrait avoir pour but de créer un instrument qui soit à l'épreuve du temps et prenne en considération toutes les formes modernes de cybercriminalité, ainsi que les tendances à venir les plus probables. L'objectif devrait aussi être de rédiger un instrument ambitieux apportant les réponses voulues aux grands problèmes de cybercriminalité. En même temps, une démarche consensuelle est indispensable.

Le Gouvernement du Royaume de Norvège tient aussi à rappeler qu'il importe d'assurer un processus ouvert, inclusif, transparent et multipartite qui permette à tous les États Membres de négocier de bonne foi en vue de solutions pratiques et éclairées, ce qui est à notre avis fondamental si l'on veut que la nouvelle convention recueille une large adhésion.

Structure

Au vu des propositions relatives au champ d'application et aux objectifs de la convention, on peut estimer que les parties principales de l'instrument sont acquises. Néanmoins, le Comité spécial et les États Membres ont tout intérêt à continuer de faire preuve d'ouverture d'esprit concernant la structure de la convention. Si les dispositions relatives à l'incrimination, aux pouvoirs procéduraux et à la coopération internationale devraient constituer les principaux éléments de la convention, d'autres aspects peuvent aussi en influencer la structure finale. Le Gouvernement du Royaume de Norvège recommande de faire preuve d'ouverture en ce qui concerne la structure de la convention.

Droits humains

Le droit international des droits de l'homme s'applique aux activités sur Internet au même titre qu'à toute autre activité. Les États doivent se conformer à leurs obligations en matière de droits humains dans le cyberespace au même titre que dans le monde physique. Les États sont tenus de respecter et de protéger les droits humains, y compris le droit à la liberté d'expression et le droit au respect de la vie privée, ainsi que les autres principes utiles à la protection des données.

Il va de soi que les normes relatives aux droits humains consacrées par le Pacte international relatif aux droits civils et politiques constituent un cadre important pour l'élaboration de toute nouvelle disposition sur la cybercriminalité. Au demeurant, le Gouvernement du Royaume de Norvège tient à rappeler l'importance des droits humains dans les négociations à venir, particulièrement en ce qui concerne les dispositions qui nécessitent des lois nationales sur les pouvoirs procéduraux.

Nouvelle-Zélande

[Original : anglais]
[29 octobre 2021]

La Nouvelle-Zélande est heureuse de répondre à l'invitation, faite aux États Membres par la Présidente du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, de présenter leurs vues sur le champ d'application, les objectifs et la structure de la nouvelle convention, eu égard aux résolutions 74/247 et 75/282 de l'Assemblée générale. La Nouvelle-Zélande se réjouit de la possibilité qui lui est donnée de communiquer ses vues et attend avec intérêt de prendre connaissance des contributions des autres pays et de pouvoir débattre de la voie à suivre dans le cadre des travaux qui seront menés de façon transparente et inclusive pour élaborer la nouvelle convention.

La cybercriminalité est un problème transfrontière. Une coopération internationale fondée sur une approche inclusive et multipartite est donc indispensable si l'on veut que la communauté internationale soit capable de lutter efficacement contre cette menace de plus en plus grave. La coopération internationale sur les questions relatives à la cybercriminalité nécessite des lois cohérentes et efficaces en la matière, qui permettent d'enquêter sur la cybercriminalité et d'en poursuivre les auteurs au niveau international. Faciliter cette coopération n'a jamais été aussi important. Alors que le travail, les activités de recherche et les relations sociales se sont dématérialisés, y compris tout au long de la pandémie de maladie à coronavirus (COVID-19), les cybercriminels ont vu leur rayon d'action s'élargir et l'on a assisté à une augmentation des cas de cybercriminalité, aussi bien en fréquence qu'en gravité.

La coopération internationale en matière de cybercriminalité est d'une importance décisive pour les petits États insulaires en développement et il est impératif que ces pays soient en mesure de prendre véritablement part aux travaux du Comité spécial. La Nouvelle-Zélande est résolue à faire en sorte que les pays insulaires du Pacifique soient en mesure de participer véritablement aux travaux du Comité spécial. Nous sommes favorables à une participation hybride (en présentiel et en ligne) aux réunions du Comité spécial et soulignons qu'il importe de ménager aux petites délégations le temps nécessaire à une préparation et une participation efficaces.

Champ d'application

La nouvelle convention sur la cybercriminalité doit compléter les instruments existants et ne pas être incompatible avec eux. Tous les États Membres conviennent que le droit international s'applique au cyberespace, ce qui signifie que la nouvelle

convention n'existera pas dans le vide. Elle sera vraiment efficace si elle complète et renforce les instruments en vigueur et le régime juridique actuel, constitué d'outils de lutte contre la cybercriminalité comme la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention du Conseil de l'Europe sur la cybercriminalité. C'est ce que prévoit le mandat défini par l'Assemblée générale dans sa résolution 74/247, où l'Assemblée a demandé que les travaux du Comité spécial tiennent pleinement compte des instruments internationaux existants et des initiatives déjà prises en la matière aux niveaux national, régional et international.

Pour la Nouvelle-Zélande, il est essentiel que tout instrument devant être élaboré protège les droits humains et reconnaisse un cyberespace libre et ouvert qui soit régi par de multiples parties prenantes. La convention sur la cybercriminalité doit donc être compatible avec l'obligation qu'ont les États de protéger et de respecter les droits humains en ligne, y compris le droit à la liberté d'expression et le droit de ne pas subir d'immixtions arbitraires ou illégales dans sa vie privée. Les mesures de lutte contre la cybercriminalité doivent être conformes au droit international des droits de l'homme.

