Nations Unies A/AC.291/9/Add.2

Assemblée générale

Distr. générale
21 avril 2022
Français
Original : anglais/arabe/espagnol/
russe

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
Deuxième session
Vienne, 30 mai-10 juin 2022

Compilation des propositions et contributions communiquées par les États Membres sur les dispositions relatives à l'incrimination, les dispositions générales et les dispositions relatives aux mesures procédurales, à la détection et à la répression d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

Additif

V.22-02336 (F) 030622 060622

Table des matières

IV. Mesures procédurales, détection et répression

Angola

[Original : anglais]
[8 avril 2022]

Mesures procédurales, détection et répression

Moyens de preuve : preuve documentaire (document électronique, document numérique), témoignage d'expert (expertise informatique).

Moyens d'obtention de preuves : recherches en ligne, conservation rapide des données, divulgation rapide des données, injonction de communiquer des données ou d'accorder l'accès aux données, recherche de données informatiques, saisie de données informatiques, saisie de courrier électronique et enregistrement de communications de nature similaire, interception de communication, actions cachées (deepweb et darkweb).

Recouvrement d'avoirs et perte d'actifs en faveur de l'État : saisie et confiscation d'actifs traditionnels et de cryptoactifs.

Les dispositions de ce chapitre devraient s'appliquer aux enquêtes et aux poursuites pénales à l'encontre des auteurs d'infractions classiques et pas seulement aux enquêtes sur la cybercriminalité.

Pour l'élaboration des concepts liés à ce chapitre, il est possible de recourir aux instruments juridiques régionaux et internationaux mentionnés ci-dessus[1].

Australie

[Original : anglais]
[8 avril 2022]

Le lien entre l'incrimination et les pouvoirs procéduraux

L'Australie reconnaît que les États souhaiteront peut-être s'assurer que la Convention améliore la coopération internationale pour les infractions courantes avec ou sans dimension cybernétique (telles que la violation de domicile ou le meurtre) et constitue un cadre pour les demandes de preuves électroniques se trouvant dans un autre pays et l'accès à ces données, en relation avec la commission de telles infractions.

Les pouvoirs procéduraux, les pouvoirs d'enquête et les cadres de coopération internationale prévus par la Convention pour détecter les infractions de cybercriminalité, enquêter à leur sujet et en poursuivre les auteurs devraient s'appliquer aux infractions énumérées dans la Convention, mais ne devraient pas être limités pour ne s'appliquer qu'à ces infractions.

Les pouvoirs procéduraux (décrits en détail ci-dessous) prévus par la Convention devraient s'appliquer à d'autres infractions pénales commises au moyen d'un système informatique ou d'une technologie numérique, ainsi qu'à la collecte des preuves électroniques nécessaires pour détecter les infractions pénales qui ne sont pas commises à l'aide d'un système informatique, enquêter à leur sujet et en poursuivre

[1] Note du Secrétariat : cette référence renvoie à des instruments qui figurent dans une autre section : Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, Convention du Conseil de l'Europe sur la cybercriminalité, Convention des Nations Unies contre la criminalité transnationale organisée et Convention des Nations Unies contre la corruption.

les auteurs, et qui répondent aux conditions et aux seuils prescrits pour ces pouvoirs procéduraux.

De même, le cadre de coopération internationale prévu par cette convention devrait s'appliquer non seulement aux infractions pénales établies par la convention, mais aussi, le cas échéant, à d'autres infractions pénales commises au moyen d'un système informatique, ainsi qu'à la collecte des preuves électroniques nécessaires pour détecter les infractions pénales cybernétiques, enquêter à leur sujet et en poursuivre les auteurs.

Par conséquent, l'objectif du chapitre sur l'incrimination n'est pas de restreindre le fonctionnement des autres chapitres de la Convention, mais plutôt d'établir une norme commune pour une forme de criminalité relativement nouvelle (la cybercriminalité) dans tous les États.

Mesures procédurales pour lutter contre la cybercriminalité

Le droit procédural est un élément essentiel des enquêtes et des poursuites en matière de cybercriminalité. La Convention devrait fournir un cadre clair de mesures procédurales pour que les services de détection et de répression puissent obtenir les preuves nécessaires à la lutte contre ce phénomène, fondé sur des garanties et des restrictions procédurales solides qui préservent l'état de droit et des protections en matière de droits humains et de libertés fondamentales. Les articles de la Convention relatifs aux mesures procédurales devraient également respecter les cadres existants et éviter la fragmentation des instruments internationaux existants.

Les mesures procédurales devraient s'appliquer aux infractions pénales proprement dites visées par la Convention et, conformément aux cadres juridiques nationaux des États, aux autres infractions pénales commises au moyen d'un système informatique ou d'une technologie numérique, ainsi qu'à la collecte des preuves électroniques nécessaires pour détecter les infractions pénales cybernétiques, enquêter à leur sujet et en poursuivre les auteurs, et qui répondent aux conditions et aux seuils prescrits pour ces pouvoirs procéduraux.

L'Australie propose que les mesures procédurales suivantes soient prises en compte dans la nouvelle Convention :

- Injonctions de préservation des données électroniques (y compris les données de contenu stockées, les informations sur les abonnés et les données de trafic) ;
- Injonctions de production de données électroniques ;
- Perquisition et saisie de données informatiques stockées ;
- Collecte en temps réel de données électroniques (y compris les données de trafic et l'interception en direct de données de contenu) ;
- Injonctions de préservation et de production rapides et urgentes de données.

Les mesures procédurales devraient tenir compte de la nature des données électroniques, de sorte que les données soient préservées rapidement et efficacement, et que les services de détection et de répression et d'autres autorités compétentes puissent obtenir ces données rapidement et efficacement et que les méthodologies et pratiques criminelles dans le cyberespace n'anéantissent pas les efforts de collecte des autorités concernées.

