Nations Unies A/AC.291/12/Add.1

Assemblée générale

Distr. générale
3 août 2022
Français
Original : anglais

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
Troisième session
New York, 29 août-9 septembre 2022

Compilation des propositions et commentaires soumis par les États Membres sur les dispositions relatives à la coopération internationale, à l'assistance technique, aux mesures préventives et au mécanisme d'application, les dispositions finales et le préambule d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

Additif

Table des matières

	Page
Contributions supplémentaires	2
Colombie	2
Jamaïque (au nom de la Communauté des Caraïbes)	6
Nouvelle-Zélande	27
Viet Nam	31

V.22-10828 (F) 020922 050922

Merci de recycler

Contributions supplémentaires

Le présent additif contient les contributions des États Membres pour la troisième 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 reçues après le 8 juillet 2022.

Colombie

Original : anglais
[13 juillet 2022]

La République de Colombie présente ci-dessous son point de vue sur les éléments qui, selon elle, devraient figurer dans les sections relatives à la coopération internationale, à l'assistance technique, aux mesures préventives, aux mécanismes d'application, aux dispositions finales et dans le préambule de la convention sur la cybercriminalité en cours de négociation.

Pour préparer ce texte, l'équipe interinstitutionnelle colombienne a analysé l'incidence que la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) a eue sur le pays. Ce texte vise à inclure ce qui, à notre avis, devrait être amélioré dans le domaine de la cybercriminalité pour que d'avantage d'instruments soient disponibles pour les services de détection et de répression.

Préambule

Les États Membres de l'Organisation des Nations Unies, reconnaissant l'intérêt de favoriser la coopération, la nécessité de poursuivre, en priorité, une politique pénale commune visant à protéger la société contre la cybercriminalité, entre autres, en adoptant une législation appropriée, le tout dans le respect de la protection des droits humains et des libertés fondamentales.

Rappelant les résolutions 2322 (2016), 2331 (2016), 2341 (2017) et 2396 (2017) du Conseil de sécurité, les résolutions 69-193 (2014) et S-30/1 (2016) de l'Assemblée générale, les résolutions 8/1 (2016), 9/3 (2018) et 10/4 (2020) de la Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée, la résolution 26/4 (2017) de la Commission pour la prévention du crime et la justice pénale et les résolutions 19 (2019) et 21 (2019) du Conseil économique et social, qui encouragent la collecte et la conservation des preuves numériques.

Coopération internationale

Principes généraux relatifs à la coopération internationale (Convention du Conseil de l'Europe sur la cybercriminalité, art. 23)

Principes relatifs à l'extradition

Extradition

1. Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales établies conformément aux articles définissant la criminalité cyberdépendante et les infractions cyberdépendantes telles que l'abus sexuel sur enfants, la fraude informatique et la violation des données personnelles, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère. [Convention du Conseil de l'Europe sur la cybercriminalité, art. 24, par. 1a)]

2. Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à

extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles. (Convention du Conseil de l'Europe sur la cybercriminalité, art. 24, par. 2)

3. Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article. (Convention du Conseil de l'Europe sur la cybercriminalité, art. 24, par. 3)

4. Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition. (Convention du Conseil de l'Europe sur la cybercriminalité, art. 24, par. 4)

5. L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition. (Convention du Conseil de l'Europe sur la cybercriminalité, art. 24, par. 5)

Principes généraux relatifs à l'entraide (Convention du Conseil de l'Europe sur la cybercriminalité, art. 25, par. 1 à 5)

1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées dans la section relative aux procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables.

3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, notamment via le système mondial de communication policière I-24/7 d'INTERPOL et le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. La Partie requise accepte et répond à la demande en utilisant ces mêmes moyens de communication rapides.

4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles définissant la criminalité cyberdépendante et les infractions cyberdépendantes telles que l'abus sexuel sur enfants, la fraude informatique et la violation des données personnelles, au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Information spontanée (Convention du Conseil de l'Europe sur la cybercriminalité, art. 26, par. 1 et 2)

Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1. Application en l'absence de traité ou d'arrangement (Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 1)

2. Autorités centrales [Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 2a) et 2b)]

2. c) Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au secrétariat de la Convention les noms et adresses des autorités désignées en application du présent paragraphe ; [Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 2c)]

2. d) Le secrétariat de la Convention établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre. [Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 2d)]

3. Entraide (Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 3)

4. Refus d'entraide [Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 4a) et 4b)]

5. Report de l'exécution (Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 5)

6. Considérations avant de différer l'entraide (Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 6)

7. Résultat de l'exécution d'une demande d'entraide (Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 7)

8. Confidentialité de la demande d'entraide (Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 8)

9. [Convention du Conseil de l'Europe sur la cybercriminalité, art. 27, par. 9a), 9b), 9c), 9d) et 9e)]

10. Confidentialité et restriction d'utilisation (Convention du Conseil de l'Europe sur la cybercriminalité, art. 28, par. 1, 2a), 2b), 3 et 4)

Dispositions particulières

Entraide en matière de mesures provisoires

1. Divulgation rapide de données de trafic conservées :

2. Lorsque, en exécutant une demande de conservation rapide de données de trafic conservées pour conserver les données de trafic concernant une communication spécifique, la Partie requise découvre qu'un fournisseur de services dans un autre État a participé à la transmission de cette communication, elle divulgue rapidement à la Partie requérante une quantité suffisante de données de trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise. (Convention du Conseil de l'Europe sur la cybercriminalité, art. 30, par. 1)

3. Divulgation des données de trafic au titre du paragraphe 1 [Convention du Conseil de l'Europe sur la cybercriminalité, art. 30, par. 2a) et 2b)]

4. Entraide concernant l'accès aux données informatiques stockées :

a) Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer

des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément aux dispositions relatives à la conservation rapide de données informatiques stockées. (Convention du Conseil de l'Europe sur la cybercriminalité, art. 31, par. 1) ;

b) La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article sur les principes généraux relatifs à la coopération internationale, et en se conformant aux dispositions pertinentes du présent chapitre. (Convention du Conseil de l'Europe sur la cybercriminalité, art. 31, par. 2) ;

c) Réponse à la demande [Convention du Conseil de l'Europe sur la cybercriminalité, art. 32, par. 3a), 3b)] ;

d) Entraide en matière de collecte en temps réel de données de trafic (Convention du Conseil de l'Europe sur la cybercriminalité, art. 33, par. 1 et 2) ;

e) Entraide en matière d'interception de données relatives au contenu (Convention du Conseil de l'Europe sur la cybercriminalité, art. 34).

Mécanisme d'application (Convention du Conseil de l'Europe sur la cybercriminalité, art. 35)

1. Chaque partie désigne un point de contact, afin d'assurer une assistance immédiate pour des investigations ou des procédures concernant les infractions pénales liées à l'utilisation des technologies de l'information et des communications à des fins criminelles.

Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

a) Prestation de conseils techniques ;

b) Conservation des données, conformément aux articles 29 et 30 ;

c) Recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2. Les points de contact coordonnent des réunions (au moins deux fois par an) pour examiner et proposer des mises à jour de la Convention et suivre l'évolution de la cybercriminalité.

3. a) Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b) Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

4. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Nouvelles formulations proposées :

Les Parties mettent en œuvre des mécanismes visant à favoriser la conception de logiciels dans les pays en développement afin de promouvoir le développement local et la sécurité informatique dans les secteurs public et privé et de prévenir la cybercriminalité.

Les Parties facilitent la diffusion des technologies nécessaires en vue d'améliorer les capacités locales des pays moins avancés pour lutter contre la cybercriminalité. Les programmes de coopération avec les pays en développement viseront à renforcer les capacités administratives et techniques pour préserver les progrès technologiques réalisés et promouvoir de nouvelles avancées.

La prévention de la cybercriminalité est un élément central des programmes de lutte contre la criminalité dans le cyberespace. Les Parties encouragent l'élaboration de mécanismes éducatifs pour le public et soutiennent le développement de technologies abordables capables de faire face aux menaces que pose la cybercriminalité.

Jamaïque (au nom de la Communauté des Caraïbes)

Original : anglais
[12 juillet 2022]

Chapitre 4 – Coopération internationale en matière pénale

Article : Coopération internationale

1. Les États parties coopèrent en matière pénale conformément au présent chapitre de la Convention.

2. En matière de coopération internationale, chaque fois que la double incrimination est considérée comme une condition, celle-ci est réputée remplie, que la législation de l'État partie requis qualifie ou désigne ou non l'infraction pénale de la même manière que l'État partie requérant, si l'acte constituant l'infraction pour laquelle l'assistance est demandée est une infraction pénale en vertu de la législation des deux États parties.

Article : Extradition

1. Le présent article s'applique aux infractions pénales établies conformément à la présente Convention lorsque la personne faisant l'objet de la demande d'extradition se trouve sur le territoire de l'État partie requis, à condition que l'infraction pour laquelle l'extradition est demandée soit punissable par le droit interne de l'État partie requérant et de l'État partie requis.

2. Nonobstant le paragraphe 1 du présent article, un État partie dont la législation le permet peut accorder l'extradition d'une personne pour l'une quelconque des infractions pénales établies conformément à la présente Convention qui ne sont pas punissables en vertu de son droit interne.

3. Si la demande d'extradition porte sur plusieurs infractions pénales distinctes, dont au moins une donne lieu à extradition en vertu du présent article et dont certaines ne donnent pas lieu à extradition en raison de la durée de l'emprisonnement mais ont un lien avec des infractions établies conformément à la présente Convention, l'État partie requis peut appliquer le présent article également à ces infractions.

4. Chacune des infractions pénales auxquelles s'applique le présent article est de plein droit incluse dans tout traité d'extradition en vigueur entre les États parties en tant qu'infraction dont l'auteur peut être extradé. Les États parties s'engagent à inclure ces infractions en tant qu'infractions dont l'auteur peut être extradé dans tout traité d'extradition qu'ils concluront entre eux. Un État partie dont la législation le permet, lorsqu'il se fonde sur la présente Convention pour l'extradition, ne considère aucune des infractions établies conformément à la présente Convention comme une infraction politique.

5. 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 présente Convention comme la base légale de l'extradition pour les infractions pénales auxquelles le présent article s'applique.

6. Un État partie qui subordonne l'extradition à l'existence d'un traité :

a) Au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion à la présente Convention, indique au Secrétaire général de l'Organisation des Nations Unies s'il considère la présente Convention comme la base légale pour coopérer en matière d'extradition avec d'autres États parties ; et

b) S'il ne considère pas la présente Convention comme la base légale pour coopérer en matière d'extradition, s'efforce, s'il y a lieu, de conclure des traités d'extradition avec d'autres États parties afin d'appliquer le présent article.

7. Les États parties qui ne subordonnent pas l'extradition à l'existence d'un traité reconnaissent entre eux aux infractions auxquelles le présent article s'applique le caractère d'infraction pénale dont l'auteur peut être extradé.

8. L'extradition est subordonnée aux conditions prévues par le droit interne de l'État partie requis ou par les traités d'extradition applicables, y compris, notamment, aux conditions concernant la peine minimale requise pour extrader et aux motifs pour lesquels l'État partie requis peut refuser l'extradition.

9. Les États parties s'efforcent, sous réserve de leur droit interne, d'accélérer les procédures d'extradition et de simplifier les exigences en matière de preuve y relatives en ce qui concerne les infractions pénales auxquelles s'applique le présent article.