Le traité devrait se concentrer avant tout sur les grands problèmes de cybercriminalité afin que l'on puisse coopérer plus efficacement face à la menace qu'ils représentent pour les individus, les entreprises et les États. Nous estimons que le traité devrait recouvrir les infractions cyberdépendantes, ainsi que les infractions facilitées par Internet, uniquement lorsque l'emploi des technologies de l'information et des communications en accroît la portée, la rapidité et l'ampleur. Nous estimons qu'il existe deux candidats évidents pour cette catégorie d'infractions : l'exploitation et les abus sexuels dont les enfants sont victimes en ligne, de même que la fraude et le vol facilités par Internet, y compris l'utilisation de logiciels rançonneurs.

La Nouvelle-Zélande ne pense pas qu'il soit nécessaire de traiter des infractions qui sont déjà couvertes par d'autres instruments juridiques, comme la corruption, le trafic, la traite ou le terrorisme, au seul motif qu'elles peuvent être commises à l'aide de technologies de l'information et des communications. On risque en effet la contradiction et la confusion en suivant une telle approche, qui n'est pas le bon moyen pour élaborer un instrument ciblé et pratique capable d'améliorer notre capacité collective de lutter contre la cybercriminalité.

Le mandat relatif à ce processus indique clairement que nous devons nous attacher à mettre au point un instrument de justice pénale afin d'améliorer la riposte internationale à la cybercriminalité, grâce à l'intervention des services nationaux de détection et de répression. Dans cette optique, il est nécessaire de définir et de sanctionner les comportements criminels dans le cyberespace, et les États doivent appliquer les processus appropriés et les outils législatifs qui permettent à ces services d'avoir accès aux preuves numériques et d'échanger celles-ci afin de pouvoir réprimer et sanctionner efficacement les actes criminels commis dans le cyberespace. Il n'est pas nécessaire de définir des normes pour les comportements non criminels en ligne. Nous estimons utile de tirer les enseignements d'autres traités de justice pénale qui ont donné de bons résultats en ce qu'ils mettent l'accent sur les questions pénales fondamentales, ainsi que sur des dispositions étendues en matière de coopération internationale et des mesures d'appui visant à renforcer les capacités dans tous les États Membres.

Autant que possible, le libellé de la convention qui verra finalement le jour devra être pragmatique, technologiquement neutre et non marqué temporellement afin qu'il résiste à l'épreuve du temps et ne demande pas des révisions fréquentes. Dès lors, l'accent devra porter sur les actes plutôt que sur la forme ou la méthode particulière utilisée pour s'y livrer.

Il serait prématuré à ce stade de définir le mécanisme d'application qui serait requis pour cette convention. Il existe un grand nombre de modèles à envisager, mais cet aspect du traité peut être laissé de côté jusqu'à ce que soient définis plus précisément le champ d'application et les objectifs.

Objectifs

Le nouvel instrument devrait avoir pour objectif premier d'établir un cadre mondial harmonisé, moderne et efficace de coopération et de coordination entre les États pour qu'ils s'attaquent à la menace croissante que la cybercriminalité représente pour les particuliers, les entreprises, les infrastructures essentielles et les gouvernements. Il devrait prévoir la fourniture d'un soutien et d'une assistance technique afin que tous les États puissent acquérir les capacités et les moyens de faire face à ces problèmes. Les États seront ainsi mieux à même de réagir efficacement à la cybercriminalité aux échelons national, régional et international.

Le traité doit donc favoriser la coopération entre les services de détection et de répression, les autorités de poursuites et les instances judiciaires de chaque pays, au niveau bilatéral ou multilatéral, en matière de prévention, d'enquêtes et de poursuites s'agissant des infractions visées par le traité. C'est un aspect déterminant pour lutter contre la cybercriminalité, étant donné que, 'en raison de son caractère transfrontière, celle-ci met souvent en présence des auteurs et des victimes qui se trouvent dans plusieurs pays. Une conception commune des actes qui constituent des infractions pénales dans le contexte du cyberespace et des infractions qu'il convient de réprimer dans le cadre du droit national sera utile à cet égard, particulièrement si on la complète par des cadres cohérents pour l'accès aux preuves numériques et la communication de celles-ci à des partenaires internationaux, moyennant les garanties appropriées.

L'utilisation de pouvoirs d'enquête et de poursuites eu égard aux infractions prévues dans le traité doit être assujettie à des garanties efficaces en matière de droits humains et de libertés fondamentales, conformément aux instruments internationaux en vigueur. Des garanties doivent aussi être en place pour faire en sorte que les pouvoirs de coopération mutuelle soient utilisés équitablement et à bon escient, et permettre aux États de refuser la coopération lorsque certaines garanties ne sont pas respectées. En outre, la Nouvelle-Zélande estime que le traité doit reconnaître l'indépendance des services de détection et de répression et des autorités de poursuites de chaque pays, et que la décision d'engager telle ou telle action doit être du seul ressort de ces services et autorités dans chaque État Membre.

Un instrument recueillant une large adhésion est le meilleur gage d'une coopération internationale efficace. La Nouvelle-Zélande estime que, à cet égard, les négociations relatives à la convention doivent être inclusives et transparentes et que tout doit être mis en œuvre pour parvenir à un consensus, de manière à garantir à la convention un mandat aussi solide que possible. Tous les États Membres doivent pouvoir faire part de leurs vues et avoir la possibilité de participer véritablement à des négociations éclairées par les compétences spécialisées et le point de vue de la société civile, du secteur privé et des autres parties concernées. Le point de vue des peuples autochtones, y compris les Maoris d'Aotearoa-Nouvelle-Zélande, ainsi que d'autres groupes minoritaires, devrait être pris en considération, de même que les conséquences possibles de la cybercriminalité et de la répression de celle-ci sur les groupes en question.

La coopération internationale en matière de lutte contre la cybercriminalité n'est pas aussi efficace qu'elle pourrait l'être. Cela ne tient pas à un manque de volonté des États Membres, mais plutôt à un manque de moyens ou de compétences. L'assistance technique aux services de détection et de répression et le renforcement de leurs capacités sont indispensables et la convention doit favoriser l'amélioration des capacités et des moyens partout dans le monde.