Conditions, exigences et garanties pour les mesures procédurales

Les mesures procédurales visant à détecter la cybercriminalité, enquêter à ce sujet et en poursuivre les auteurs peuvent entraîner des obligations en matière de droits humains et de libertés au titre des instruments internationaux pertinents relatifs aux droits humains, notamment du Pacte international relatif aux droits civils et politiques. Il s'agit notamment de ce qui suit :

Droits à un procès équitable et droit à ce que la cause soit entendue équitablement, (Pacte international relatif aux droits civils et politiques, article 14)

L'article 14 du Pacte prévoit le droit à un procès équitable et le droit à ce que la cause soit entendue équitablement, y compris des garanties procédurales, la primauté du droit et la présomption d'innocence. Le Comité des droits de l'homme a déclaré que « l'article 14 du Pacte vise à assurer une bonne administration de la justice, et à cette fin, protège une série de droits spécifique ».

L'article 14 n'est pas un droit absolu, il est soumis à des restrictions admissibles, à condition que ces restrictions soient prévues par la loi et constituent des moyens raisonnables, nécessaires et proportionnés à la poursuite d'un objectif légitime.

Liberté de ne pas subir d'immixtions dans sa vie privée (Pacte international relatif aux droits civils et politiques, article 17)

L'article 17 du Pacte établit le droit à la liberté de ne pas subir d'immixtions dans sa vie privée et prévoit que « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance ».

Le contenu de ce droit est décrit plus en détail dans l'observation générale n° 16 du Comité des droits de l'homme, qui précise que « la protection de ce droit doit être garantie contre toutes ces immixtions et atteintes, qu'elles émanent des pouvoirs publics ou de personnes physiques ou morales ». Aux termes du paragraphe 3 de l'observation générale n° 16, « l'adjectif " illégal " signifie qu'aucune immixtion ne peut avoir lieu, sauf dans les cas envisagés par la loi. Les immixtions autorisées par les États ne peuvent avoir lieu qu'en vertu d'une loi, qui doit elle-même être conforme aux dispositions, aux buts et aux objectifs du Pacte ».

Le droit à la liberté d'expression (Pacte international relatif aux droits civils et politiques, article 19, paragraphe 2)

L'article 19 du Pacte prévoit le droit à la liberté d'expression. Le paragraphe 2 de l'article 19 du Pacte reconnaît le droit de chercher, de recevoir et de répandre des informations et des idées par quelque moyen que ce soit, notamment sous une forme orale ou écrite, par la diffusion dans les médias et la publicité commerciale.

Le droit à la liberté d'expression n'est pas un droit absolu. En vertu du paragraphe 3 de l'article 19, l'exercice de la liberté d'expression peut être soumis à certaines restrictions dans les conditions fixées par la loi et qui sont nécessaires pour protéger les droits ou la réputation d'autrui, la sécurité nationale, l'ordre public ou la santé ou la moralité publiques. Les restrictions doivent être expressément fixées par la loi, être nécessaires à des fins précises et être proportionnées à la nécessité sur laquelle elles se fondent.

L'objectif de la Convention et de ses mesures procédurales est de réduire la menace et les incidences de la cybercriminalité et les dommages causés par ce phénomène - ce qui peut constituer un fondement acceptable pour restreindre les droits humains et les libertés fondamentales lorsque les restrictions apportées sont conformes au droit, fondées, nécessaires et proportionnées.

Il sera impératif que les mesures procédurales énoncées dans la Convention soient établies, mises en œuvre et appliquées dans le respect des conditions et des garanties prévues par le Pacte et les autres instruments applicables en matière de droits humains.

Ces conditions et garanties doivent inclure, selon le cas, pour chaque mesure procédurale les éléments suivants :

- Surveillance ou supervision judiciaire ou autre surveillance ou supervision indépendante ;
- Motifs justifiant l'application de la mesure procédurale ;
- Restrictions quant à la portée et à la durée de la mesure procédurale ;

- Examen de l'incidence des mesures procédurales sur les droits, les responsabilités et les intérêts légitimes des tiers.

Brésil

[Original : anglais]
[8 avril 2022]

Chapitre III

Mesures procédurales, détection et répression

Article 18
Champ d'application des dispositions procédurales[2]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans le présent chapitre à des fins de prévention, de détection, de perturbation, d'enquêtes, de poursuites et de jugements d'actes de cybercriminalité.

2. Sauf disposition contraire, chaque Partie applique les pouvoirs et les procédures visés au paragraphe 1 du présent article :

a) Aux infractions pénales établies conformément au chapitre II de la présente Convention ;

b) À toutes les autres infractions pénales commises au moyen des technologies de l'information et des communications ;

c) À la collecte de preuves sous forme électronique relatives à la commission d'infractions pénales.

Article 19
Conditions et sauvegardes[3]

1. Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits humains et des libertés, notamment des droits découlant des obligations qu'elle a contractées au titre du Pacte international relatif aux droits civils et politiques et d'autres instruments du droit international des droits de l'homme s'appliquant, et qui doit intégrer les principes de la proportionnalité.

2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans la présente section sur les droits, responsabilités et intérêts légitimes des tiers.

Article 20
Préservation accélérée de données informatiques stockées[4]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une façon similaire la préservation accélérée de données électroniques, y compris des

[2] *Source* : Proposition de la Chine et de la Fédération de Russie, avec des modifications apportées par le Brésil.
[3] *Sources* : Convention de Budapest et proposition de la Chine et de la Fédération de Russie.
[4] *Source* : Convention de Budapest.

données de trafic, qui ont été stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie porte application du paragraphe 1 ci-dessus, au moyen d'une injonction adressée à une personne de préserver des données stockées se trouvant en sa possession ou sous son contrôle, elle adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à préserver et protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, dans la limite de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction sera renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 18 et 19.