10. Sous réserve de son droit 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.

11. Un État partie sur le territoire duquel se trouve l'auteur présumé d'une infraction, s'il n'extrade pas cette personne au titre d'une infraction pénale à laquelle s'applique le présent article au seul motif qu'elle est l'un de ses ressortissants, à la demande de l'État partie requérant l'extradition, soumet l'affaire sans retard excessif à ses autorités compétentes aux fins de poursuites. Lesdites autorités prennent leur décision et mènent les poursuites de la même manière que pour toute autre infraction pénale grave au regard du droit interne de cet État partie. Les États parties intéressés coopèrent entre eux, notamment en matière de procédure et de preuve, afin d'assurer l'efficacité des poursuites.

12. Lorsqu'un État partie, en vertu de son droit interne, n'est autorisé à extrader ou remettre de toute autre manière l'un de ses ressortissants que si cette personne est ensuite renvoyée sur son territoire pour purger la peine prononcée à l'issue du procès ou de la procédure à l'origine de la demande d'extradition ou de remise, et lorsque cet État partie requis et l'État partie requérant s'accordent sur cette option et d'autres conditions qu'ils peuvent juger appropriées, cette extradition ou remise conditionnelle est suffisante aux fins de l'exécution de l'obligation énoncée au paragraphe 11 du présent article.

13. Si l'extradition, demandée aux fins d'exécution d'une peine, est refusée parce que la personne faisant l'objet de cette demande est un ressortissant de l'État partie requis, celui-ci, si son droit interne le lui permet, en conformité avec les prescriptions de ce droit et à la demande de l'État partie requérant, envisage de faire exécuter lui-même la peine prononcée conformément au droit interne de l'État partie requérant, ou le reliquat de cette peine.

14. Toute personne faisant l'objet de poursuites en raison de l'une quelconque des infractions pénales auxquelles le présent article s'applique se voit 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 le droit interne de l'État partie sur le territoire duquel elle se trouve.

15. Aucune disposition de la présente Convention ne doit être interprétée comme faisant obligation à l'État partie requis d'extrader s'il a de sérieuses raisons de penser que la demande a été présentée aux fins de poursuivre ou de punir une personne en raison de son sexe, de sa race, de sa religion, de sa nationalité, de son origine ethnique ou de ses opinions politiques, ou que donner suite à cette demande causerait un préjudice à cette personne pour l'une quelconque de ces raisons.

16. Un État partie ne peut refuser une demande d'extradition au seul motif que l'infraction est considérée comme touchant aussi à des questions fiscales.

17. Avant de refuser l'extradition, l'État partie requis consulte, s'il y a lieu, l'État partie requérant afin de lui donner toute possibilité de présenter ses opinions et de fournir des informations à l'appui de ses allégations.

18. Les États parties s'efforcent de conclure des accords ou arrangements bilatéraux et multilatéraux pour permettre l'extradition ou pour en accroître l'efficacité.

Article : Transfèrement des personnes condamnées

Les États parties peuvent envisager de conclure des accords ou des arrangements bilatéraux ou multilatéraux relatifs au transfèrement sur leur territoire de personnes condamnées à des peines d'emprisonnement ou autres peines privatives de liberté du fait d'infractions pénales établies conformément à la présente Convention afin qu'elles puissent y purger le reliquat de leur peine.

Article : Entraide judiciaire

1. Les États parties s'accordent mutuellement l'entraide judiciaire la plus large possible lors des enquêtes, poursuites et procédures judiciaires concernant les infractions pénales établies conformément à la présente Convention.

2. L'entraide judiciaire la plus large possible est accordée, autant que les lois, traités, accords et arrangements pertinents de l'État partie requis le permettent, lors des enquêtes, poursuites et procédures judiciaires concernant des infractions dont une personne morale peut être tenue responsable dans l'État partie requérant, conformément à l'article [Responsabilité des personnes morales] de la présente Convention.

3. L'entraide judiciaire qui est accordée en application du présent article peut être demandée aux fins suivantes :

a) Recueillir des témoignages ou des dépositions ;

b) Signifier des actes dans les procédures judiciaires ;

c) Effectuer des perquisitions et des saisies, ainsi que des gels ;

d) Examiner les informations/données électroniques, les objets et les sites ;

e) Fournir des informations, des pièces à conviction pour inclure des informations électroniques, et des estimations d'experts ;

f) Fournir des originaux ou des copies certifiées conformes de documents et dossiers pertinents, y compris des documents administratifs, bancaires, financiers ou commerciaux et des documents de société ;

g) Identifier ou localiser des produits du crime, des biens, des instruments ou d'autres choses afin de recueillir des éléments de preuve ;

h) Faciliter la comparution volontaire de personnes dans l'État partie requérant ;

i) Fournir tout autre type d'assistance compatible avec le droit interne de l'État partie requis ;

j) Identifier, geler et localiser le produit du crime, conformément au (chapitre sur le recouvrement d'avoirs) de la présente Convention ;

k) Recouvrer des avoirs, conformément au (chapitre sur le recouvrement d'avoirs) de la présente Convention.

4. Sans préjudice du droit interne, les autorités compétentes d'un État partie peuvent, sans demande préalable, communiquer des informations concernant des affaires pénales à une autorité compétente d'un autre État partie, si elles pensent que ces informations pourraient aider celle-ci à entreprendre ou à mener à bien des

enquêtes et des poursuites pénales, ou amener ce dernier État partie à formuler une demande en vertu de la présente Convention.

5. La communication d'informations conformément au paragraphe 4 du présent article se fait sans préjudice des enquêtes et poursuites pénales dans l'État partie dont les autorités compétentes fournissent les informations. Les autorités compétentes qui reçoivent ces informations accèdent à toute demande tendant à ce que lesdites informations restent confidentielles, même temporairement, ou à ce que leur utilisation soit assortie de restrictions. Toutefois, cela n'empêche pas l'État partie qui reçoit les informations de révéler, lors de la procédure judiciaire, des informations à la décharge d'un prévenu. Dans ce dernier cas, l'État partie qui reçoit les informations avise l'État partie qui les communique avant la révélation, et s'il lui en est fait la demande, consulte ce dernier. Si, dans un cas exceptionnel, une notification préalable n'est pas possible, l'État partie qui reçoit les informations informe sans retard de la révélation l'État partie qui les communique.

6. Le présent article n'affecte en rien les obligations découlant de tout autre traité bilatéral ou multilatéral régissant ou devant régir, entièrement ou partiellement, l'entraide judiciaire.

7. Les paragraphes 9 à 29 du présent article sont applicables aux demandes faites conformément au présent article si les États parties en question ne sont pas liés par un traité d'entraide judiciaire. Lorsque les États parties sont liés par un tel traité, les dispositions correspondantes de ce traité sont applicables, à moins que les États parties ne conviennent d'appliquer à leur place les dispositions des paragraphes 9 à 29 du présent article.

8. Les États parties ne peuvent invoquer le secret bancaire pour refuser l'entraide judiciaire prévue au présent article.

9. Lorsqu'en application du présent article il répond à une demande d'aide en l'absence de double incrimination, un État partie requis tient compte de l'objet de la présente Convention tel qu'énoncé à l'article premier.

10. En application du présent article, les États parties peuvent refuser de donner suite à une demande d'entraide au motif de l'absence de double incrimination. Toutefois, un État partie requis, lorsque cela est compatible avec les concepts fondamentaux de son système juridique, accorde l'aide demandée si elle n'implique pas de mesures coercitives, mais cette aide peut être refusée lorsque la demande porte sur des questions mineures ou des questions pour lesquelles la coopération ou l'aide demandée peut être obtenue sur le fondement d'autres articles de la présente Convention.

11. Chaque État partie peut envisager de prendre les mesures nécessaires pour lui permettre de fournir une aide plus large en application du présent article, en l'absence de double incrimination.

12. Toute personne détenue ou purgeant une peine sur le territoire d'un État partie, dont la présence est requise dans un autre État partie à des fins d'identification ou de témoignage ou pour qu'elle apporte de toute autre manière son concours à l'obtention de preuves dans le cadre d'enquêtes, de poursuites ou de procédures judiciaires relatives aux infractions pénales établies conformément à la présente Convention, peut faire l'objet d'un transfèrement si les conditions ci-après sont réunies :

a) Ladite personne y consent librement et en toute connaissance de cause ;

b) Les autorités compétentes des deux États parties concernés consentent au transfèrement, sous réserve des conditions que ces États parties peuvent juger appropriées.

13. Aux fins du paragraphe 12 du présent article :

a) L'État partie vers lequel la personne est transférée a le pouvoir et l'obligation de la garder en détention, sauf demande ou autorisation contraire de la part de l'État partie à partir duquel elle a été transférée ;

b) L'État partie vers lequel la personne est transférée s'acquitte sans retard de l'obligation de la remettre à la garde de l'État partie à partir duquel elle a été transférée, conformément à ce qui aura été convenu au préalable ou autrement décidé par les autorités compétentes des deux États parties ;

c) L'État partie vers lequel la personne est transférée ne peut exiger de l'État partie à partir duquel elle a été transférée qu'il engage une procédure d'extradition pour qu'elle lui soit remise ;

d) Il est tenu compte de la période que la personne a passée en détention dans l'État partie vers lequel elle a été transférée aux fins du décompte de la peine à purger dans l'État partie à partir duquel elle a été transférée.

14. À moins que l'État partie à partir duquel une personne doit être transférée en vertu des paragraphes 12 et 13 du présent article ne donne son accord, ladite personne, quelle que soit sa nationalité, n'est pas poursuivie, détenue, punie ni soumise à d'autres restrictions de sa liberté personnelle sur le territoire de l'État partie vers lequel elle est transférée à raison d'actes, d'omissions ou de condamnations antérieurs à son départ du territoire de l'État partie à partir duquel elle a été transférée.

15. Chaque État partie désigne une autorité centrale qui a la responsabilité et le pouvoir de recevoir les demandes d'entraide judiciaire et, soit de les exécuter, soit de les transmettre aux autorités compétentes pour exécution. Si un État partie a une région ou un territoire spécial doté d'un système d'entraide judiciaire différent, il peut désigner une autorité centrale distincte qui aura la même fonction pour ladite région ou ledit territoire. Les autorités centrales assurent l'exécution ou la transmission rapide et en bonne et due forme des demandes reçues. Si l'autorité centrale transmet la demande à une autorité compétente pour exécution, elle encourage l'exécution rapide et en bonne et due forme de la demande par l'autorité compétente.

16. L'autorité centrale désignée aux fins du paragraphe 15 fait l'objet d'une notification adressée au Secrétaire général de l'Organisation des Nations Unies au moment où chaque État partie dépose ses instruments de ratification, d'acceptation ou d'approbation ou d'adhésion à la présente Convention.

17. Les demandes d'entraide judiciaire et toute communication y relative sont transmises aux autorités centrales désignées par les États parties. La présente disposition s'entend sans préjudice du droit de tout État partie d'exiger que ces demandes et communications lui soient adressées par la voie diplomatique et, en cas d'urgence, si les États parties en conviennent, par l'intermédiaire de l'Organisation internationale de police criminelle, si cela est possible.