Structure

Nous attendons avec intérêt de prendre connaissance des vues des autres États concernant le champ d'application et les objectifs de la convention à l'occasion du processus en cours, et à la première session de négociation en janvier 2022. Après cette étape, nous comptons que des orientations précises se dégageront rapidement quant à la structure de la convention.

Oman

[Original : arabe]
[18 octobre 2021]

Les attaques contre des installations civiles, en particulier les infrastructures vitales – dont les réseaux d'électricité et d'eau, les institutions financières et le secteur des transports – devraient être reconnues comme des infractions pénales Ces installations ne devraient pas devenir le théâtre de conflits entre pays et de règlements de comptes.

Panama

[Original : espagnol]
[28 octobre 2021]

Du fait de l'évolution constante de la technologie, les États doivent adopter des mécanismes visant à prévenir et à combattre les nouvelles formes de criminalité. La pandémie de COVID-19 n'a fait qu'aggraver un problème déjà bien réel : nous ne sommes pas suffisamment préparés à lutter contre la cybercriminalité et les infractions commises à l'aide de moyens technologiques.

Être prêt à livrer cette bataille implique, entre autres, de bien comprendre qu'il est impossible d'enquêter sur la cybercriminalité et les infractions commises par des moyens informatiques sans tenir compte de la dimension internationale du phénomène. Tous les États sont concernés par les activités criminelles de ceux qui prospèrent sur le terreau du transnationalisme, où ils peuvent réaliser leurs objectifs et échapper aux conséquences de leurs actes.

Au vu de ces éléments, la convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles devrait servir d'outil pour faciliter les enquêtes menées par les États. Dans cette optique, il est essentiel que la convention couvre non seulement les agissements qui affectent directement l'information, les systèmes informatiques et la technologie proprement dite, mais aussi ceux commis par des moyens technologiques, quel que soit le droit légalement protégé.

Selon nous, ce nouvel outil devrait prévoir des mesures visant à renforcer les systèmes de communication formelle et informelle entre les États pour que les enquêtes soient plus efficaces, compte tenu de la volatilité de l'information.

Parallèlement au renforcement des systèmes de communication, il conviendrait d'examiner les concepts juridiques qui encadrent des mesures d'enquête telles que la saisie de données et de la correspondance, la conservation des données et le traitement des preuves électroniques.

Nous sommes conscients qu'il peut y avoir des divergences de vues sur certains points, mais cela ne change rien à l'objectif, qui est de créer un instrument qui contribue à la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

République dominicaine

[Original : espagnol]
[5 novembre 2021]

La République dominicaine se félicite de l'occasion qui lui est donnée de prendre part, avec l'ensemble des États Membres, à cet exercice collectif destiné à leur permettre de présenter des observations sur le champ d'application, les objectifs et la structure d'un nouvel instrument international relatif à la cybercriminalité,

conformément aux résolutions 74/247 et 75/282 de l'Assemblée générale, respectivement en date du 27 décembre 2019 et du 26 mai 2021.

La cybercriminalité est une forme émergente de criminalité transnationale dont l'expansion est l'une des plus rapides dans le monde. Son essor est étroitement lié à l'évolution et au développement exponentiel des technologies de l'information et des communications et elle touche chaque année des millions de citoyens et d'entreprises.

Notre région, l'Amérique latine et les Caraïbes, est particulièrement touchée par ce phénomène. Les pays en développement sont dépourvus dans une large mesure des capacités nécessaires pour combattre la cybercriminalité, ce qui se traduit directement par un nombre élevé de victimes recensées.

De même, la récente pandémie de maladie à coronavirus 2019 (COVID-19) a mis en lumière la vulnérabilité de la communauté internationale face à la cybercriminalité, situation qui confirme combien il importe de mener une action mondiale fondée sur la collaboration et la coordination, non seulement entre les États Membres, mais aussi entre les gouvernements et les organisations non gouvernementales, la société civile, le milieu universitaire et le secteur privé. En effet, la complexité et l'ampleur de la cybercriminalité sont telles que toute action doit reposer sur une approche multidisciplinaire si l'on entend garantir son efficacité.

La République dominicaine se joint avec enthousiasme à cette entreprise menée par la communauté internationale dans le cadre de l'Organisation des Nations Unies et réitère sa volonté d'œuvrer conjointement avec tous les États Membres à l'élaboration d'un traité international qui représente tout un chacun et qui souscrive en tous points aux principes de transparence, d'impartialité et d'inclusion.

Champ d'application

La République dominicaine estime qu'un nouvel instrument international de lutte contre la cybercriminalité devrait avant tout constituer un outil efficace permettant de prévenir et détecter les actes de cybercriminalité, d'enquêter sur ces actes et d'en poursuivre les auteurs, dans le plein respect de la vie privée, de la protection des données, des libertés civiles et des droits humains.

Un tel instrument devrait notamment faciliter la conduite des enquêtes pénales en permettant de recueillir rapidement des preuves numériques et de les utiliser ultérieurement, et de réduire ainsi l'impunité associée à ce type d'infractions, laquelle constitue l'un des principaux obstacles auxquels sont confrontés les agents des services de détection et de répression.

Cet outil devrait également promouvoir et faciliter la coopération internationale entre les États Membres, ainsi que la fourniture d'une assistance technique et la conduite d'activités de renforcement des capacités en faveur des États parties qui en ont besoin pour lutter contre la cybercriminalité.

En outre, la République dominicaine estime qu'il faudra établir clairement que le nouvel instrument international se limitera au domaine de la cybercriminalité et qu'il n'abordera pas les questions relatives à la cybersécurité et à la gouvernance de l'Internet, qui sont traitées au sein d'autres instances.