Article 21
Conservation rapide d'informations électroniques accumulées[5]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la préservation rapide d'informations électroniques désignées expressément, y compris des données de trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles d'être supprimées, copiées ou modifiées, y compris en raison de l'expiration de la période de conservation fixée par sa législation nationale ou par les conditions de service du fournisseur.

2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne (y compris une personne morale) de préserver certaines informations stockées se trouvant en sa possession ou sous son contrôle, elle adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à préserver et à protéger l'intégrité desdites informations pendant une durée aussi longue que nécessaire, mais ne dépassant pas la durée prévue par la législation nationale de la Partie, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction sera renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le dépositaire des informations ou une autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures visés dans le présent article sont conformes aux dispositions des articles 18 et 19 de la présente Convention.

Article 22
Conservation et divulgation partielle rapides de données relatives au trafic[6]

Afin d'assurer la préservation des données de trafic, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires :

a) Pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ; et

[5] *Source* : Proposition de la Chine et de la Fédération de Russie.
[6] *Sources* : Convention de Budapest et proposition de la Chine et de la Fédération de Russie.

b) Pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 18 et 19.

Article 23
Injonction de produire[7]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a) À une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et

b) À un fournisseur de services assurant des prestations sur son territoire de communiquer des données en sa possession ou sous son contrôle sur des abonnés à de tels services.

2. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 18 et 19.

Article 24
Perquisition et saisie d'informations stockées ou traitées électroniquement[8]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à chercher à obtenir accès sur son territoire ou dans sa juridiction :

a) Aux dispositifs de technologies de l'information et des communications et aux informations qui y sont stockées ; et

b) Aux supports de stockage d'informations où les informations électroniques recherchées sont susceptibles d'être stockées.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que, lorsque ses autorités compétentes, dans le cadre d'une perquisition menée en application des dispositions du paragraphe 1 a), ont des raisons de penser que les informations recherchées sont stockées dans un autre appareil informatique situé sur son territoire, elles soient en mesure d'étendre rapidement la perquisition pour obtenir l'accès à cet autre appareil ou aux données qu'il contient.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire des informations électroniques sur son territoire ou dans sa juridiction. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un appareil ou système électronique utilisé pour stocker des informations ;

b) Réaliser et conserver une copie de ces données aux formats électronique et numérique ;

c) Préserver l'intégrité des informations stockées pertinentes ;

d) Supprimer les informations stockées ou traitées électroniquement.

---

[7] *Sources* : Convention de Budapest et proposition de la Chine et de la Fédération de Russie, avec les modifications apportées par le Brésil.

[8] *Source* : Proposition de la Chine et de la Fédération de Russie. Disposition similaire à l'article 19 de la Convention de Budapest, avec des modifications apportées par la Chine et la Fédération de Russie.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner, selon la procédure établie par son droit interne, à toute personne possédant une connaissance spécialisée du fonctionnement du système informatique en question, du réseau d'information et de télécommunications, ou de leurs éléments constitutifs, ou des mesures appliquées pour protéger les informations que contiennent ces dispositifs, de fournir toutes les informations ou l'assistance nécessaires pour permettre l'application des mesures visées aux paragraphes 1 à 3 du présent article.

5. Les pouvoirs et procédures visés dans le présent article sont conformes aux dispositions des articles 18 et 19 de la présente Convention.

Article 25
Collecte en temps réel des données relatives au trafic[9]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes :

a) À collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b) À obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ; ou

ii) À prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a), elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 18 et 19.

Article 26
Interception de données relatives au contenu[10]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ; et

b) À obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

[9] *Source* : Convention de Budapest.
[10] *Source* : Convention de Budapest.

i) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii) À prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a), elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 18 et 19.

Article 27
Compétence[11]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise :

a) Sur son territoire ; ou

b) À bord d'un navire battant pavillon de cette Partie ; ou

c) À bord d'un aéronef immatriculé selon les lois de cette Partie ; ou

par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.

2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1 b) à 1 d) du présent article ou dans une partie quelconque de ces paragraphes.

3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5. Si un État partie qui exerce sa compétence en vertu du paragraphe 1 ou 2 du présent article est avisé, ou apprend de toute autre façon, que d'autres États parties mènent une enquête ou ont engagé des poursuites ou une procédure judiciaire concernant le même acte, les autorités compétentes de ces États parties se consultent, selon qu'il convient, pour coordonner leurs actions[12].

[11] *Source* : Convention de Budapest, avec des modifications apportées par le Brésil.
[12] *Source* : Proposition de la Chine et de la Fédération de Russie.

Canada

[Original : anglais]
9 avril 2022

Pouvoirs procéduraux

Champ d'application des pouvoirs procéduraux

1. Chaque État partie précise que les pouvoirs et procédures prévus dans la présente section concernent des enquêtes ou procédures criminelles spécifiques.

2. Sauf disposition contraire, chaque État partie applique les pouvoirs et procédures mentionnés au paragraphe 1 :

a) Aux infractions pénales établies conformément à la présente Convention ;

b) À toutes les autres infractions pénales commises au moyen d'un système informatique ;

c) À la collecte des preuves électroniques de toute infraction pénale.

Conservation rapide de données informatiques stockées

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour permettre à ses autorités nationales compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Si un État partie fait application du paragraphe 1, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cet État partie adopte les mesures législatives et autres nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Un État partie peut prévoir le renouvellement d'une telle injonction.

3. Chaque État partie adopte les mesures législatives et autres nécessaires pour obliger, lorsque cela est justifié et autorisé, le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

Conservation et divulgation partielle rapides de données relatives au trafic

Afin d'assurer la conservation des données relatives au trafic, en application de l'article précédemment cité, chaque État partie :

a) Veille à la conservation rapide des données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ;

b) Assure la divulgation rapide à l'autorité compétente de l'État partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

Injonction de produire

Chaque État partie adopte les mesures nécessaires pour habiliter ses autorités nationales compétentes à ordonner à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique.