18. Les demandes sont adressées au titre du paragraphe 17 par écrit ou, si possible, par tout autre moyen pouvant produire un document écrit, dans une langue acceptable pour l'État partie requis, dans des conditions permettant audit État partie d'en établir l'authenticité. La ou les langues acceptables pour chaque État partie sont notifiées au Secrétaire général de l'Organisation des Nations Unies au moment où ledit État partie dépose son instrument de ratification, d'acceptation ou d'approbation ou d'adhésion à la présente Convention. En cas d'urgence et si les États parties en conviennent, les demandes peuvent être faites oralement mais doivent être confirmées sans délai par écrit.

19. L'État partie requis accepte une demande par la voie électronique. Un État partie peut également accepter une demande transmise oralement et peut exiger une confirmation électronique. Il peut exiger des conditions suffisantes de sécurité et d'authentification avant d'accepter la demande.

20. Une demande d'entraide judiciaire doit contenir les renseignements suivants :

a) La désignation de l'autorité dont émane la demande ;

b) L'objet et la nature de l'enquête, des poursuites ou de la procédure judiciaire auxquelles se rapporte la demande, ainsi que le nom et la fonction de l'autorité qui en est chargée ;

c) Un résumé des faits pertinents, sauf pour les demandes adressées aux fins de la signification d'actes judiciaires ;

d) Une description de l'assistance requise et le détail de toute procédure particulière que l'État partie requérant souhaite voir appliquée ;

e) Si possible, l'identité, l'adresse et la nationalité de toute personne visée ; et

f) Le but dans lequel le témoignage, les informations ou les mesures sont demandés.

21. L'État partie requis peut demander un complément d'information lorsque cela apparaît nécessaire pour exécuter la demande conformément à son droit interne ou lorsque cela en facilite l'exécution.

22. Toute demande est exécutée conformément au droit interne de l'État partie requis et, dans la mesure où cela ne contrevient pas au droit interne de l'État partie requis et lorsque cela est possible, conformément aux procédures spécifiées dans la demande.

23. Lorsque cela est possible et conforme à son droit interne, si une personne qui se trouve sur le territoire d'un État partie doit être entendue comme témoin ou comme expert par les autorités judiciaires d'un autre État partie, le premier État partie peut, à la demande de l'autre, autoriser son audition par vidéoconférence s'il n'est pas possible ou souhaitable qu'elle comparaisse en personne sur le territoire de l'État partie requérant. Les États parties peuvent convenir que l'audition sera conduite par une autorité judiciaire de l'État partie requérant et qu'une autorité judiciaire de l'État partie requis y assistera.

24. L'État partie requérant ne communique ni n'utilise les informations ou les éléments de preuve fournis par l'État partie requis pour des enquêtes, poursuites ou procédures judiciaires autres que celles visées dans la demande sans le consentement préalable de l'État partie requis. Rien dans le présent paragraphe n'empêche l'État partie requérant de révéler, lors de la procédure, des informations ou des éléments de preuve à décharge. Dans ce cas, l'État partie requérant avise l'État partie requis avant la révélation et, s'il lui en est fait la demande, consulte ce dernier. Si, dans un cas exceptionnel, une notification préalable n'est pas possible, l'État partie requérant informe sans retard l'État partie requis de la révélation.

25. L'État partie requérant peut exiger que l'État partie requis garde le secret sur la demande et sa teneur, sauf dans la mesure nécessaire pour l'exécuter. Si l'État partie requis ne peut satisfaire à cette exigence, il en informe sans délai l'État partie requérant.

26. L'entraide judiciaire peut être refusée :

a) Si la demande n'est pas conforme au présent article ;

b) Si l'État partie requis estime que l'exécution de la demande est susceptible de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels ;

c) Au cas où le droit interne de l'État partie requis interdirait à ses autorités de prendre les mesures demandées s'il s'agissait d'une infraction analogue ayant fait l'objet d'une enquête, de poursuites ou d'une procédure judiciaire dans le cadre de sa propre compétence ;

d) Au cas où il serait contraire au système juridique de l'État partie requis concernant l'entraide judiciaire d'accepter la demande.

27. Les États parties ne peuvent refuser une demande d'entraide judiciaire au seul motif que l'infraction est considérée comme touchant aussi à des questions fiscales.

28. Tout refus d'entraide judiciaire doit être motivé.

29. L'État partie requis exécute la demande d'entraide judiciaire aussi promptement que possible et tient compte dans toute la mesure possible de tous délais suggérés par l'État partie requérant et qui sont motivés, de préférence dans la demande. L'État partie requérant peut présenter des demandes raisonnables d'informations sur l'état d'avancement des mesures prises par l'État partie requis pour faire droit à sa demande. L'État partie requis répond aux demandes raisonnables de l'État partie requérant concernant les progrès réalisés dans l'exécution de la demande. Quand l'entraide demandée n'est plus nécessaire, l'État partie requérant en informe promptement l'État partie requis.

30. L'entraide judiciaire peut être différée par l'État partie requis au motif qu'elle entraverait une enquête, des poursuites ou une procédure judiciaire en cours.

31. Avant de refuser une demande en vertu du paragraphe 26 du présent article ou d'en différer l'exécution en vertu de son paragraphe 30, l'État partie requis étudie avec l'État partie requérant la possibilité d'accorder l'entraide sous réserve des conditions qu'il juge nécessaires. Si l'État partie requérant accepte l'entraide sous réserve de ces conditions, il se conforme à ces dernières.

32. Sans préjudice de l'application du paragraphe 12 du présent article, un témoin, un expert ou une autre personne qui, à la demande de l'État partie requérant, consent à déposer au cours d'une procédure ou à collaborer à une enquête, à des poursuites ou à une procédure judiciaire sur le territoire de l'État partie requérant ne sera pas poursuivi, détenu, puni ni soumis à d'autres restrictions de sa liberté personnelle sur ce territoire à raison d'actes, d'omissions ou de condamnations antérieurs à son départ du territoire de l'État partie requis. Cette immunité cesse lorsque le témoin, l'expert ou ladite personne ayant eu, pendant une période de quinze jours consécutifs ou toute autre période convenue par les États parties à compter de la date à laquelle ils ont été officiellement informés que leur présence n'était plus requise par les autorités judiciaires, la possibilité de quitter le territoire de l'État partie requérant, y sont néanmoins demeurés volontairement ou, l'ayant quitté, y sont revenus de leur plein gré.

33. Les frais ordinaires encourus pour exécuter une demande sont à la charge de l'État partie requis, à moins qu'il n'en soit convenu autrement entre les États parties concernés. Lorsque des dépenses importantes ou extraordinaires sont ou se révèlent ultérieurement nécessaires pour exécuter la demande, les États parties se consultent pour fixer les conditions selon lesquelles la demande sera exécutée, ainsi que la manière dont les frais seront assumés.

34. L'État partie requis :

a) Fournit à l'État partie requérant copie des dossiers, documents et renseignements administratifs en sa possession et auxquels, en vertu de son droit interne, le public a accès ;

b) Peut fournir à l'État partie requérant intégralement, en partie ou aux conditions qu'il estime appropriées, copie de tous dossiers, documents ou renseignements administratifs en sa possession et auxquels, en vertu de son droit interne, le public n'a pas accès.

35. Les États parties envisagent, s'il y a lieu, la possibilité de conclure des accords ou des arrangements bilatéraux ou multilatéraux qui servent les objectifs du présent article, le mettent en pratique ou le renforcent.

Échange spontané d'informations

1. Sans préjudice du droit interne, les autorités compétentes d'un État partie peuvent, sans demande préalable, communiquer des informations concernant les affaires pénales à une autorité compétente d'un autre État partie, si elles pensent que ces informations pourraient aider celui-ci à entreprendre ou à mener à bien des enquêtes et des poursuites pénales, ou amener ce dernier État partie à formuler une demande en vertu de la présente Convention.

2. La communication d'informations conformément au présent article se fait sans préjudice des enquêtes et poursuites pénales dans l'État partie dont les autorités compétentes fournissent les informations. Les autorités compétentes qui reçoivent ces informations accèdent à toute demande tendant à ce que lesdites informations restent confidentielles, même temporairement, ou à ce que leur utilisation soit assortie de restrictions. Toutefois, cela n'empêche pas l'État partie qui reçoit les informations de révéler, lors de sa procédure judiciaire, des informations à la décharge d'un prévenu. Dans ce dernier cas, l'État partie qui reçoit les informations avise l'État partie qui les communique avant la révélation, et s'il lui en est fait la demande, consulte ce dernier. Si, dans un cas exceptionnel, une notification préalable n'est pas possible, l'État partie qui reçoit les informations informe sans retard de la révélation l'État partie qui les communique.

Article : Entraide judiciaire en matière de mesures provisoires

a) Assistance – préservation de données informatiques/informations numériques (Préservation accélérée de données informatiques stockées)

1. Un État partie peut demander à un autre État partie d'ordonner ou d'imposer d'une autre façon la préservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cet autre État partie, et au sujet desquelles l'État partie requérant a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2. Une demande de préservation faite en application du paragraphe 1 doit préciser :

a) L'autorité qui demande la préservation ;

b) L'infraction pénale faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent ;

c) Les données informatiques stockées à préserver et la nature de leur lien avec l'infraction pénale ;

d) Toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;

e) La nécessité de la mesure de préservation ; et

f) Le fait que l'État partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3. Après avoir reçu la demande d'un autre État partie, l'État partie requis doit prendre toutes les mesures appropriées afin de procéder sans délai à la préservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la préservation.

4. Un État partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions pénales autres que celles visées par la présente Convention, se réserver le droit de refuser la demande de préservation au titre du présent article dans le cas où il a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5. En outre, une demande de préservation peut être refusée uniquement :

a) Si la demande porte sur une infraction pénale que l'État partie requis considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b) Si l'État partie requis estime que l'exécution de la demande est susceptible de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

6. Lorsque l'État partie requis estime que la préservation simple ne suffira pas à garantir la disponibilité future des données stockées, ou compromettra la confidentialité de l'enquête de l'État partie requérant, ou nuira d'une autre façon à celle-ci, il en informe rapidement l'État partie requérant, qui décide alors s'il convient néanmoins d'exécuter la demande.

7. Toute préservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins quatre-vingt-dix jours afin de permettre à l'État partie requérant de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données stockées. Après la réception d'une telle demande, les données doivent continuer à être préservées en attendant l'adoption d'une décision concernant la demande.

Article : Production accélérée de données informatiques stockées en situation d'urgence

1. Chaque État partie adopte les mesures législatives et autres pouvant se révéler nécessaires, en cas d'urgence, pour que son point de contact du Réseau 24/7 visé à l'article [Réseau 24/7] de la Convention (« point de contact ») puisse transmettre une demande à un point de contact dans un autre État partie et recevoir une demande de ce dernier pour une assistance immédiate en vue de l'obtention, par un fournisseur de services situé sur le territoire de l'État partie concerné, de la production accélérée de données informatiques stockées spécifiées qui sont en la possession ou sous le contrôle dudit fournisseur de services.

2. Chaque État partie peut se réserver le droit de ne pas divulguer à l'État partie requérant les données informatiques stockées spécifiées jusqu'à ce que l'État partie requérant transmette une demande d'entraide judiciaire d'urgence conformément à l'article [Demande d'entraide judiciaire d'urgence].

3. Un État partie peut, au moment de la signature de la présente Convention ou au moment du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'il n'exécutera pas de demandes introduites en vertu du paragraphe 1 pour la divulgation d'informations relatives à l'abonné seulement.