Par ailleurs, il devra être tenu compte des dispositions des instruments internationaux et régionaux existants, afin d'éviter tout conflit inutile avec les systèmes juridiques des États Membres qui ont fondé leur législation nationale sur ces instruments, ou toute entrave inutile au bon fonctionnement de ces derniers. À cet égard, il faudra tirer parti de l'expérience acquise dans la mise en œuvre de ces instruments, en relevant les points forts que la nouvelle convention pourrait compléter ainsi que les faiblesses qu'elle pourrait pallier. Il convient également de tenir compte des travaux menés par les groupes spécialisés, dont le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité.

Objectifs

Un nouvel instrument international visant à prévenir et à combattre la cybercriminalité devrait notamment poursuivre les objectifs suivants :

- Promouvoir et faciliter une coopération internationale rapide, pratique et efficace entre les États parties ;
- Traiter de la prévention, de la détection, des enquêtes et des poursuites pénales concernant les infractions de cybercriminalité auxquelles il s'applique, ainsi que de la collecte et du traitement des preuves numériques relatives à d'autres infractions, en dotant les États parties des outils nécessaires pour lutter contre cette forme de criminalité transnationale ;
- Définir clairement les types d'actes qui seront visés par les dispositions de la nouvelle convention et qui devront être considérés comme illicites dans les systèmes juridiques de tous les États parties ;
- Promouvoir et faciliter le renforcement des capacités dans les États parties qui en ont besoin afin d'empêcher la création de « paradis cybernétiques » ;
- Promouvoir l'échange des bonnes pratiques et des enseignements tirés de l'expérience ;
- Définir des règles claires permettant d'établir la compétence nécessaire pour demander aux fournisseurs « mondiaux » d'accès à Internet des preuves numériques, cette question constituant, pour l'heure, l'un des défis majeurs à relever pour lutter contre l'impunité et venir en aide aux victimes de la cybercriminalité ;
- Définir des garanties claires et prévoir des dispositions sanctionnant leur non-respect ;
- Établir des pouvoirs suffisants pour enquêter sur les infractions pénales visées, en ne perdant jamais de vue le respect de la vie privée, de la protection des données, des libertés civiles et des droits humains ;
- Compte tenu de l'évolution rapide des technologies, la convention doit adopter une vision large et à long terme ; à ce titre, elle devra employer des termes technologiquement neutres pour ne pas perdre en pertinence dans le futur en raison des avancées technologiques ;
- Définir une approche multidisciplinaire qui permette au secteur public et au secteur privé de collaborer activement entre eux.

Structure

- Définitions.
- Infractions pénales.
- Outils procéduraux pour les enquêtes.
- Garanties.
- Coopération internationale.
- Accès aux preuves numériques.
- Assistance technique et renforcement des capacités d'enquête.
- Modes opératoires normalisés.
- Mesures préventives.
- Mécanisme d'application.

Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

[Original : anglais]
[28 octobre 2021]

Champ d'application

Le Royaume-Uni estime que la nouvelle convention internationale sur la cybercriminalité devrait se concentrer sur le renforcement de la coopération face au danger grandissant que représentent les activités criminelles pour les citoyens, les entreprises et les gouvernements.

Un certain nombre de traités régionaux et internationaux sur la cybercriminalité ont déjà contribué de manière significative aux efforts déployés pour combattre la cybercriminalité. Il est important de tirer parti des acquis découlant de ces traités et de reconnaître les dispositions pertinentes contenues dans des traités de justice pénale tels que la Convention des Nations Unies contre la corruption et la Convention des Nations Unies contre la criminalité transnationale organisée.

Le champ d'application du traité devrait couvrir : a) les enquêtes sur les infractions définies dans le traité et les poursuites contre leurs auteurs ; b) le développement des capacités et des moyens permettant à tous les États Membres de lutter contre ces infractions ; et c) la reconnaissance d'un forum d'experts grâce auquel les menaces nouvelles et émergentes pourront être identifiées.

La Convention des Nations Unies sur la cybercriminalité devrait couvrir les infractions cyberdépendantes au même titre que les infractions facilitées par Internet, dont l'ampleur, la portée et la rapidité sont accrues par l'utilisation d'un ordinateur. La coopération est efficace dès lors que tous les systèmes juridiques interprètent et reconnaissent de la même manière les infractions prévues dans le traité.

Les infractions visées dans le traité ne doivent pas porter atteinte à l'exercice de la liberté d'expression ou d'opinion.

En tant que traité de droit pénal, la convention devrait se concentrer sur les actions que les autorités nationales devront entreprendre. Elle devrait également examiner comment, grâce à une approche multiparticipative, les citoyens, les organisations non gouvernementales, les organisations de la société civile, les établissements universitaires et le secteur privé peuvent travailler ensemble pour se protéger contre la cybercriminalité.

Tout traité doit prévoir de solides garanties, qui incluent le respect de la vie privée et des autres droits humains tels qu'ils sont définis dans le droit international des droits de l'homme et reconnus dans les résolutions pertinentes adoptées par l'Assemblée générale et le Conseil des droits de l'homme.

Le traité doit être élaboré de manière inclusive et transparente, dans le respect des vues de tous les États Membres et avec la participation active d'un large éventail de parties concernées, notamment d'organisations non gouvernementales, d'organisations de la société civile, d'établissements universitaires et du secteur privé. En outre, les dispositions du traité, en particulier celles relatives à la mise en œuvre et au renforcement des capacités, devraient aussi encourager une approche inclusive et transparente de la lutte contre la cybercriminalité.

Le traité devrait être formulé de manière technologiquement neutre pour résister à l'épreuve du temps et éviter des mises à jour constantes.

Il ne devrait pas faire double emploi avec des travaux qui ont déjà été effectués ou qui devraient l'être ailleurs. Il ne devrait pas aborder les questions de cybersécurité, dont s'occupe déjà la Première Commission de l'Assemblée générale, ni les questions de gouvernance d'Internet, qui sont déjà traitées dans des instances multipartites spécialisées.