Perquisition et saisie de données informatiques stockées

1. Chaque État partie adopte les mesures nécessaires pour habiliter ses autorités nationales compétentes à opérer des perquisitions ou à accéder d'une autre manière :

a) À un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ;

b) À un support de stockage informatique permettant de stocker des données informatiques sur son territoire.

2. Chaque État partie adopte les mesures nécessaires pour permettre à ses autorités nationales compétentes d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système lorsqu'elles ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial.

3. Chaque État partie adopte les mesures nécessaires pour habiliter ses autorités nationales compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées pertinentes ;

d) Rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4. Chaque État partie adopte les mesures nécessaires pour habiliter ses autorités nationales compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques de fournir toutes les informations raisonnablement nécessaires pour permettre l'application des mesures visées par les paragraphes 1 et 2.

Compétence

1. Chaque État partie adopte les mesures nécessaires pour établir sa compétence à l'égard des infractions pénales établies conformément à la présente Convention :

a) Lorsque l'infraction est commise sur son territoire ;

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

c) Ou lorsque l'infraction est commise par l'un de ses ressortissants ou par une personne apatride résidant habituellement sur son territoire.

2. Chaque État partie doit pouvoir établir sa compétence à l'égard des infractions établies conformément à la présente Convention lorsque l'auteur présumé se trouve sur son territoire et qu'il n'extrade pas cette personne au seul motif qu'elle est l'un de ses ressortissants.

3. Chaque État partie doit également pouvoir établir sa compétence à l'égard des infractions établies conformément à la présente Convention lorsque l'auteur présumé se trouve sur son territoire et qu'il ne l'extrade pas.

4. Si un État partie qui exerce sa compétence en vertu du paragraphe 1 ou 2 a été avisé, ou a appris de toute autre façon, qu'un autre État partie mène une enquête ou a engagé des poursuites ou une procédure judiciaire concernant le même acte, les autorités compétentes de ces États parties se consultent, selon qu'il convient, pour coordonner leurs actions.

5. Sans préjudice des normes du droit international général, la présente Convention n'exclut pas l'exercice de toute compétence pénale établie par un État partie conformément à son droit interne.

Colombie

[Original : espagnol]
8 avril 2022

Mesures procédurales, détection et répression

Compte tenu des dispositions qui lient la Colombie en matière de pouvoirs et procédures au titre de la Convention des Nations Unies contre la criminalité transnationale organisée, la Convention des Nations Unies contre la corruption et la Convention de Budapest sur la cybercriminalité, il est proposé ce qui suit en ce qui concerne les mesures procédurales, la détection et la répression :

Mesures	*Disposition de l'instrument international existant*
Pouvoirs et procédures	Article 14 de la Convention de Budapest
Conditions et sauvegardes	Article 15 de la Convention de Budapest
Conservation rapide de données informatiques stockées	Article 16 de la Convention de Budapest
Conservation et divulgation partielle rapides de données relatives au trafic	Article 17 de la Convention de Budapest
Injonction de produire	Article 18 de la Convention de Budapest
Perquisition et saisie de données informatiques stockées	Article 19 de la Convention de Budapest
Collecte en temps réel des données relatives au trafic	Article 20 de la Convention de Budapest
Interception de données relatives au contenu	Article 21 de la Convention de Budapest
Compétence	Article 22 de la Convention de Budapest, article 15 de la Convention contre la criminalité organisée et article 42 de la Convention contre la corruption.
Gel, saisie et confiscation	Article 31 de la Convention contre la corruption

Égypte

[Original : arabe]
8 avril 2022

Chapitre III. Procédure pénale et application de la loi

Il est proposé que ce chapitre comprenne les trois articles principaux suivants :

Article 31. Champ d'application des questions de procédure

1. Chaque État partie adopte les mesures législatives qui se révèlent nécessaires pour instaurer les pouvoirs et procédures aux fins de la prévention, de l'identification, de la détection et de l'instruction des infractions et autres actes illégaux, ainsi que des procédures judiciaires engagées à leur sujet.

2. Chaque État partie applique les pouvoirs et procédures susmentionnés :

a) Aux infractions pénales et autres actes illégaux définis dans la présente Convention ;

b) À toutes les autres infractions pénales et aux autres actes illégaux commis au moyen des technologies de l'information et des communications ;

c) À la collecte de preuves électroniques.

Article 32
Procédures pénales

Les procédures pénales prévoient :

1. La conservation rapide des données stockées numériquement, y compris des données de suivi des utilisateurs, en particulier lorsqu'on estime que ces données sont susceptibles d'être perdues ou modifiées, ordre étant donné à la personne concernée de protéger l'intégrité des données en sa possession ou sous son contrôle pour permettre aux autorités compétentes de mener les perquisitions et les enquêtes voulues, en gardant secrète toute mesure prise à cet égard ;

2. La conservation et la divulgation partielle rapides des données de suivi des utilisateurs, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de ces données, et la garantie de la divulgation rapide par les autorités compétentes d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise ;

3. L'ordre de fournir des informations en la possession d'une personne se trouvant sur le territoire de l'État partie et stockées dans un système informatique ou sur un support de stockage, ou en la possession ou sous le contrôle d'un fournisseur de services qui opère sur le territoire de l'État partie ;

4. L'inspection des informations stockées ou l'accès aux informations stockées dans un système informatique ou sur un support de stockage ;

5. La saisie, la copie et la conservation des informations stockées dans le cadre de procédures de perquisition ou d'accès à l'information ;

6. La collecte en temps réel de données de suivi des utilisateurs et l'obligation pour les fournisseurs de services soumis à la juridiction de l'État partie de recueillir ces informations, de les enregistrer et de les garder confidentielles ;

7. L'interception de données relatives au contenu en permettant aux autorités compétentes de recueillir et d'enregistrer en temps réel, à l'aide de moyens techniques, les informations transmises par l'intermédiaire des technologies de l'information et des communications ;

8. Chaque État partie prend les mesures législatives et autres nécessaires pour permettre à ses autorités compétentes de mettre fin à la transmission ou la diffusion de tout contenu contraire aux dispositions de la présente Convention.