4. Chaque État partie adopte, conformément au paragraphe 1, les mesures législatives et autres nécessaires pour permettre :

a) À ses autorités de demander des données à un fournisseur de services situé sur son territoire à la suite d'une demande émise en vertu du paragraphe 1 ;

b) À un fournisseur de services situé sur son territoire de divulguer les données informatiques demandées à ses autorités en réponse à une demande émise en vertu de l'alinéa a) ; et

c) À ses autorités de fournir les données informatiques demandées à l'État partie requérant.

5. La demande introduite en vertu du paragraphe 1 :

a) Spécifie l'autorité compétente qui cherche des données informatiques et la date à laquelle la demande a été faite ;

b) Contient une déclaration selon laquelle la demande est émise en vertu de la présente Convention ;

c) Précise le nom et l'adresse du (ou des) fournisseur(s) de services qui est (sont) en possession des données informatiques recherchées ou en a (ont) le contrôle ;

d) Précise la ou les infractions objet(s) de l'enquête ou des procédures pénales et indique la référence à ses dispositions légales et les sanctions applicables ;

e) Mentionne suffisamment de faits démontrant que la situation est urgente et comment les données demandées sont liées à la situation ;

f) S'accompagne d'une description détaillée des données informatiques demandées ;

g) Mentionne tout type d'instructions spéciales afférentes à la procédure ; et

h) Mentionne toute autre information pouvant aider à obtenir la divulgation des données informatiques demandées.

6. L'État partie requis accepte une demande faite par voie électronique. Un État partie peut également accepter une demande transmise oralement et exiger une confirmation électronique. Il peut exiger des conditions suffisantes de sécurité et d'authentification avant d'accepter la demande.

7. Un État partie peut, au moment de la signature de la présente Convention ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'il exige de l'État partie requérant que celui-ci, après l'exécution de la demande, lui soumette la demande et toutes informations supplémentaires transmises à l'appui de cette dernière, dans le format et par le canal, qui peut couvrir une demande d'entraide judiciaire, spécifiés par l'État partie requis.

8. L'État partie requis informe l'État partie requérant selon une procédure accélérée de sa décision concernant la demande visée au paragraphe 1 et, au besoin, spécifie les éventuelles conditions dans lesquelles il fournirait les données et toutes autres formes de coopération qui peuvent être disponibles.

9. Si un État partie requérant ne peut se conformer à une condition imposée par l'État partie requis en vertu du paragraphe 8, il en informe rapidement l'État partie requis. L'État partie requis détermine alors si les informations ou les documents devraient néanmoins être fournis. Si l'État partie requérant accepte la condition, il est lié par celle-ci.

10. L'État partie requis qui fournit des renseignements ou du matériel soumis à une telle condition peut exiger de l'État partie requérant qu'il explique, en relation avec cette condition, l'utilisation qui a été faite de ces renseignements ou de ces documents.

Article : Entraide d'urgence

1. Chaque État partie peut demander une entraide judiciaire par les moyens les plus rapides lorsqu'il estime qu'il y a urgence. Une demande d'entraide en vertu du présent article doit présenter, outre les autres contenus requis, une description des faits étayant l'existence d'une situation d'urgence et une explication de la manière dont l'entraide demandée est liée à cette situation.

2. Un État partie requis accepte une demande faite par voie électronique. Il peut exiger des conditions suffisantes de sécurité et d'authentification avant d'accepter la demande.

3. L'État partie requis peut, par les moyens les plus rapides, demander un complément d'information afin d'évaluer la demande d'entraide. L'État partie requérant fournit ce complément d'information par les moyens les plus rapides.

4. Après avoir conclu à l'existence d'une situation d'urgence et s'être assuré que les autres conditions de l'entraide sont satisfaites, l'État partie requis répond à la demande d'entraide par les moyens les plus rapides.

5. Chaque État partie veille à ce qu'une personne de son autorité centrale ou d'autres autorités responsables des demandes d'entraide soit disponible 24 heures sur 24, 7 jours sur 7, pour répondre à une demande présentée en vertu du présent article.

6. L'autorité centrale ou les autres autorités responsables des demandes d'entraide des États parties requérant et requis peuvent décider de prévoir que les résultats de l'exécution d'une demande d'entraide effectuée en vertu du présent article, ou une

copie préliminaire de ces résultats, peuvent être transmis à l'État partie requérant par un canal autre que celui utilisé pour la transmission de la demande.

7. Lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base d'une législation uniforme ou réciproque en vigueur entre les États parties requérant et requis, l'article 27 (Procédures relatives aux demandes d'entraide en l'absence d'instruments internationaux applicables) et l'article 28 (Confidentialité et restriction d'utilisation) de la Convention de Budapest s'appliquent au présent article.

8. Lorsqu'un tel traité ou arrangement existe, le présent article est complété par les dispositions de ce traité ou arrangement, à moins que les États parties concernés ne décident d'un commun accord d'appliquer à la place l'une ou la totalité des dispositions de la Convention visées au paragraphe 7 du présent article.

9. Chaque État partie peut, au moment de la signature de la présente Convention ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer que des demandes d'entraide peuvent aussi être adressées directement par ses autorités judiciaires, ou par le biais de l'Organisation internationale de police criminelle (INTERPOL) ou du point de contact 24/7 établi au titre de l'article 35 de la Convention. Dans un tel cas, copie est adressée simultanément aux autorités centrales de l'État partie requis par le biais de l'autorité centrale de l'État partie requérant. Lorsqu'une demande est adressée directement à une autorité judiciaire de l'État partie requis et que celle-ci n'est pas compétente pour traiter la demande, elle transmet la demande à l'autorité nationale compétente et en informe directement l'État partie requérant.

Article : Aide à la saisie, à la consultation, à la collecte et à la divulgation de données informatiques et d'informations numériques

1. Lorsque, en exécutant une demande de préservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article [Entraide judiciaire en matière de mesures provisoires – Préservation accélérée de données], l'État partie requis découvre qu'un fournisseur de services dans un autre État a participé à la transmission de cette communication, l'État partie requis divulgue rapidement à l'État partie requérant une quantité jugée suffisante de données et d'informations numériques concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2. La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :

a) Si la demande porte sur une infraction pénale que l'État partie requis considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b) Si l'État partie requis estime que l'exécution de la demande est susceptible de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Article : Entraide concernant l'accès à des données informatiques stockées

1. Un État partie peut demander à un autre État partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre partie, y compris les données préservées conformément à l'article [Entraide judiciaire en matière de mesures provisoires – Préservation accélérée de données].

2. L'État partie requis satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article [Principes généraux relatifs à la coopération internationale], et en se conformant aux dispositions pertinentes du présent chapitre.

3. La demande doit être satisfaite aussi rapidement que possible dans les cas suivants :

a) Il existe des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou

b) Les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article : Entraide concernant l'interception de données relatives au contenu

Les États s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Article : Accès transfrontière à des données informatiques stockées, avec consentement ou lorsqu'elles sont accessibles au public

Un État partie peut, sans l'autorisation d'un autre État partie :

a) Accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou

b) Accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État partie, si l'État partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article : Accès aux technologies de l'information – L'information par-delà les frontières

Un État partie peut, sans l'autorisation d'un autre État partie :

a) Accéder à des informations numériques disponibles au public (source ouverte), indépendamment de la localisation géographique de ces informations ;

b) Accéder à, ou recevoir, par le biais des technologies de l'information disponibles sur son territoire, des informations numériques trouvées dans l'autre État partie, à condition d'avoir obtenu l'accord volontaire et légal de la personne ayant l'autorité légale pour divulguer les informations à cet État partie au moyen desdites technologies de l'information.

Article : Entraide concernant la collecte en temps réel de données relatives au trafic

1. Les États parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2. Chaque État partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article : Coopération entre les services de détection et de répression

1. Les États parties coopèrent étroitement, conformément à leurs systèmes juridiques et administratifs respectifs, en vue de renforcer l'efficacité de la détection et de la répression des infractions pénales visées par la présente Convention. En particulier, les États parties prennent des mesures efficaces pour :

a) Renforcer les voies de communication entre leurs autorités, organismes et services compétents et, si nécessaire, en établir afin de faciliter l'échange sûr et rapide d'informations concernant tous les aspects des infractions pénales visées par la

présente Convention, y compris, si les États parties concernés le jugent approprié, les liens avec d'autres activités criminelles ;

b) Coopérer avec d'autres États parties, s'agissant des infractions pénales visées par la présente Convention, dans la conduite d'enquêtes concernant les points suivants :

i) Identité et activités des personnes soupçonnées d'implication dans lesdites infractions, lieu où elles se trouvent ou lieu où se trouvent les autres personnes concernées ;

ii) Mouvement du produit du crime ou des biens provenant de la commission de ces infractions ;

iii) Mouvement des biens, des matériels ou d'autres instruments utilisés ou destinés à être utilisés dans la commission de ces infractions ;

c) Fournir, lorsqu'il y a lieu, les pièces ou quantités de substances nécessaires à des fins d'analyse ou d'enquête ;

d) Échanger, lorsqu'il y a lieu, avec d'autres États parties des informations sur les moyens et procédés spécifiques employés pour commettre les infractions pénales visées par la présente Convention, tels que l'usage de fausses identités, de documents contrefaits, modifiés ou falsifiés ou d'autres moyens de dissimulation des activités ;

e) Faciliter une coordination efficace entre leurs autorités, organismes et services compétents et favoriser l'échange de personnel et d'experts, y compris, sous réserve de l'existence d'accords ou d'arrangements bilatéraux entre les États parties concernés, le détachement d'agents de liaison ;

f) Échanger des informations et coordonner les mesures administratives et autres prises, comme il convient, pour détecter au plus tôt les infractions pénales visées par la présente Convention.

2. Afin de donner effet à la présente Convention, les États parties envisagent de conclure des accords et des arrangements bilatéraux ou multilatéraux prévoyant une coopération directe entre leurs services de détection et de répression et, lorsque de tels accords ou arrangements existent déjà, de les modifier. En l'absence de tels accords ou arrangements entre les États parties concernés, ces derniers peuvent se baser sur la présente Convention pour instaurer une coopération en matière de détection et de répression concernant les infractions pénales visées par la présente Convention. Chaque fois que cela est approprié, les États parties utilisent pleinement les accords ou arrangements, y compris les organisations internationales ou régionales, pour renforcer la coopération entre leurs services de détection et de répression.

3. Les États parties s'efforcent de coopérer, dans la mesure de leurs moyens, pour lutter contre les infractions pénales visées par la présente Convention commises au moyen de techniques modernes.

Article : Techniques d'enquête spéciales

1. Si les principes fondamentaux de son système juridique national le permettent, chaque État partie, compte tenu de ses possibilités et conformément aux conditions prescrites dans son droit interne, prend les mesures nécessaires pour permettre le recours à des techniques d'enquête spéciales telles que la surveillance électronique ou d'autres formes de surveillance et les opérations d'infiltration par ses autorités compétentes sur son territoire en vue de combattre efficacement l'utilisation des technologies de l'information et des communications à des fins criminelles.

2. Aux fins des enquêtes sur les infractions visées par la présente Convention, les États parties sont encouragés à conclure, si nécessaire, des accords ou des arrangements bilatéraux ou multilatéraux appropriés pour recourir à ces techniques d'enquête spéciales dans le cadre de la coopération internationale. Ces accords ou

arrangements sont conclus et appliqués conformément au principe de l'égalité souveraine des États et mis en œuvre dans le strict respect des dispositions qu'ils contiennent.