Objectifs

L'objectif premier du traité devrait être de soutenir la coopération effective, bilatérale ou multilatérale, des services nationaux de détection et de répression et des organes de poursuite pour enquêter sur les infractions visées par le traité et poursuivre leurs auteurs. Si le traité est largement soutenu, la coopération internationale sera optimale.

Pour favoriser une coopération mutuelle qui soit efficace, il faut prévoir la possibilité de refuser de donner suite à une demande de coopération en l'absence de double incrimination, en cas de délit politique, notamment lorsque l'infraction présumée porte sur l'exercice de la liberté d'expression, ou en cas de demande visant à punir ou à persécuter la personne en raison de sa race, de sa religion, de son genre ou d'autres caractéristiques protégées. Il serait utile de prévoir des critères minimaux dont l'autorité requérante devrait confirmer qu'ils ont été remplis, à savoir par exemple que la demande est nécessaire, proportionnée, limitée dans le temps et autorisée à un niveau spécifique.

En ce qui concerne les infractions visées par le traité, l'utilisation de pouvoirs d'enquête et de poursuite, y compris dans les affaires bilatérales ou multilatérales, doit être soumise à des garanties effectives en matière de droits humains et de libertés fondamentales, conformément au droit international des droits de l'homme.

Le traité doit reconnaître que les services nationaux d'enquête et de poursuite sont indépendants sur le plan opérationnel et que la décision d'engager ou non une action est de leur seul ressort.

Le traité doit soutenir le développement des capacités au niveau mondial et favoriser leur renforcement.

Les menaces liées aux activités criminelles dans le cyberespace étant appelées à évoluer, le traité devrait établir un processus intergouvernemental et multipartite pour identifier les menaces futures, sans préjudice de la question de savoir si ce processus fait partie du traité.

Les femmes et les hommes n'étant pas touchés de la même manière par la cybercriminalité, le traité devrait tenir compte des questions de genre pour nous aider à lutter plus efficacement contre le phénomène. Élaborer un traité sur la cybercriminalité qui se soucie des incidences, différenciées selon le genre, de ses dispositions encouragera davantage de femmes à participer à tous les niveaux et à tous les processus. Les solutions n'en seront que plus diversifiées, plus riches et finalement meilleures. Lors de la réunion du Groupe intergouvernemental d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, en avril 2021, tous les États Membres ont convenu qu'ils devaient promouvoir, en particulier, la participation de femmes expertes.

Le traité devrait promouvoir la participation de l'ensemble de la société à la lutte contre la cybercriminalité et encourager les États Membres à collaborer avec des acteurs non gouvernementaux, notamment des experts, des entreprises et le grand public, dans des domaines tels que la sensibilisation, l'amélioration de l'éducation, la formation sur le genre et la cybercriminalité, et l'aide aux victimes.

Structure

Le Royaume-Uni estime que la structure suivante serait un moyen efficace d'organiser le traité :

a) Dispositions générales

Les dispositions générales devraient définir la base et le but de l'instrument et inclure les définitions qui seront utilisées tout au long du traité. Les définitions doivent être comprises et approuvées par toutes les parties ; elles doivent être technologiquement neutres et tenir compte de la terminologie qui est largement

approuvée dans les instruments régionaux et utilisée dans les cadres législatifs nationaux ;

b) Principales infractions

Elles doivent inclure les infractions cyberdépendantes (par exemple, l'accès illégal), accompagnées de descriptions et de définitions qui soient acceptables pour toutes les parties. Les infractions facilitées par Internet (par exemple, l'exploitation et les atteintes sexuelles visant des enfants, la fraude) doivent être prévues dès lors que l'infraction est principalement commise en ligne, que les ordinateurs changent l'échelle et la rapidité de commission de l'infraction et que les définitions de l'infraction sont comprises par toutes les parties ;

c) Droits humains et garanties

Le fonctionnement et l'application du traité doivent être fondés sur des garanties procédurales efficaces et des protections solides en matière de droits humains, et mentionner le droit international des droits de l'homme ;

d) Mesures préventives

Comme la Convention contre la corruption et la Convention contre la criminalité organisée, le traité devrait prévoir des dispositions dans lesquelles les États sont encouragés à mettre en œuvre des mesures de prévention de la cybercriminalité, notamment en travaillant avec toutes les parties prenantes concernées ;

e) Dispositions relatives au droit procédural

Les pouvoirs visant à faciliter les enquêtes et les poursuites doivent permettre aux autorités compétentes de conserver, de rechercher et de saisir des preuves électroniques dès lors que l'infraction est commise au moyen d'un ordinateur ou que les preuves en rapport avec une infraction se présentent sous forme électronique, que ce soit dans le cadre d'enquêtes nationales ou internationales ;

f) Coopération internationale

Les dispositions relatives à la coopération internationale doivent prévoir l'entraide judiciaire et l'assistance en cas d'urgence, y compris l'obligation pour les pays de mettre en place des points de contact fonctionnant 24 heures sur 24 et 7 jours sur 7. Outre l'échange d'éléments de preuve dans la pratique, les recommandations formulées par le Groupe d'experts en avril 2021 indiquent clairement que les États Membres souhaitent continuer à partager leurs expériences et leurs meilleures pratiques, ainsi que des informations sur les menaces nouvelles et grandissantes ;

g) Assistance technique et renforcement des capacités

Le renforcement des capacités devrait être encouragé – un rôle important devrait être conféré à l'Office des Nations Unies contre la drogue et le crime à cet égard – et la coordination de ces travaux devrait être assurée dans le cadre de structures existantes comme le Forum mondial sur la cyberexpertise. Le Royaume-Uni constate qu'un grand nombre de recommandations approuvées par le Groupe d'experts en avril 2021 sont axées sur le renforcement des capacités, notamment la mise en place d'une formation spécialisée et actualisée à l'intention des praticiens sur les enquêtes en matière de cybercriminalité, le traitement des preuves électroniques, la chaîne de conservation et l'analyse criminalistique ;

h) Application

L'application du traité devrait être clairement planifiée.