Article 33. Admissibilité des preuves numériques

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

El Salvador

[Original : espagnol]
12 avril 2022

Mesures procédurales, détection et répression

Champ d'application des mesures procédurales

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

Sauf disposition contraire, chaque État partie applique les pouvoirs et procédures mentionnés au paragraphe précédent du présent article :

a) Aux infractions établies conformément aux articles de la présente Convention ;

b) À toutes les autres infractions pénales commises au moyen d'un système informatique ;

c) À la collecte des preuves électroniques de toute infraction pénale.

Conditions et sauvegardes

Chaque État partie veille à ce que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumis aux conditions et sauvegardes prévues par son droit interne, qui doit assurer la protection adéquate des droits de l'homme et des libertés.

Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou indépendante, les motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

Dans la mesure où cela est conforme à l'intérêt général, en particulier à la bonne administration de la justice, chaque État partie examine l'effet des pouvoirs et procédures visés dans la présente section sur les droits, responsabilités et intérêts légitimes des tiers.

Pouvoirs d'exiger des informations sur les infractions

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne physique ou morale présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique, ou à l'obliger à le faire.

Conservation des données stockées dans les systèmes informatiques

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

Lorsqu'un État partie fait application du paragraphe précédent, au moyen d'une injonction ordonnant à une personne de conserver certaines données stockées se trouvant en sa possession ou sous son contrôle, cet État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité de ces données pendant une durée aussi longue que nécessaire, au maximum de 90 jours, afin de permettre aux autorités compétentes

d'obtenir leur divulgation. L'État partie peut prévoir le renouvellement d'une telle injonction.

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

Perquisition et saisie de données stockées dans les systèmes informatiques

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a) À un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ;

b) À un support de stockage informatique permettant de stocker des données informatiques sur son territoire.

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui ci, conformément au paragraphe 1 a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes précédents. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées pertinentes ;

d) Rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'adoption des mesures visées par les paragraphes précédents.

Collecte en temps réel des données relatives au trafic

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes :

a) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b) À obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

Lorsqu'un État partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a), il peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

Interception de données relatives au contenu

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b) À obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

Lorsqu'un État partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a), il peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

Confiscation et gel

Les États parties adoptent, dans toute la mesure possible dans le cadre de leurs systèmes juridiques nationaux, les mesures nécessaires pour permettre la confiscation :

a) Du produit du crime provenant d'infractions visées par la présente Convention ou de biens dont la valeur correspond à celle de ce produit ;

b) Des biens, des matériels et autres instruments utilisés ou destinés à être utilisés pour les infractions visées par la présente Convention.

Les États parties adoptent les mesures nécessaires pour permettre l'identification, la localisation, le gel ou la saisie de tout ce qui est mentionné au paragraphe précédent aux fins de confiscation ultérieure.

Si le produit du crime a été transformé ou converti, en totalité ou en partie, en d'autres biens, ces derniers peuvent faire l'objet des mesures visées au présent article en lieu et place dudit produit.

Si le produit du crime a été mêlé à des biens acquis légitimement, ces biens, sans préjudice de tous pouvoirs de gel ou de saisie, peuvent être confisqués à concurrence de la valeur estimée du produit qui y a été mêlé.

Les revenus ou autres avantages tirés du produit du crime, des biens en lesquels le produit a été transformé ou converti ou des biens auxquels il a été mêlé peuvent aussi faire l'objet des mesures visées au présent article, de la même manière et dans la même mesure que le produit du crime.

Chaque État partie habilite ses tribunaux ou autres autorités compétentes à ordonner la production ou la saisie de documents bancaires, financiers ou commerciaux. Les États parties ne peuvent invoquer le secret bancaire pour refuser de donner effet aux dispositions du présent paragraphe.

Les États parties peuvent envisager d'exiger que l'auteur d'une infraction établisse l'origine licite du produit présumé du crime ou d'autres biens pouvant faire l'objet d'une confiscation, dans la mesure où cette exigence est conforme aux principes de leur droit interne et à la nature de la procédure judiciaire et des autres procédures.

L'interprétation des dispositions du présent article ne doit en aucun cas porter atteinte aux droits des tiers de bonne foi.

Aucune disposition du présent article ne porte atteinte au principe selon lequel les mesures qui y sont visées sont définies et exécutées conformément au droit interne de chaque État partie et selon les dispositions dudit droit.

Disposition du produit du crime ou des biens confisqués

Un État partie qui confisque le produit du crime ou des biens en application de la présente Convention en dispose conformément à son droit interne et à ses procédures administratives.

Lorsque les États parties agissent à la demande d'un autre État partie en application de la présente Convention, ils doivent, dans la mesure où leur droit interne le leur permet et si la demande leur en est faite, envisager à titre prioritaire de restituer le produit du crime ou les biens confisqués à l'État partie requérant, afin que ce dernier puisse indemniser les victimes de l'infraction ou restituer ce produit du crime ou ces biens à leurs propriétaires légitimes.

Lorsqu'un État partie agit à la demande d'un autre État partie en application des dispositions de la présente Convention, il peut envisager spécialement de conclure des accords ou arrangements prévoyant :

a) De verser la valeur du produit ou des biens, ou les fonds provenant de leur vente, ou une partie de ceux-ci, au compte établi en application des dispositions de la présente Convention ou selon la méthode établie par les organismes intergouvernementaux spécialisés dans la lutte contre la criminalité organisée ;

b) De partager avec d'autres États parties, systématiquement ou au cas par cas, ce produit ou ces biens, ou les fonds provenant de leur vente, conformément à son droit interne ou à ses procédures administratives.