3. En l'absence d'accords ou d'arrangements visés au paragraphe 2 du présent article, la décision de recourir à des techniques d'enquête spéciales au niveau international est prise au cas par cas et peut, si nécessaire, tenir compte d'ententes et d'arrangements financiers quant à l'exercice de leur compétence par les États parties concernés.

4. La décision de recourir à des techniques d'enquête spéciales au niveau international peut inclure, avec le consentement des États parties concernés, des méthodes telles que l'interception de données de trafic et l'autorisation de la poursuite de leur acheminement, sans altération ou après soustraction ou remplacement de la totalité ou d'une partie de ces données.

Article : Transfert des procédures pénales

Les États parties envisagent la possibilité de se transférer mutuellement les procédures relatives à la poursuite d'une infraction pénale visée par la présente Convention dans les cas où ce transfert est jugé être dans l'intérêt d'une bonne administration de la justice, en particulier lorsque plusieurs juridictions sont concernées, en vue de centraliser les poursuites.

Article : Collecte, échange et analyse d'informations sur l'utilisation des technologies de l'information et des communications à des fins criminelles

Les États parties envisagent de développer et de mettre en commun, directement entre eux et par le biais d'organisations internationales et régionales, leurs statistiques et leur connaissance analytique de l'utilisation des technologies de l'information et des communications à des fins criminelles en vue d'élaborer, dans la mesure du possible, des définitions, normes et méthodes communes, ainsi que des informations sur les pratiques les mieux à même de prévenir et de combattre cette utilisation.

Article : Réseau 24/7

1. Chaque État partie désigne un point de contact joignable 24 heures sur 24, 7 jours sur 7, afin d'assurer une assistance immédiate pour des investigations ou des procédures concernant des infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves électroniques d'une infraction pénale. Cette assistance englobera la facilitation ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

a) Prestation de conseils techniques ;

b) Préservation des données conformément aux articles [Préservation accélérée des données informatiques stockées et Divulgation accélérée des données relatives au trafic préservées] ;

c) Recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2. Le point de contact d'un État partie aura les moyens de correspondre avec le point de contact d'un autre État partie selon une procédure accélérée.

3. Si le point de contact désigné par un État partie ne dépend pas de l'autorité ou des autorités de cet État partie responsables de l'entraide internationale ou de l'extradition, il veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

4. Chaque État partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre 5 – Assistance technique

Article : Formation et assistance technique

1. Chaque État partie lance, développe ou améliore, dans la mesure des besoins, des programmes de formation spécifiques à l'intention du personnel de ses services de détection et de répression, y compris des magistrats du parquet, des juges d'instruction, des officiers de justice, des agents des cellules de renseignement financier et des agents des douanes, ainsi que d'autres personnels chargés de prévenir, de détecter et de réprimer les infractions pénales visées par la présente Convention. Ces programmes peuvent comprendre des détachements et des échanges de personnel et portent notamment, et dans la mesure où le droit interne le permet, sur les points suivants :

a) Méthodes employées pour prévenir, détecter et combattre les infractions visées par la présente Convention ;

b) Itinéraires empruntés et techniques employées par les personnes soupçonnées d'implication dans des infractions visées par la présente Convention, y compris dans les États de transit, et mesures de lutte appropriées ;

c) Surveillance du mouvement des données ;

d) Détection et surveillance du mouvement du produit du crime, des biens, des matériels ou des autres instruments, méthodes de transfert, de dissimulation ou de déguisement de ce produit, de ces biens, de ces matériels ou de ces autres instruments, et méthodes de lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ;

e) Recueil d'éléments de preuve ;

f) Matériel moderne de détection et de répression et techniques d'enquête spéciales, y compris la surveillance électronique et les opérations d'infiltration ;

g) Méthodes utilisées dans la lutte contre les infractions pénales commises au moyen des technologies de l'information et des communications ;

h) Méthodes employées pour protéger les victimes et les témoins qui coopèrent avec les autorités judiciaires ;

i) Formation aux réglementations nationales et internationales.

2. Chaque État partie, dans la mesure où cela est nécessaire et possible, lance, développe ou améliore des programmes de formation spécifiques pour les membres du pouvoir judiciaire, y compris les magistrats.

3. Des mesures allant dans le même sens que celles prises en application des paragraphes 1 et 2 du présent article sont instituées et appliquées au sein des services de poursuite dans les États parties où ceux-ci forment un corps distinct, mais jouissent d'une indépendance semblable à celle des juges.

4. Les États parties s'entraident pour planifier et exécuter des programmes de recherche et de formation conçus pour échanger des connaissances spécialisées dans les domaines visés aux paragraphes 1 et 2 du présent article et, à cette fin, mettent aussi à profit, lorsqu'il y a lieu, des conférences et séminaires régionaux et internationaux pour favoriser la coopération et stimuler les échanges de vues sur les problèmes communs, y compris les problèmes et besoins particuliers des États de transit.

5. Les États parties encouragent les activités de formation et d'assistance technique de nature à faciliter l'extradition et l'entraide judiciaire. Ces activités de formation et d'assistance technique peuvent inclure une formation linguistique, des détachements et des échanges entre les personnels des autorités centrales ou des organismes ayant des responsabilités dans les domaines visés.

6. Lorsqu'il existe des accords ou arrangements bilatéraux et multilatéraux en vigueur, les États parties renforcent, autant qu'il est nécessaire, les mesures prises

pour optimiser les activités opérationnelles et de formation au sein des organisations internationales et régionales et dans le cadre d'autres accords ou arrangements bilatéraux et multilatéraux conclus en la matière.

Chapitre 6 – Mesures préventives

Article : Mesures propres à renforcer la coopération avec les services de détection et de répression

1. Chaque État partie prend des mesures appropriées pour encourager les personnes qui participent ou ont participé à l'utilisation des technologies de l'information et des communications à des fins criminelles :

a) À fournir des informations utiles aux autorités compétentes à des fins d'enquête et de recherche de preuves sur des questions telles que :

i) L'identité, la nature, la composition, la structure ou l'emplacement des technologies de l'information et des communications ;

ii) Les liens, y compris internationaux, avec toute personne utilisant les technologies de l'information et des communications à des fins criminelles ;

iii) Les infractions pénales que toute personne utilisant les technologies de l'information et des communications à des fins criminelles a commises ou pourrait commettre ;

b) À fournir aux autorités compétentes une aide substantielle pouvant contribuer à priver toute personne utilisant les technologies de l'information et des communications à des fins criminelles de ses ressources ou du produit du crime.

2. Chaque État partie envisage de prévoir la possibilité, dans les cas appropriés, d'alléger la peine dont est passible un prévenu qui coopère de manière substantielle à l'enquête ou aux poursuites relatives à une infraction pénale visée par la présente Convention.

3. Chaque État partie envisage de prévoir la possibilité, conformément aux principes fondamentaux de son droit interne, d'accorder l'immunité de poursuites à une personne qui coopère de manière substantielle à l'enquête ou aux poursuites relatives à une infraction pénale visée par la présente Convention.

4. La protection des personnes visée aux paragraphes 2 et 3 du présent article est celle prévue à l'article […] de la présente Convention.

5. Lorsqu'une personne visée au paragraphe 1 du présent article se trouve dans un État partie et peut apporter une coopération substantielle aux autorités compétentes d'un autre État partie, les États parties concernés peuvent envisager de conclure des accords ou arrangements, conformément à leur droit interne, concernant l'éventuel octroi, par l'autre État partie, du traitement décrit aux paragraphes 2 et 3 du présent article.

Article : Collecte, échange et analyse d'informations sur la nature de l'utilisation des technologies de l'information et des communications à des fins criminelles

1. Chaque État partie peut analyser, en consultation avec les experts, les tendances de l'utilisation des technologies de l'information et des communications à des fins criminelles sur son territoire, les circonstances dans lesquelles ces infractions sont commises, ainsi que les groupes et les technologies impliqués.

2. Les États parties peuvent mettre en place et partager, entre eux et par l'intermédiaire d'organisations internationales et régionales, des compétences analytiques concernant l'utilisation des technologies de l'information et des communications à des fins criminelles. À cet effet, des définitions, normes et méthodes communes devront être élaborées et appliquées selon qu'il conviendra.

3. Chaque État partie assure le suivi de ses politiques et mesures effectives de lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et procède à des évaluations de leur efficacité et de leur efficience.

Article : Participation de la société

1. Chaque État partie prend des mesures appropriées, dans la limite de ses moyens et conformément aux principes fondamentaux de son droit interne, pour favoriser la participation active de personnes et de groupes n'appartenant pas au secteur public, comme la société civile, les organisations non gouvernementales et les communautés de personnes, à la prévention de l'utilisation des technologies de l'information et des communications à des fins criminelles et à la lutte contre ce phénomène, et pour mieux sensibiliser le public à son existence, à ses causes et à sa gravité ainsi qu'à la menace qu'il représente. Cette participation devrait être renforcée par des mesures consistant notamment à :

a) Accroître la transparence des processus de décision et promouvoir la participation du public à ces processus ;

b) Assurer l'accès effectif du public à l'information ;

c) Entreprendre des activités d'information incitant le public à ne pas tolérer l'utilisation des technologies de l'information et des communications à des fins criminelles, ainsi que des programmes d'éducation, notamment dans les écoles et les universités ; et

d) Respecter, promouvoir et protéger la liberté de rechercher, de recevoir, de publier et de diffuser des informations concernant l'utilisation des technologies de l'information et des communications à des fins criminelles. Cette liberté peut être soumise à certaines restrictions, qui doivent toutefois être prescrites par la loi et nécessaires :

i) Au respect des droits ou de la réputation d'autrui ;

ii) À la protection de la sécurité nationale, de l'ordre public ou de la santé publique.

2. Chaque État partie prend des mesures appropriées pour veiller à ce que les organes compétents de lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles mentionnés dans la présente Convention soient connus du public et fait en sorte qu'ils soient accessibles, lorsqu'il y a lieu, pour que tous faits susceptibles d'être considérés comme constituant une infraction visée par la présente Convention puissent leur être signalés, y compris sous couvert d'anonymat.

Article : Coopération entre autorités nationales et secteur privé

Chaque État partie prend les mesures nécessaires pour encourager, conformément à son droit interne, la coopération entre les autorités nationales chargées des enquêtes et des poursuites et des entités du secteur privé, en particulier les institutions financières et les fournisseurs d'accès à Internet, sur des questions concernant la commission d'infractions pénales visées par la présente Convention.

Chapitre 7 – Mécanisme d'application

Article : Application de la Convention par le développement économique et l'assistance technique

1. Les États parties prennent des mesures propres à assurer l'application optimale de la présente Convention dans la mesure du possible, par la coopération internationale, compte tenu des effets négatifs de l'utilisation des technologies de l'information et des communications à des fins criminelles sur la société en général et sur le développement durable en particulier.