Suisse

[Original : anglais]
[28 octobre 2021]

Les technologies de l'information et des communications (TIC) ont eu de profondes répercussions sur notre société, mais si elles ont offert des possibilités de développement social, culturel et économique, elles ont aussi fourni une base pour la commission d'activités à des fins criminelles dans le cyberespace. La cybercriminalité se développe à mesure que la numérisation de notre société progresse. Par sa résolution 74/247, l'Assemblée générale a établi un comité intergouvernemental spécial à composition non limitée qui a 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. Dans notre réponse, nous présentons le point de vue de la Suisse sur les objectifs, le champ d'application et la structure de cet instrument.

Objectifs

Pour la Suisse, une convention des Nations Unies sur la lutte contre l'utilisation des TIC à des fins criminelles doit avoir pour objectif général de protéger les utilisateurs de ces technologies, afin qu'ils puissent s'en servir librement et profiter des avantages qu'elles présentent. Le caractère mondial et ouvert des TIC est de fait un élément moteur dans la réalisation du développement social et économique. L'objectif de la convention est donc la sécurité des utilisateurs, laquelle ne doit pas entraver leur liberté d'utiliser ces TIC. Ils doivent pouvoir exercer leurs droits humains et leurs libertés fondamentales en ligne, et réaliser ainsi le plein potentiel d'un monde numérisé inclusif. La convention devrait donc être un pas de plus pour garantir des TIC libres, fiables et sûres.

Une convention des Nations Unies peut nous aider à atteindre cet objectif global. Pour ce faire, elle devrait prévoir une approche coordonnée de la lutte contre la cybercriminalité. Les TIC étant par nature transnationales, les auteurs des actes de cybercriminalité et leurs victimes peuvent se trouver dans plusieurs pays. La coopération internationale est donc essentielle pour garantir un niveau optimal de protection contre la cybercriminalité. La convention devrait déboucher sur une conception commune de ce qui constitue une infraction pénale dans le contexte des TIC et des infractions qui devraient être réprimées par le droit national. Cette conception commune est un prérequis pour permettre quelque forme de coopération que ce soit. Partant de cette conception et terminologie communes, la convention devrait viser à créer le cadre d'une coopération internationale efficace pour protéger les utilisateurs des TIC et obtenir justice pour les victimes de cyberinfractions.

Une approche coordonnée de la lutte contre la cybercriminalité au niveau mondial passera nécessairement par un processus inclusif. Tous les États Membres devraient pouvoir participer utilement ; ils devraient avoir la possibilité de donner leurs vues sur la convention et de débattre de celles des autres lors des séances de fond du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, lequel devrait s'efforcer de parvenir à un consensus, dans toute la mesure possible.

La cybercriminalité est transnationale, mais elle implique aussi, par nature, des acteurs non étatiques. Si nous voulons que la convention soit adaptée à l'objectif visé, chaque voix doit être entendue pendant son processus d'élaboration. Pour qu'elle puisse atteindre cet objectif, il est essentiel d'inclure toutes les parties prenantes – parmi lesquelles des organisations non gouvernementales, des organisations de la

société civile, des établissements universitaires et le secteur privé – dans chacune des étapes coordonnées de son élaboration[4].

Champ d'application

Le droit international s'applique au cyberespace. La nouvelle convention n'existera pas hors de tout contexte, pas plus qu'elle ne videra les accords internationaux antérieurs de leur substance. La Suisse est convaincue que cette convention doit s'appuyer sur le régime juridique en place et le renforcer. Elle devrait être conçue de manière à compléter les initiatives que la communauté internationale a déjà prises et à s'appuyer sur les synergies pour lutter efficacement contre la cybercriminalité.

Puisque la convention sera un traité pénal, elle devrait s'appuyer sur le droit pénal international et le respecter. Des outils mondiaux de lutte contre la cybercriminalité existent déjà. Avec la Convention des Nations Unies contre la criminalité transnationale organisée, la Convention sur la cybercriminalité du Conseil de l'Europe est une norme dont les pays du monde entier, y compris la Suisse, se sont servis pour moderniser leurs lois sur la cybercriminalité. Elle constitue aussi une base importante pour la coopération internationale à l'ère d'Internet. La future convention des Nations Unies devrait tirer parti de cette expérience. Les travaux du Comité spécial devraient être guidés par ceux d'autres groupes et instances, notamment le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité.

La convention doit refléter, protéger et renforcer de manière adéquate le droit des droits humains. La cybercriminalité constituant une menace pour les droits humains, les efforts déployés pour la combattre doivent protéger ces droits et non les affaiblir. Les droits individuels protégés hors ligne doivent aussi être protégés en ligne. Les mesures prises pour lutter contre la cybercriminalité doivent être compatibles avec le droit international des droits de l'homme.

Structure

La Suisse estime que la structure des instruments de droit pénal international existants négociés dans le cadre des Nations Unies constitue une approche prometteuse et efficace pour concrétiser les objectifs mentionnés ci-dessus. La convention pourrait donc être structurée comme suit :

a) Dispositions générales ;

b) Mesures préventives ;

c) Incrimination, détection et répression ;

d) Coopération internationale.

e) Assistance technique et échange d'informations ;

f) Mécanismes d'application ;

g) Dispositions finales.

Pour la Suisse, il n'est pas nécessaire de dupliquer des infractions qui sont déjà couvertes par des traités spécifiques (la corruption, le trafic, la traite et le terrorisme, par exemple) au seul motif qu'elles peuvent (aussi) être commises à l'aide des TIC. La convention devrait plutôt être axée sur les infractions spécifiques au cyberespace. Une longue liste d'infractions, même si toutes sont susceptibles d'être commises au moyen de systèmes informatiques, comporte un risque de contradiction et devrait être évitée.