Établissement des antécédents judiciaires

Chaque État partie peut adopter les mesures législatives ou autres qui sont nécessaires pour tenir compte, dans les conditions et aux fins qu'il juge appropriées, de toute condamnation dont l'auteur présumé d'une infraction aurait antérieurement fait l'objet dans un autre État, afin d'utiliser cette information dans le cadre d'une procédure pénale relative à une infraction visée par la présente Convention.

Protection des témoins

Chaque État partie prend, dans la limite de ses moyens, des mesures appropriées pour assurer une protection efficace contre des actes éventuels de représailles ou d'intimidation aux témoins qui, dans le cadre de procédures pénales, font un témoignage concernant les infractions visées par la présente Convention et, le cas échéant, à leurs parents et à d'autres personnes qui leur sont proches.

Les mesures envisagées au précédent paragraphe du présent article peuvent consister notamment, sans préjudice des droits du défendeur, y compris du droit à une procédure régulière :

a) À établir, pour la protection physique de ces personnes, des procédures visant notamment, selon les besoins et dans la mesure du possible, à leur fournir un nouveau domicile et à permettre, s'il y a lieu, que les renseignements concernant leur identité et le lieu où elles se trouvent ne soient pas divulgués ou que leur divulgation soit limitée ;

b) À prévoir des règles de preuve qui permettent aux témoins de déposer d'une manière qui garantisse leur sécurité, notamment à les autoriser à déposer en recourant à des techniques de communication telles que les liaisons vidéo ou à d'autres moyens adéquats ;

c) Les États parties envisagent de conclure des arrangements avec d'autres États en vue de fournir un nouveau domicile aux personnes mentionnées au premier paragraphe du présent article ;

d) Les dispositions du présent article s'appliquent également aux victimes lorsqu'elles sont témoins.

Octroi d'une assistance et d'une protection aux victimes

Chaque État partie prend, dans la limite de ses moyens, des mesures appropriées pour prêter assistance et accorder protection aux victimes d'infractions visées par la présente Convention, en particulier dans les cas de menace de représailles ou d'intimidation.

Chaque État partie établit des procédures appropriées pour permettre aux victimes d'infractions visées par la présente Convention d'obtenir réparation.

Chaque État partie, sous réserve de son droit interne, fait en sorte que les avis et préoccupations des victimes soient présentés et pris en compte aux stades appropriés de la procédure pénale engagée contre les auteurs d'infractions, d'une manière qui ne porte pas préjudice aux droits de la défense.

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

Chaque État partie prend des mesures appropriées pour encourager les personnes qui participent ou ont participé à des groupes criminels organisés :

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 les activités des groupes et organisations criminels, ou le lieu où ils se trouvent ;

ii) Les liens, y compris à l'échelon international, avec d'autres groupes criminels organisés ;

iii) Les infractions que les groupes criminels organisés ont commises ou pourraient commettre ;

b) À fournir une aide factuelle et concrète aux autorités compétentes, qui pourrait contribuer à priver les groupes criminels organisés de leurs ressources ou du produit du crime.

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 visée par la présente Convention.

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 visée par la présente Convention.

La protection de ces personnes est assurée comme le prévoit l'article correspondant de la présente Convention.

Lorsqu'une personne visée au premier paragraphe 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.

Union européenne et ses États membres

[Original : anglais]
[6 avril 2022]

Chapitre III
Procédures pénales et détection et répression

Article 13
Champ d'application des mesures du droit de procédure

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans le présent chapitre aux fins d'enquêtes ou de procédures pénales particulières.

2. Chaque État partie applique les pouvoirs et procédures visés au paragraphe 1 du présent article :

a) Aux infractions pénales établies conformément aux articles 5 à 10 de la présente Convention ; et

b) À la collecte des preuves sous forme électronique d'une infraction pénale établie conformément aux articles 5 à 10 de la présente Convention.

Article 14
Conditions et sauvegardes

1. Chaque État partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le présent chapitre soient soumises aux conditions et sauvegardes prévues par son droit interne, lequel doit assurer, conformément aux normes internationales relatives aux droits humains, une protection adéquate et totale des droits humains et des libertés fondamentales, notamment des droits découlant des obligations qu'il a contractées au titre de la Déclaration universelle des droits de l'homme, du Pacte international relatif aux droits civils et politiques, de la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants, de la Convention relative aux droits de l'enfant, du Protocole facultatif à la Convention relative aux droits de l'enfant concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, et d'autres instruments internationaux relatifs aux droits humains, intégrer les principes de la proportionnalité, de la légalité et de la nécessité et garantir la protection de la vie privée et des données à caractère personnel.

2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque État partie examine l'effet des pouvoirs et

procédures énoncés dans le présent chapitre sur les droits, responsabilités et intérêts légitimes des tiers.

Article 15
Préservation accélérée de données informatiques stockées

1. Chaque État partie adopte les mesures nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une façon similaire la préservation accélérée de données électroniques, dont les données de trafic, qui ont été stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'un État partie porte application du paragraphe 1 ci-dessus au moyen d'une injonction adressée à une personne de préserver des données stockées se trouvant en sa possession ou sous son contrôle, il adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à préserver et protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, dans la limite de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prendre les dispositions nécessaires pour qu'une telle injonction soit renouvelée par la suite.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données informatiques ou une autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 14 et 15.

Article 16
Injonction de produire

1. Chaque État partie adopte les mesures nécessaires pour habiliter ses autorités compétentes à ordonner :

a) À une personne présente sur son territoire de communiquer des données informatiques en sa possession ou sous son contrôle qui sont stockées dans un système informatique ou un support de stockage ; et

b) À un fournisseur de services assurant des prestations sur son territoire de communiquer des renseignements en sa possession ou sous son contrôle sur des abonnés à de tels services.

2. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 14 et 15.

Article 17
Perquisition et saisie de données informatiques stockées

1. Chaque État partie adopte les mesures nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a) À un système informatique ou à une partie de celui-ci ainsi qu'aux données qui y sont stockées ; et

b) À un support permettant de stocker des données informatiques sur son territoire.