2. Les États parties font des efforts concrets, dans la mesure du possible et en coordination les uns avec les autres ainsi qu'avec les organisations régionales et internationales :

a) Pour développer leur coopération à différents niveaux avec les pays en développement en vue de renforcer la capacité de ces derniers à prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles ;

b) Pour accroître l'assistance financière et matérielle apportée aux pays en développement afin d'appuyer les efforts qu'ils déploient pour prévenir et combattre efficacement l'utilisation des technologies de l'information et des communications à des fins criminelles et de les aider à appliquer la présente Convention avec succès ;

c) Pour fournir une assistance technique à tout État partie qui souhaite être aidé à s'acquitter pleinement des obligations qui lui incombent en vertu de la présente Convention. Pour ce faire, les États parties s'efforcent de verser volontairement des contributions appropriées et régulières à un compte créé à cet effet dans le cadre d'un mécanisme de financement des Nations Unies. Les États parties peuvent aussi envisager spécialement, conformément à leur droit interne et aux dispositions de la présente Convention, de verser au compte susvisé un pourcentage des fonds ou de la valeur correspondante du produit du crime ou des biens confisqués en application des dispositions de la présente Convention ;

d) Pour encourager et convaincre d'autres États et des institutions financières, selon qu'il convient, de s'associer aux efforts faits conformément au présent article, notamment en fournissant aux pays en développement davantage de programmes de formation et de matériel moderne afin de les aider à atteindre les objectifs de la présente Convention.

3. Dans toute la mesure possible, les mesures prises au titre du présent article sont sans préjudice des engagements existants en matière d'aide extérieure ou d'autres arrangements de coopération financière aux niveaux bilatéral, régional ou international.

4. Les États parties peuvent conclure des accords ou des arrangements bilatéraux ou multilatéraux sur l'assistance matérielle et logistique, en tenant compte des arrangements financiers nécessaires pour assurer l'efficacité des moyens de coopération internationale prévus par la présente Convention et pour prévenir, détecter et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Article : Application de la Convention

1. Chaque État partie prend les mesures nécessaires, y compris législatives et administratives, conformément à son droit interne, pour assurer l'exécution de ses obligations en vertu de la présente Convention.

2. Les infractions pénales visées aux articles […] de la présente Convention sont incorporées dans le droit interne de chaque État partie indépendamment de toute personne impliquée dans l'utilisation des technologies de l'information et des communications à des fins criminelles, à l'exception des personnes mentionnées aux paragraphes 2 et 3 de l'article [Mesures propres à renforcer la coopération avec les services de détection et de répression] de la présente Convention.

3. Chaque État partie peut prendre des mesures plus strictes ou plus sévères que celles prévues par la présente Convention pour prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Article : Conférence des Parties à la Convention

1. Une Conférence des Parties à la Convention est instituée pour améliorer la capacité des États parties à combattre l'utilisation des technologies de l'information

et des communications à des fins criminelles et pour promouvoir et examiner l'application de la présente Convention.

2. Le Secrétaire général de l'Organisation des Nations Unies convoque la Conférence des Parties au plus tard un an après l'entrée en vigueur de la présente Convention. La Conférence des Parties adoptera un règlement intérieur et des règles régissant les activités énoncées aux paragraphes 3 et 4 du présent article (y compris des règles relatives au financement des dépenses encourues au titre de ces activités).

3. La Conférence des Parties arrête des mécanismes en vue d'atteindre les objectifs visés au paragraphe 1 du présent article, notamment :

a) Elle facilite les activités menées par les États parties au titre des articles [Formation et assistance technique ; Autres mesures : application de la Convention par le développement économique et l'assistance technique ; et Prévention][1] de la présente Convention, y compris en encourageant la mobilisation de contributions volontaires ;

b) Elle facilite l'échange d'informations entre États parties sur les caractéristiques et tendances de l'utilisation des technologies de l'information et des communications à des fins criminelles et les pratiques efficaces pour la combattre ;

c) Elle coopère avec les organisations régionales et internationales et les organisations non gouvernementales compétentes ;

d) Elle examine à intervalles réguliers l'application de la présente Convention ; et

e) Elle formule des recommandations en vue d'améliorer la présente Convention et son application.

4. Aux fins des alinéas d) et e) du paragraphe 3 du présent article, la Conférence des Parties s'enquiert des mesures adoptées et des difficultés rencontrées par les États parties pour appliquer la présente Convention en utilisant les informations que ceux-ci lui communiquent ainsi que les mécanismes complémentaires d'examen qu'elle pourra établir.

5. Chaque État partie communique à la Conférence des Parties, comme celle-ci le requiert, des informations sur ses programmes, plans et pratiques ainsi que sur les mesures législatives et administratives qu'il prend pour appliquer la présente Convention.

Chapitre 8 – Dispositions finales

Article : Règlement des différends

1. Les États parties s'efforcent de régler les différends concernant l'interprétation ou l'application de la présente Convention par la négociation ou tout autre moyen pacifique.

2. Tout différend entre des États parties concernant l'interprétation ou l'application de la présente Convention qui ne peut être réglé par la négociation ou tout autre moyen pacifique dans un délai raisonnable est, à la demande de l'un de ces États parties, soumis à l'arbitrage. Si, dans un délai de six mois à compter de la date de la demande d'arbitrage, les États parties ne peuvent s'entendre sur l'organisation de ce dernier, l'un quelconque d'entre eux peut soumettre le différend à la Cour internationale de Justice en adressant une requête conformément au Statut de la Cour.

3. Chaque État partie peut, au moment de la signature, de la ratification, de l'acceptation ou de l'approbation de la présente Convention ou de l'adhésion à celle-ci, déclarer qu'il ne se considère pas lié par le paragraphe 2 du présent article.

[1] Ces dispositions sont tirées des articles 29, 30 et 31 de la Convention des Nations Unies contre la criminalité transnationale organisée.

Les autres États parties ne sont pas liés par le paragraphe 2 du présent article envers tout État partie ayant émis une telle réserve.

4. Tout État partie qui a émis une réserve en vertu du paragraphe 3 du présent article peut la retirer à tout moment en adressant une notification au Secrétaire général de l'Organisation des Nations Unies.

Article : Signature, ratification, acceptation, approbation et adhésion

1. La présente Convention est ouverte à la signature de tous les États du [date] au [date] à [lieu].

2. La présente Convention est également ouverte à la signature des organisations régionales d'intégration économique à la condition qu'au moins un État membre d'une telle organisation l'ait signée conformément au paragraphe 1 du présent article.

3. La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation seront déposés auprès du Secrétaire général de l'Organisation des Nations Unies.

4. Une organisation régionale d'intégration économique qui a signé la présente Convention peut déposer son instrument de ratification, d'acceptation ou d'approbation si au moins un de ses États membres l'a fait. Dans cet instrument de ratification, d'acceptation ou d'approbation, cette organisation déclare l'étendue de sa compétence concernant les questions régies par la présente Convention. Elle informe également le dépositaire de toute modification pertinente de l'étendue de sa compétence.

5. La présente Convention est ouverte à l'adhésion de tout État ou de toute organisation régionale d'intégration économique dont au moins un État membre est partie à la présente Convention. Les instruments d'adhésion seront déposés auprès du Secrétaire général de l'Organisation des Nations Unies. Au moment de son adhésion, une organisation régionale d'intégration économique déclare l'étendue de sa compétence concernant les questions régies par la présente Convention. Elle informe également le dépositaire de toute modification pertinente de l'étendue de sa compétence.

Article : Entrée en vigueur

1. La présente Convention entre en vigueur le [quatre-vingt-dixième jour suivant la date du dépôt du cinquantième instrument de ratification], d'acceptation, d'approbation ou d'adhésion. Aux fins du présent paragraphe, aucun des instruments déposés par une organisation régionale d'intégration économique n'est considéré comme un instrument venant s'ajouter aux instruments déjà déposés par les États membres de cette organisation.

2. Pour chaque État ou organisation régionale d'intégration économique qui ratifiera, acceptera ou approuvera la présente Convention ou y adhérera après le dépôt du quarantième instrument pertinent, la présente Convention entrera en vigueur le trentième jour suivant la date de dépôt de l'instrument pertinent par ledit État ou ladite organisation.

Article : Amendement

1. À l'expiration d'un délai de cinq ans à compter de l'entrée en vigueur de la présente Convention, un État partie peut proposer un amendement et en déposer le texte auprès du Secrétaire général de l'Organisation des Nations Unies. Ce dernier communique alors la proposition d'amendement aux États parties et à la Conférence des Parties à la Convention en vue de l'examen de la proposition et de l'adoption d'une décision. La Conférence des Parties n'épargne aucun effort pour parvenir à un consensus sur toute proposition de modification. Si tous les efforts en ce sens ont été épuisés sans qu'un accord soit intervenu, il faudra, en dernier recours, pour que

l'amendement soit adopté, un vote à la majorité des deux tiers des États parties présents à la Conférence des Parties et exprimant leur vote.

2. Les organisations régionales d'intégration économique disposent, pour exercer, en vertu du présent article, leur droit de vote dans les domaines qui relèvent de leur compétence, d'un nombre de voix égal au nombre de leurs États membres parties à la présente Convention. Elles n'exercent pas leur droit de vote si leurs États membres exercent le leur, et inversement.

3. Un amendement adopté conformément au paragraphe 1 du présent article est soumis à la ratification, à l'acceptation ou à l'approbation des États parties.

4. Un amendement adopté conformément au paragraphe 1 du présent article entrera en vigueur pour un État partie quatre-vingt-dix jours après la date de dépôt par ledit État partie auprès du Secrétaire général de l'Organisation des Nations Unies d'un instrument de ratification, d'acceptation ou d'approbation dudit amendement.

5. Un amendement entré en vigueur a force obligatoire à l'égard des États parties qui ont exprimé leur consentement à être liés par lui. Les autres États parties restent liés par les dispositions de la présente Convention et tous amendements antérieurs qu'ils ont ratifiés, acceptés ou approuvés.

Article : Dénonciation

1. Tout État partie peut dénoncer la présente Convention par notification écrite adressée au Secrétaire général de l'Organisation des Nations Unies et cette dénonciation prendra effet un an après la date de réception de la notification par le Secrétaire général.

2. Une organisation régionale d'intégration économique cesse d'être partie à la présente Convention lorsque tous ses États membres l'ont dénoncée.

3. La dénonciation de la présente Convention conformément au paragraphe 1 du présent article entraîne la dénonciation de tout protocole y relatif.

Article : Dépositaire et langues

1. Le Secrétaire général de l'Organisation des Nations Unies est le dépositaire de la présente Convention.

2. L'original de la présente Convention, dont les textes anglais, arabe, chinois, espagnol, français et russe font également foi, est déposé auprès du Secrétaire général de l'Organisation des Nations Unies.

EN FOI DE QUOI, les plénipotentiaires soussignés, à ce dûment autorisés par leurs gouvernements respectifs, ont signé la présente Convention.