Les infractions liées au contenu devraient être ramenées au minimum et systématiquement évaluées au regard de leur valeur ajoutée.

[4] Conformément à la résolution 75/282 de l'Assemblée générale, par. 9 et 10.

La Suisse tient à souligner la nécessité et l'importance des garanties procédurales qui protègent la légalité et l'équité des procédures ainsi que les droits des personnes concernées, notamment dans le cadre de l'entraide judiciaire, de l'échange d'informations et de l'extradition aux conditions fixées par les États concernés. Le droit à la protection de la vie privée doit être pleinement garanti. Un niveau de protection adéquat des données personnelles doit être prévu.

Des conditions et garanties adaptées doivent être prévues et adoptées, notamment en ce qui concerne le maintien et le renforcement des droits humains, y compris le principe de la non-discrimination.

Turquie

[Original : anglais]
[4 novembre 2021]

La Turquie attache la plus grande importance à l'utilisation libre, ouverte et sécurisée des technologies de l'information et des communications au niveau mondial.

Le développement des technologies de l'information et des communications accroît le risque d'utilisation abusive de ces technologies à des fins criminelles. L'élimination de ce risque et des menaces contre la sécurité des infrastructures critiques et contre les droits et libertés fondamentaux doit être au premier rang des préoccupations de la communauté internationale. En raison de la nature transnationale du cyberespace, les répercussions des cyberattaques peuvent être mondiales. Seule une coopération efficace au niveau mondial permettra de réduire ces répercussions.

À cet égard, la Turquie est très attachée à une coopération internationale efficace pour que le cyberespace soit plus stable et sécurisé au niveau mondial et est disposée à apporter sa contribution au Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, et à le soutenir. C'est pourquoi nous souhaitons partager nos premières vues sur le champ d'application, les objectifs et la structure de la convention.

Plusieurs points doivent être examinés dans le cadre de la convention, à savoir :

a) Le développement de canaux de coopération efficaces entre les États ;

b) La définition claire des questions liées à l'utilisation criminelle des technologies de l'information et des communications ;

c) Le développement de canaux de communication d'urgence entre les États ;

d) Le renforcement des ressources pour la collecte et l'obtention de renseignements sur les cybermenaces ;

e) Le développement de l'échange de renseignements entre les institutions compétentes des États ;

f) L'échange d'informations dans les affaires portant sur l'utilisation criminelle des technologies de l'information et des communications.

Des mesures efficaces visant à empêcher les communications internes entre criminels ou terroristes ainsi que leurs activités de propagande devraient aussi être prévues dans la convention.

La pandémie de COVID-19 ayant considérablement accru l'utilisation des systèmes de télécommunication, nous devrions également tenir compte, dans le cadre des négociations relatives à la convention, des effets de la pandémie sur l'utilisation criminelle des technologies de l'information et des communications.

Il conviendra en outre d'examiner, dans le champ d'application de la convention, l'utilisation en toute sécurité des technologies de nouvelle génération telles que l'informatique en nuage, la 5G, la chaîne de blocs, l'Internet des objets et l'intelligence artificielle dans la lutte contre la criminalité et les cyberattaques.

Union européenne et ses États membres

[Original : anglais]
[2 novembre 2021]

Le présent document expose les vues et la position de l'Union européenne et de ses États membres[5] sur le champ d'application, les objectifs et la structure (éléments) à prendre en compte pour élaborer une nouvelle convention des Nations Unies sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et pour contribuer à la préparation de la première session du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, créé à cette fin conformément à la résolution 74/247 de l'Assemblée générale.

Cette contribution ne préjuge pas des positions futures que l'Union européenne et ses États membres pourraient adopter au cours des futures négociations sur le champ d'application, les objectifs et la structure d'une future convention des Nations Unies.

I. Objectifs

L'Union européenne et ses États membres soulignent qu'une future convention des Nations Unies devrait servir d'instrument pratique pour les services de détection et de répression et les autorités judiciaires dans la lutte mondiale contre la cybercriminalité, le but étant d'apporter une valeur ajoutée à la coopération internationale. Comme indiqué dans les résolutions 74/247 et 75/282 de l'Assemblée générale, une future convention des Nations Unies devrait prendre pleinement en considération le cadre existant d'instruments internationaux et régionaux ayant fait leurs preuves dans le domaine de la criminalité organisée et de la cybercriminalité. Par conséquent, toute nouvelle convention devrait compléter et éviter d'entraver de quelque manière que ce soit l'application des instruments existants ou l'adhésion d'un pays à ces instruments, et, dans la mesure du possible, éviter les doubles emplois.

Une future convention des Nations Unies devrait prévoir la protection des droits humains et des libertés fondamentales, qui s'appliquent aussi bien hors ligne qu'en ligne, et être compatible avec les instruments pertinents dans ce domaine.

Une future convention des Nations Unies, comme convenu par l'Assemblée générale dans sa résolution 75/282, devrait prendre pleinement en considération les travaux[6] et le document[7] issu de la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité.

II. Champ d'application

À cette fin, l'Union européenne et ses États membres estiment que le champ d'application d'une future convention des Nations Unies devrait être axé principalement sur le droit pénal matériel et le droit de la procédure pénale, ainsi que sur les mécanismes de coopération associés. À cet égard, la convention devrait également être conforme aux normes internationales en matière de droits humains et

[5] Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Suède et Tchéquie.

[6] Voir https://www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html.

[7] Voir UNODC/CCPCJ/EG.4/2021/2.

avoir pour objectif de lutter contre la cybercriminalité de la manière la plus efficace possible et protéger ainsi les victimes.

L'Union européenne et ses États membres estiment que ce nouvel instrument devrait définir précisément les termes qu'il utilise et privilégier les concepts déjà admis dans les textes internationaux en vigueur.