2. Chaque État partie adopte les mesures nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent un système informatique ou une partie de celui-ci ou y accèdent d'une façon similaire, conformément à l'alinéa a) du paragraphe 1, et qu'elles ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique situé sur son territoire, ou une partie de celui-ci, et que ces données sont légalement accessibles à partir du premier système ou disponibles

pour celui-ci, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou le moyen similaire d'accéder à l'autre système.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques auxquelles elles ont accédé en application du paragraphe 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage de données informatiques ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées concernées ;

d) Rendre ces données informatiques inaccessibles ou les retirer du système informatique consulté.

4. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées aux paragraphes 1 et 2.

5. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 14 et 15.

Article 18
Compétence

1. Chaque État partie adopte les mesures nécessaires pour établir sa compétence à l'égard d'une infraction établie conformément aux articles 5 à 10 de la présente Convention dans les cas suivants :

a) Lorsque l'infraction est commise sur son territoire ;

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

c) Lorsque l'infraction est commise par un de ses ressortissants, si elle est punissable pénalement là où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État.

2. Chaque État partie peut également établir sa compétence à l'égard d'une telle infraction dans les cas suivants :

a) Lorsque l'infraction est commise à l'encontre d'un de ses ressortissants ;

b) Lorsque l'infraction est commise par l'un de ses ressortissants ou par une personne apatride résidant habituellement sur son territoire.

3. Chaque État partie peut également adopter les mesures nécessaires pour établir sa compétence à l'égard des infractions visées par la présente Convention lorsque l'auteur présumé se trouve sur son territoire et qu'il ne l'extrade pas, au seul titre de sa nationalité, après une demande d'extradition.

4. Si un État partie qui exerce sa compétence en vertu du paragraphe 1 ou 2 du présent article a été avisé, ou a appris de toute autre façon, qu'un ou plusieurs autres États parties menaient une enquête ou avaient engagé des poursuites ou une procédure judiciaire concernant le même acte, les autorités compétentes de ces États parties se concertent, selon qu'il convient, pour coordonner leur action.

5. Sans préjudice des normes du droit international général, la présente Convention n'exclut pas l'exercice de toute compétence pénale établie par un État partie conformément à son droit interne.

Article 19
Octroi d'une assistance et d'une protection aux victimes

1. Chaque État partie prend, dans la limite de ses moyens, des mesures appropriées pour prêter assistance et accorder protection aux victimes d'infractions établies conformément aux articles 5 à 10 de la présente Convention.

2. Chaque État partie établit des procédures appropriées pour permettre aux victimes d'infractions établies conformément aux articles 5 à 10 de la présente Convention d'obtenir réparation.

3. Chaque État partie fait en sorte, sous réserve de son droit interne, que les avis et préoccupations des victimes soient présentés et pris en compte aux stades appropriés de la procédure pénale engagée contre les auteurs d'infractions, d'une manière qui ne porte pas préjudice aux droits de la défense.

Ghana

[Original : anglais]
[12 avril 2022]

Chapitre III
Mesures procédurales et détection et répression[13]

Article 23
Champ d'application des mesures du droit de procédure

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales particulières.

2. Sauf disposition contraire, chaque Partie applique les pouvoirs et procédures visés au paragraphe 1 du présent article :

a) Aux infractions pénales établies conformément aux articles 5 à 20 de la présente Convention ;

b) À toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c) À la collecte de preuves sous forme électronique d'une infraction pénale.

3. Chaque Partie peut se réserver le droit de n'appliquer les mesures visées à l'article 29 qu'aux infractions ou catégories d'infractions mentionnées dans la réserve, pourvu que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus restreint que celui des infractions auxquelles elle applique les mesures visées à l'article 30. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible des mesures visées à l'article 29.

4. Lorsqu'une Partie n'est pas en mesure, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, d'appliquer les mesures visées aux articles 29 et 30 aux communications transmises dans le système informatique d'un fournisseur de services :

a) Qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé ; et

b) Qui n'emploie pas les réseaux publics de communications et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé, cette Partie peut

[13] Le texte de la présente section est tiré principalement de la Convention de Budapest, de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, de la loi de 2008 sur les transactions électroniques (loi 772) et de la loi de 2020 sur la cybersécurité (loi 1038). Ces instruments constituent le cadre législatif de la cybercriminalité au Ghana.

se réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible des mesures visées aux articles 29 et 30.

5. Lorsqu'une Partie n'est pas en mesure, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, d'appliquer les mesures visées à l'article 31, elle peut se réserver le droit de ne pas le faire. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible desdites mesures.

Article 24
Conditions et sauvegardes

1. Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, lequel doit assurer une protection adéquate des droits humains et des libertés, notamment des droits découlant des obligations qu'elle a contractées au titre de la Charte internationale des droits de l'homme[14], qui comprend la Déclaration universelle des droits de l'homme et le Pacte international relatif aux droits civils et politiques, et d'autres instruments internationaux applicables relatifs aux droits humains, intégrer les principes de la proportionnalité et de la nécessité et garantir le contrôle judiciaire.

2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans la présente section sur les droits, responsabilités et intérêts légitimes des tiers.

Article 25
Préservation accélérée de données informatiques stockées[15]

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une façon similaire la préservation accélérée de données électroniques, dont les données de trafic, qui ont été stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie porte application du paragraphe 1 ci-dessus, au moyen d'une injonction adressée à une personne de préserver des données stockées se trouvant en sa possession ou sous son contrôle, elle adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à préserver et protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, dans la limite de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prendre les dispositions nécessaires pour qu'une telle injonction soit renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de

[14] Haut-Commissariat des Nations Unies aux droits de l'homme, « Le droit international relatif aux droits de l'homme » (https://www.ohchr.org/fr/instruments-and-mechanisms/international-human-rights-law).