Préambule

Les États parties à la présente Convention,

Ayant à l'esprit les buts et principes de la Charte des Nations Unies et la mission qu'ont les Nations Unies d'harmoniser l'action menée par les nations pour atteindre ces buts et respecter ces principes,

Convaincus que les infractions commises au moyen des technologies de l'information et des communications sont des infractions transnationales et qu'elles exigent donc une réponse globale de tous les États,

Reconnaissant que le développement des technologies de l'information et des communications ces deux dernières décennies a révolutionné la façon dont les sociétés fonctionnent,

Reconnaissant également que si les technologies de l'information et des communications ont contribué de manière significative au développement des États, l'évolution de ces technologies et leur utilisation accrue ont fait apparaître de

nouvelles possibilités, pour les personnes mal intentionnées, de mésuser de ces technologies pour mener des activités criminelles,

Profondément préoccupés par la menace internationale et nationale que les infractions commises au moyen des technologies de l'information et des communications font peser sur les sociétés, ainsi que par son impact sur le bien-être des individus,

Considérant que les infractions commises au moyen des technologies de l'information et des communications constituent un motif de grave préoccupation pour l'ensemble de la communauté internationale, ce qui rend essentielle la mise en place d'une coopération internationale pour les prévenir et les combattre,

Convaincus de la nécessité de mettre en place des mesures pénales communes pour protéger la société contre le fléau de ces infractions par la mise en œuvre de dispositions législatives et administratives appropriées,

Convaincus également que la présente Convention est nécessaire pour prévenir le mésusage des technologies de l'information et des communications et faciliter, au niveau tant national qu'international, la détection, l'instruction et la poursuite des infractions pénales commises au moyen de ces technologies,

Reconnaissant la nécessité, pour les États, de défendre et de respecter les droits humains et les principes fondamentaux d'une procédure régulière et de la primauté du droit dans les procédures pénales, civiles ou administratives lorsqu'ils agissent en application des mesures instituées par la présente Convention,

Reconnaissant également les principes de souveraineté, d'égalité souveraine et d'intégrité territoriale des États,

Convaincus que l'offre d'assistance technique peut grandement contribuer à rendre les États mieux à même, y compris par le renforcement des capacités et des institutions, de prévenir et de combattre efficacement les infractions commises au moyen des technologies de l'information et des communications,

Rappelant la résolution 74/247 de l'Assemblée générale du 27 janvier 2019, dans laquelle l'Assemblée a décidé que le Comité spécial créé en vertu de cette résolution devrait élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles,

Sont convenus de ce qui suit :

Nouvelle-Zélande

Original : anglais
[15 juillet 2022]

1. La Nouvelle-Zélande a le plaisir de répondre à l'invitation faite 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 des propositions pour la troisième session de négociation, qui se tiendra du 29 août au 9 septembre, sur les points suivants :

- Coopération internationale ;
- Assistance technique ;
- Mesures préventives ;
- Mécanisme d'application ;
- Dispositions finales ;
- Préambule.

2. Dans la présente communication, la Nouvelle-Zélande présente des propositions concernant les chapitres relatifs à la coopération internationale, aux mesures préventives et à l'assistance technique. Outre ces propositions, nous fournissons (entre parenthèses) des exemples tirés d'autres instruments internationaux pertinents, qui pourraient constituer une bonne base de négociation. Nous attendons avec intérêt de nouvelles discussions constructives sur toutes les questions lors de la troisième session de négociation.

Des dispositions efficaces sur la coopération internationale, la prévention et l'assistance technique vont de pair

3. La Nouvelle-Zélande estime que la présente convention devrait viser à combattre la cybercriminalité et à améliorer les mesures internationales à cette fin, notamment au moyen d'une coopération internationale accrue, de mesures de prévention efficaces et d'une assistance technique solide pour assurer une application universelle. Le renforcement des capacités est un élément essentiel. Une convention ne peut être véritablement efficace que si tous les États parties sont en mesure d'en respecter les dispositions.

Nous devons nous fonder sur les instruments existants et assurer la cohérence avec les obligations en matière de droits humains

4. La nouvelle convention ne devrait pas entrer en conflit avec les instruments en vigueur ou les obligations ou pratiques existantes en matière d'entraide judiciaire et de partage d'informations, ni les mettre en péril, mais plutôt en tenir compte et s'en inspirer le cas échéant. En outre, tous les aspects de la convention devraient être conformes aux obligations internationales existantes des États en matière de droits humains, qui s'appliquent en ligne comme hors ligne, notamment le droit à la liberté d'expression et le droit de ne pas subir d'immixtions arbitraires ou illégales dans sa vie privée.

Coopération internationale

5. Compte tenu de leur nature souvent transnationale et transfrontalière, les enquêtes et les poursuites en matière de cybercriminalité exigent une coopération internationale efficace, notamment l'accès en temps utile aux données et aux preuves électroniques pertinentes.

Entraide judiciaire

6. Les dispositions existantes relatives à l'entraide judiciaire (Convention des Nations Unies contre la criminalité transnationale organisée, art. 18, et Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), art. 25) constituent une bonne base pour nos négociations. En règle générale, les États parties s'accordent mutuellement l'entraide judiciaire la plus large possible lors des enquêtes, poursuites et procédures judiciaires concernant les infractions visées par la présente convention, dans le plein respect des droits humains et des libertés fondamentales.

7. Nous reconnaissons également que les régimes et les pratiques actuels en matière d'entraide judiciaire ne sont pas toujours bien adaptés pour lutter contre la cybercriminalité, domaine où des interventions rapides et agiles sont nécessaires pour garantir la préservation et le partage rapide des informations. Dans la mesure du possible, nous devrions nous efforcer d'améliorer la cohérence et la rapidité avec laquelle il est donné suite aux demandes d'entraide judiciaire, notamment en élaborant des pratiques optimales visant à normaliser les procédures d'entraide judiciaire et en les diffusant.

8. Compte tenu de la complexité des enquêtes sur la cybercriminalité et de la nécessité d'un accès rapide aux données, la convention devrait inclure (sous réserve de garanties procédurales solides et de protections en matière de droits humains) des dispositions relatives aux demandes d'entraide judiciaire portant sur les questions visées à l'article 18 3) a) à i) de la Convention contre la criminalité organisée, et plus

particulièrement en ce qui concerne la collecte de preuves sous forme électronique, les demandes d'entraide judiciaire portant sur :

- La conservation de données informatiques à l'égard desquelles un État a l'intention de présenter une demande d'entraide judiciaire (Convention de Budapest, art. 29) ;
- La perquisition, l'accès, la saisie, l'obtention et la divulgation de données stockées au moyen d'un système informatique (Convention de Budapest, art. 31) ;
- La collecte en temps réel de données relatives au trafic, associées à des communications spécifiques, transmises au moyen d'un système informatique, comme régie par le droit interne des États (Convention de Budapest, art. 31) ;
- La collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique, dans la mesure où les traités et les lois nationales applicables le permettent (Convention de Budapest, art. 31) ;
- Sous réserve de garanties appropriées, la Nouvelle-Zélande pourrait soutenir une disposition autorisant les demandes d'entraide judiciaire par les moyens les plus rapides pour la divulgation de données informatiques dans les cas d'urgence, par exemple lorsqu'il existe un risque important et imminent pour la vie ou la sécurité d'une personne ;
- La présente convention devrait encourager la création d'autorités centrales bien dotées en ressources et bien formées pour répondre aux demandes d'entraide judiciaire et promouvoir des normes élevées, par exemple en veillant à ce que les informations fournies puissent répondre aux exigences en matière de preuve lorsqu'elles sont demandées à cette fin.

9. Sous réserve de l'inclusion, dans la convention, de garanties et de protections solides en matière de droits humains, la Nouvelle-Zélande pourrait soutenir l'extension de certains aspects des dispositions relatives à la collecte, à la conservation et au partage des preuves électroniques afin qu'elles s'appliquent également à des infractions pénales suffisamment graves autres que les infractions établies dans la convention.

10. La convention devrait donner aux États parties la possibilité de refuser de donner suite à une demande d'entraide parce que l'exécution de cette demande pourrait porter atteinte à leur souveraineté, leur sécurité, à l'ordre public ou à d'autres intérêts fondamentaux. En outre, les États parties devraient pouvoir refuser de donner suite à une demande d'entraide conformément à leur législation nationale, notamment en l'absence de double incrimination, en cas d'infractions politiques/de motivations politiques ; mais pas au motif que l'infraction est également considérée comme touchant aussi à des questions fiscales (Convention contre la criminalité organisée, art. 18, par. 21 et 22).

Extradition

11. La convention doit contenir des dispositions relatives à l'extradition qui s'appliquent aux infractions qu'elle vise. L'article 16 de la Convention contre la criminalité organisée constitue une bonne base de négociation et, comme pour l'entraide judiciaire, les États parties devraient pouvoir refuser les demandes d'extradition pour les motifs établis par leur droit interne et les traités applicables. La Nouvelle-Zélande soutient l'adoption d'une disposition prévoyant que chaque État puisse établir sa compétence à l'égard des infractions établies par la convention lorsque l'auteur présumé se trouve sur son territoire et qu'il ne l'extrade pas. Nous sommes également disposés à examiner l'opportunité d'inclure dans la présente convention une obligation contraignante d'envisager des poursuites dans certaines circonstances (*aut dedere aut judicare*), par exemple dans les cas où les infractions sont suffisamment graves pour déclencher une obligation contraignante.

Point de contact joignable 24 heures sur 24, 7 jours sur 7

12. La Nouvelle-Zélande est favorable à l'inclusion d'une disposition sur la création d'un système de point de contact joignable 24 heures sur 24, 7 jours sur 7 (Convention de Budapest, art. 35), afin d'assurer une assistance rapide pour les enquêtes sur la cybercriminalité et la collecte de preuves électroniques. Nous proposons en outre d'examiner les instruments et cadres existants relatifs à la communication entre les points de contact 24/7. Nous notons également que, d'un État à l'autre, il existe divers degrés de capacité à fournir et à maintenir un système de point de contact unique joignable 24 heures sur 24, 7 jours sur 7. Par conséquent, nous sommes d'avis que les dispositions de la convention sur le renforcement des capacités devraient garantir que les États disposeront à la fois des ressources et de la formation nécessaires pour respecter cette norme.

Coopération entre les services de détection et de répression

13. Afin d'adopter une approche proactive de la coopération internationale, la convention devrait encourager la coopération entre les autorités compétentes et le partage spontané d'informations ou de données relatives aux enquêtes ou aux procédures, dans les limites imposées par le droit interne et dans la lutte commune contre les actes criminels (Convention de Budapest, art. 26, Convention contre la criminalité organisée, art. 18-4, et Convention contre la corruption, art. 46-4)

Enquêtes conjointes

14. La convention devrait inclure des dispositions encourageant les États parties à conclure des accords ou des arrangements bilatéraux ou multilatéraux qui permettraient de créer des instances d'enquête conjointes en ce qui concerne les infractions visées par la convention. En l'absence de tels arrangements formels, les États parties devraient autoriser les enquêtes conjointes au cas par cas (Convention contre la criminalité organisée, art. 19).

Assistance technique

15. Des mesures efficaces de renforcement des capacités augmenteront la probabilité d'une vaste application de la convention et réduiront les possibilités pour les cybercriminels de se réfugier en lieu sûr. La convention devrait inclure des dispositions sur la formation et l'assistance technique (Convention contre la criminalité organisée, art. 29) et sur l'application effective de la convention par le développement économique et l'assistance technique (Convention contre la criminalité organisée, art. 30).

16. Les mesures de renforcement des capacités prévues par la convention devraient mettre l'accent sur l'utilité de la formation et du partage des meilleures pratiques, notamment en ce qui concerne la réponse efficace aux demandes d'entraide judiciaire, la préservation des preuves électroniques et les techniques de partage des preuves. À cet égard, nous notons que l'Office des Nations Unies contre la drogue et le crime (ONUDC) a acquis une expérience importante dans la mise au point de tels outils, notamment de guides relatifs aux demandes d'entraide judiciaire, aux demandes de divulgation volontaire, aux demandes de préservation et aux demandes de divulgation d'urgence. Nous pourrions donc envisager un rôle pour l'ONUDC, ainsi que pour d'autres organisations ayant une expérience dans la facilitation de la coopération internationale en matière de répression, comme l'Organisation internationale de police criminelle (INTERPOL), dans la mise en œuvre des programmes de renforcement des capacités nécessaires pour garantir l'efficacité de ce traité.