L'Union européenne et ses États membres recommandent que le contenu de cette convention soit resserré et se concentre sur les éléments essentiels de la justice pénale, et exclue donc autant que possible tout élément accessoire.

Sur la base des principes exposés ci-dessus, l'Union européenne et ses États membres considèrent que les éléments suivants devraient figurer dans une future convention des Nations Unies :

1. **Les dispositions de droit pénal matériel** liées aux actes de cybercriminalité qui devraient être incriminés par tous les États parties à une future convention des Nations Unies. Ces dispositions ne devraient en général concerner que les infractions touchant la haute technologie et les infractions cyberdépendantes, telles que l'accès illégal à des données et systèmes informatiques ou leur interception, ou encore toute atteinte à leur intégrité[8].

Les dispositions de droit pénal matériel doivent être clairement et étroitement définies et être pleinement compatibles avec les normes internationales en matière de droits humains et avec un cyberespace mondial, ouvert, libre, stable et sûr. Des dispositions vagues incriminant des types de comportement qui ne sont pas clairement définis dans une future convention des Nations Unies ou dans d'autres instruments juridiques universels risqueraient de porter indûment atteinte et de manière disproportionnée aux droits humains et aux libertés fondamentales, notamment au droit à la liberté de parole et d'expression, et créeraient de surcroît une incertitude juridique.

Les dispositions de droit pénal matériel devraient, dans la mesure du possible, être rédigées de manière technologiquement neutre afin d'englober les progrès technologiques à venir[9]. Dans le même temps, il conviendrait d'encourager l'échange de vues et d'informations sur les nouveaux problèmes posés par ces progrès technologiques.

L'incompatibilité avec d'autres conventions internationales doit être évitée, en particulier lorsque certaines infractions, telles que le trafic d'armes ou la distribution illicite de stupéfiants, sont déjà largement couvertes par les dispositions existantes des conventions internationales, de sorte que l'inclusion de ces types de comportement dans une convention sur la cybercriminalité n'apporterait aucune valeur ajoutée.

De manière générale, une future convention des Nations Unies devrait s'abstenir de fixer des normes (minimales) en matière de sanctions ou de peines pour des infractions spécifiques au-delà des modèles existants, comme indiqué au paragraphe 1 de l'article 11 de la Convention des Nations Unies contre la criminalité transnationale organisée.

En ce qui concerne les règles relatives à la compétence, une future convention des Nations Unies devrait s'inspirer de l'approche définie dans les instruments juridiques existants, comme l'article 15 de la Convention contre la criminalité organisée.

2. **Les conditions et garanties matérielles et procédurales appropriées** pour assurer la compatibilité avec les droits humains et les libertés fondamentales, y compris les principes de légalité, de nécessité et de proportionnalité des mesures de détection et de répression et les garanties matérielles et procédurales spécifiques assurant, en particulier, le droit à la vie privée et à la protection des données personnelles, le droit à la liberté d'expression et d'information et le droit à un procès

[8] Conformément à la recommandation 5 sur l'incrimination, adoptée par le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité lors de sa réunion tenue à Vienne du 6 au 8 avril 2021 (voir UNODC/CCPCJ/EG.4/2021/2, annexe, recommandation 5).

[9] Voir UNODC/CCPCJ/EG.4/2021/2, annexe, recommandation 1, sur la législation et les cadres.

équitable. Ces garanties devraient s'appuyer sur les garanties figurant dans d'autres instruments juridiques internationaux pertinents et être au moins du même niveau que celles-ci.

3. **Les mesures procédurales et les dispositions de procédure pénale relatives aux mécanismes de coopération entre les parties à une future convention des Nations Unies**, y compris la coopération concernant les enquêtes et d'autres procédures judiciaires ainsi que l'obtention de preuves électroniques, lorsque cela est approprié et pertinent, tout en veillant à ce que celles-ci puissent être recueillies, conservées, authentifiées et utilisées dans le cadre de procédures pénales[10]. Ces mesures et dispositions devraient être compatibles avec les modèles fournis par celles figurant dans d'autres instruments juridiques internationaux pertinents, s'en inspirer et être complétées par des garanties appropriées, notamment en matière de coopération dans les situations d'urgence.

4. Les éléments, conformément aux droits humains, concernant **le renforcement des capacités, la mise en commun des meilleures pratiques et des enseignements tirés de l'expérience et l'assistance technique**, y compris le rôle majeur joué par l'Office des Nations Unies contre la drogue et le crime dans ces domaines.

L'Union européenne et ses États membres considèrent que ce qui suit doit être exclu du champ d'application d'une future convention des Nations Unies :

- Les questions concernant ou réglementant la sécurité nationale ou le comportement des États ;
- Les questions concernant ou réglementant les règles de gouvernance d'Internet, qui sont déjà traitées dans le cadre de politiques et d'instances multipartites spécialisées.

Enfin, en tant qu'instrument intergouvernemental, une future convention des Nations Unies devrait s'abstenir d'imposer directement des obligations aux organisations non gouvernementales, y compris celles du secteur privé, comme les fournisseurs de services Internet.

III. Structure

Compte tenu de ce qui précède, une future convention des Nations Unies pourrait comporter les différents chapitres ci-après :

Préambule (champ d'application et objectifs d'une future convention des Nations Unies) ;

I. Types et définitions précises des infractions ;

II. Règles de procédure internes et principes fondamentaux à respecter à cet égard, par exemple le respect des droits humains, y compris les droits à la vie privée et à la protection des données personnelles, et les principes de nécessité et de proportionnalité ;

III. Coopération internationale ;

IV. Assistance technique, formation et renforcement des capacités, et rôle de l'Office des Nations Unies contre la drogue et le crime à cet égard.

[10] Ibid., recommandation 16, sur les preuves électroniques et la justice pénale.