Prévention

17. Cette convention devrait reconnaître l'importance de la coopération multisectorielle dans la lutte contre la cybercriminalité, y compris l'importance de l'établissement d'un cadre de coopération entre les gouvernements et les acteurs du

secteur privé fondé sur la confiance et la transparence. En outre, la Nouvelle-Zélande reconnaît qu'il importe de promouvoir la participation de l'ensemble de la société pour prévenir efficacement la cybercriminalité. La convention devrait favoriser une large participation à cet égard (Convention contre la corruption, art. 13).

18. La Nouvelle-Zélande est d'avis que la convention devrait encourager les mesures qui soulignent l'importance de sensibiliser la société aux risques de la cybercriminalité au moyen de campagnes d'éducation et de formation.

19. En outre, la convention devrait favoriser une approche de la prévention de la cybercriminalité fondée sur des données probantes, notamment en analysant les tendances de la cybercriminalité et leur incidence sur les sociétés, y compris les femmes, les enfants et les autres groupes vulnérables. Ce travail doit être effectué en consultation avec les acteurs concernés du secteur privé, les universitaires, les groupes autochtones et les organisations non gouvernementales intéressées (Convention contre la criminalité organisée, art. 28). De même, la convention pourrait également inclure des dispositions qui encouragent les États parties, conformément au droit national, à favoriser la coopération entre les services de détection et de répression et les acteurs concernés du secteur privé dans la lutte contre l'activité criminelle établie dans le cadre de la présente convention (Convention contre la corruption, art. 39-1).

Viet Nam

Original : anglais
[19 juillet 2022]

A. Mesures préventives

1. Politiques et pratiques visant à prévenir et à combattre la cybercriminalité/l'utilisation des technologies de l'information et des communications à des fins criminelles

1. Les États parties s'efforcent d'établir et de promouvoir les meilleures pratiques et politiques visant à prévenir la cybercriminalité/l'utilisation des technologies de l'information et des communications (TIC) à des fins criminelles et autres actes illicites liés à l'utilisation des TIC.

2. Les États parties s'efforcent d'empêcher que leur propre territoire ou les systèmes informatiques/systèmes de TIC/dispositifs de TIC situés sur leur territoire soient utilisés à des fins criminelles contre d'autres tiers et/ou citoyens des autres parties.

3. Conformément aux principes fondamentaux de leur droit interne, les États parties s'efforcent de réduire, par des mesures législatives, administratives ou autres appropriées, les possibilités actuelles ou futures des cybercriminels/criminels utilisant les TIC de participer à l'activité des marchés licites en utilisant le produit du crime. Ces mesures devraient inclure la promotion de règlements et procédures conçus pour superviser le commerce des actifs virtuels et les plateformes d'échange de cryptomonnaies.

4. Les États parties s'efforcent de prendre des mesures appropriées pour prévenir la récidive, y compris la récidive visant des victimes dans d'autres États parties.

5. Les États parties collaborent, selon qu'il convient et conformément aux principes fondamentaux de leur système juridique, avec les autres États membres, les organisations gouvernementales et les organisations internationales et régionales compétentes pour la promotion et la mise au point des mesures visées dans le présent article.

6. Les États parties s'efforcent de promouvoir la réinsertion dans la société des personnes reconnues coupables d'infractions visées par la présente convention.

2. Sensibilisation du public à la prévention de la cybercriminalité

1. Les États parties s'efforcent de mieux sensibiliser le public à l'existence, aux nouvelles formes, aux caractéristiques, à la gravité de la cybercriminalité/de l'utilisation des TIC à des fins criminelles et à la menace que représente ce phénomène.

2. Les États parties encouragent les organismes publics à coopérer avec les organisations privées et d'autres personnes pour mettre en œuvre des programmes d'éducation, de formation et de sensibilisation du public sur la prévention de la cybercriminalité/l'utilisation des TIC à des fins criminelles et la lutte contre ce phénomène.

3. Secteur public

1. Les États parties prennent des mesures appropriées, conformément aux principes fondamentaux de leur droit interne, pour prévenir les infractions visées par la présente convention et les autres actes de cybercriminalité/l'utilisation des TIC à des fins criminelles au sein des organisations gouvernementales.

2. Les États parties prennent des mesures appropriées, conformément aux principes fondamentaux de leur droit interne, pour empêcher que les systèmes informatiques/systèmes de TIC/dispositifs et ressources informatiques placés sous le contrôle d'organisations gouvernementales ne soient utilisés abusivement pour commettre les infractions visées par la présente convention et d'autres actes relevant de la cybercriminalité/de l'utilisation des TIC à des fins criminelles.

4. Secteur privé

1. Chaque État partie prend des mesures appropriées, dans la limite de ses moyens et conformément aux principes fondamentaux de son droit interne, pour promouvoir la participation active du secteur privé, y compris des fournisseurs de services Internet, à la prévention de la cybercriminalité/de l'utilisation des TIC à des fins criminelles et à la lutte contre ce phénomène.

2. Chaque État partie prend les mesures appropriées, conformément aux principes fondamentaux de son droit interne, pour prévenir les infractions visées par la présente convention et les autres actes de cybercriminalité/l'utilisation des TIC à des fins criminelles dans le secteur privé.

5. Contrôle des produits

Les États parties s'efforcent, conformément aux principes fondamentaux de leur droit interne, d'établir des politiques de contrôle de la qualité des produits appliqués à la protection des systèmes informatiques/dispositifs de TIC avant que ces produits ne soient mis à la disposition du public.

B. Coopération internationale

6. Coopération internationale

1. Les États parties coopèrent pour enquêter sur les infractions visées par la présente Convention ainsi que sur tout autre acte de cybercriminalité/toute utilisation des TIC à des fins criminelles. Lorsqu'il y a lieu et conformément à leur système juridique interne, les États parties envisagent de se prêter mutuellement assistance dans les enquêtes et les procédures concernant la cybercriminalité et l'utilisation des TIC à des fins criminelles.

2. En matière de coopération internationale, chaque fois que la double incrimination est considérée comme une condition, celle-ci est réputée remplie, que la législation de l'État partie requis qualifie ou désigne ou non l'infraction de la même manière que l'État partie requérant, si l'acte constituant l'infraction pour laquelle

l'assistance est demandée est une infraction pénale en vertu de la législation des deux États parties[2].

7. *Coopération internationale en matière de sensibilisation du public*

1. Les États parties coopèrent pour mieux sensibiliser le public à l'existence, aux nouvelles formes, aux caractéristiques, à la gravité de la cybercriminalité/l'utilisation des TIC à des fins criminelles et à la menace que représente ce phénomène.

2. Les États parties coopèrent pour mettre en œuvre des programmes d'éducation, de formation et de sensibilisation du public sur la prévention de la cybercriminalité/l'utilisation des TIC à des fins criminelles et la lutte contre ce phénomène.

8. *Échange d'informations*

Chaque État partie, conformément aux principes fondamentaux de son droit interne, adopte des mesures efficaces pour renforcer les voies de communication existantes entre ses autorités compétentes et les autorités compétentes d'un autre État partie et, si nécessaire, en établir ainsi que les utiliser afin de faciliter l'échange sûr et rapide d'informations concernant tous les aspects des infractions visées par la présente convention, notamment pour alerter les autres parties, y compris, si les parties intéressées le jugent approprié, les liens avec d'autres activités criminelles.

9. *Gel, saisie et confiscation*

L'article 31 de la Convention des Nations Unies contre la corruption et l'article 12 de la Convention des Nations Unies contre la criminalité transnationale organisée s'appliquent, *mutatis mutandis*, aux actes de cybercriminalité/d'utilisation des TIC à des fins criminelles. Toutefois, la notion de produit du crime devrait être définie de manière à couvrir les cryptomonnaies ou autres données dont la valeur peut être identifiée sur le marché.

10. *Dispositions types sur le recouvrement d'avoirs*

Les États parties s'accordent mutuellement la coopération et l'assistance les plus étendues en ce qui concerne la restitution d'avoirs.

11. *Mesures de recouvrement direct des biens*

L'article 53 de la Convention contre la corruption s'applique, *mutatis mutandis*, aux actes de cybercriminalité/à l'utilisation des TIC à des fins criminelles.

12. *Mécanismes de recouvrement de biens par la coopération internationale aux fins de confiscation*

L'article 54 de la Convention contre la corruption s'applique, *mutatis mutandis*, aux actes de cybercriminalité/à l'utilisation des TIC à des fins criminelles.

13. *Coopération internationale aux fins de confiscation*

L'article 55 de la Convention contre la corruption s'applique, *mutatis mutandis*, aux actes de cybercriminalité/à l'utilisation des TIC à des fins criminelles.

---

[2] Par exemple, le serveur utilisé pour l'exploitation des jeux de hasard en ligne et l'organisation qui exploite cette plateforme située dans un État partie où les jeux de hasard en ligne, même non réglementés, ne constituent pas une infraction en tant que telle, impliquent la fraude fiscale, l'exploitation, la traite des êtres humains, etc.

C. Assistance technique

14. Assistance technique

1. Les États parties s'efforcent de fournir, sous réserve de la disponibilité des ressources, des programmes d'assistance technique aux États parties en développement et aux États parties les moins avancés, à la demande de ces derniers, afin de renforcer les capacités des autorités compétentes chargées de la prévention, de la détection et du contrôle des infractions visées par la présente convention. Ces programmes pourraient inclure les éléments ci-après :

a) Renforcement des capacités et développement des capacités en matière d'élaboration des politiques ;

b) Mise en commun de données d'expérience et de meilleures pratiques en matière de prévention, de détection, d'investigation et de répression des actes de cybercriminalité/de l'utilisation des TIC à des fins criminelles, y compris la collecte, l'analyse, la récupération des données numériques, et les méthodes d'investigation dans le cyberespace ;

c) Réponse efficace en cas de cyberincidents ;

d) Mesures efficaces pour sauvegarder les infrastructures nationales d'information critiques ;

e) Solutions pour la sécurité des données, y compris en ce qui concerne les données personnelles ;

f) Formation d'experts en cybersécurité et en défense des réseaux informatiques ;

g) Meilleure sensibilisation du public et pratiques optimales pour une utilisation sûre de l'Internet.

2. Les États parties s'entraident pour planifier et exécuter des programmes de recherche et de formation conçus pour échanger des connaissances spécialisées dans les domaines visés au paragraphe 1 du présent article et, à cette fin, ils favorisent également, le cas échéant, la coopération et encouragent les échanges de vues sur des questions d'intérêt commun dans le cadre de conférences et de séminaires régionaux et internationaux.

3. Les États parties encouragent le dialogue et les échanges entre les autorités compétentes, notamment par le biais de détachements de personnel et de programmes de renforcement et de développement des capacités.

4. Les États parties favorisent le transfert de technologies, d'équipements, de logiciels et de solutions techniques visant à prévenir et à combattre la cybercriminalité/l'utilisation des TIC à des fins criminelles.