[15] Conformément à la Convention de Budapest, à la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, et aux lois de 2008 sur les transactions électroniques (loi 772) et de 2020 sur la cybersécurité (loi 1038) du Ghana.

préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 19 et 20.

Article 26
Préservation et divulgation partielle accélérées de données de trafic[16]

1. Afin d'assurer la préservation des données de trafic prévue par l'article 21, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires :

a) Pour veiller à la préservation accélérée de ces données de trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ; et

b) Pour veiller à la divulgation accélérée à son autorité compétente, ou à une personne désignée par cette autorité, d'une quantité suffisante de données de trafic afin de permettre à la Partie d'identifier les fournisseurs de services et la voie par laquelle la communication a été transmise.

2. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 23 et 24.

Article 27
Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a) À une personne présente sur son territoire de communiquer des données informatiques en sa possession ou sous son contrôle qui sont stockées dans un système informatique ou un support de stockage ; et

b) À un fournisseur de services assurant des prestations sur son territoire de communiquer des renseignements en sa possession ou sous son contrôle sur des abonnés à de tels services.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que l'injonction de produire les données informatiques ou les renseignements sur l'abonné ne soient obtenus que par une autorité compétente placée sous la supervision d'une entité indépendante, telle qu'une autorité judiciaire. Ces mesures garantissent que l'autorité compétente est tenue de convaincre l'autorité de supervision indépendante qu'il y a des motifs raisonnables de croire que les données informatiques ou les renseignements sur l'abonné se rapportant à une personne faisant l'objet d'une enquête sont nécessaires aux fins de cette enquête pénale particulière.

3. Aux fins du paragraphe 2, l'autorité compétente :

a) Explique à l'autorité de supervision indépendante pourquoi elle pense que les données informatiques ou les renseignements sur l'abonné recherchés seront disponibles auprès :

i) De la personne sous le contrôle ou en la possession de laquelle se trouvent les données informatiques ou le système informatique ; ou

ii) D'un fournisseur de services ;

b) Définit et explique précisément le type de données informatiques ou de renseignements sur l'abonné recherchés ;

[16] Conformément à la Convention de Budapest.

c) Indique les mesures à prendre pour obtenir les renseignements sur l'abonné ou les données informatiques ;

i) Tout en préservant la vie privée des autres utilisateurs, des clients et des tiers ; et

ii) Sans divulguer les renseignements sur l'abonné ou les données informatiques d'une partie non concernée par l'enquête.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que l'autorité de supervision indépendante puisse autoriser une injonction de produire au titre du paragraphe 2 si elle est convaincue que :

a) Les renseignements demandés sont adaptés, proportionnés et nécessaires aux fins d'une enquête ou de poursuites pénales particulières ;

b) Des mesures seront prises pour faire exécuter l'injonction tout en préservant la vie privée des autres utilisateurs, des clients et des tiers et sans divulguer de renseignements et de données d'une partie non concernée par l'enquête ; et

c) L'enquête risque d'être entravée ou sérieusement compromise si la production des renseignements n'est pas autorisée.

5. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 23 et 24.

6. Aux fins du présent article, le terme « renseignements sur l'abonné » s'entend de toute information détenue par un fournisseur de services sous forme de données informatiques ou sous toute autre forme, se rapportant aux abonnés de ses services, autres que des données de trafic ou de contenu, et permettant d'établir :

a) Le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b) L'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c) Toute autre information relative à l'endroit où se trouve le matériel de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Article 28
Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a) À un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b) À un support permettant de stocker des données informatiques sur son territoire.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent un système informatique ou une partie de celui-ci ou y accèdent d'une façon similaire, conformément à l'alinéa a) du paragraphe 1, et qu'elles ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique situé sur son territoire, ou une partie de celui-ci, et que ces données sont légalement accessibles à partir du premier système ou disponibles pour celui-ci, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou le moyen similaire d'accéder à l'autre système.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques auxquelles elles ont accédé en application du paragraphe 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage de données informatiques ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées concernées ;

d) Rendre ces données informatiques inaccessibles ou les retirer du système informatique consulté.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées aux paragraphes 1 et 2.

5. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à être accompagnées d'une personne autorisée et est en droit de permettre, avec l'assistance de cette personne, l'application des mesures visées par les paragraphes 1, 2 et 3.

6. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir tout ordinateur, document électronique, programme, renseignement, document ou objet dans le cadre de l'exécution d'un mandat de perquisition au titre de son droit interne, si l'autorité compétente a des motifs raisonnables de croire que l'une des infractions établies conformément aux articles 1 à 16 de la présente Convention a été commise ou est sur le point de l'être.

7. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 23 et 24.

Article 29
Collecte en temps réel de données de trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; et

b) Obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; ou

ii) Prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, des données de trafic associées à des communications transmises sur son territoire au moyen d'un système informatique.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que le pouvoir que confère le présent article ne soit obtenu que par une autorité compétente placée sous la supervision d'une entité indépendante, telle qu'une autorité judiciaire. Ces mesures garantissent que l'autorité compétente est tenue de convaincre l'autorité de supervision indépendante qu'il y a des motifs raisonnables de croire que les données de trafic se rapportant à une personne faisant l'objet d'une enquête sont nécessaires aux fins de cette enquête pénale particulière.

3. Aux fins du paragraphe 2, l'autorité compétente :

a) Explique à l'autorité de supervision indépendante pourquoi elle pense que les données informatiques ou les renseignements sur l'abonné recherchés seront disponibles auprès :

i) De la personne sous le contrôle ou en la possession de laquelle se trouve le système informatique ; ou

ii) D'un fournisseur de services ;

b) Définit et explique précisément le type de données de trafic recherchées ;

c) Définit et explique précisément les infractions au titre desquelles le pouvoir conféré par le présent article est demandé ;

d) Indique les mesures à prendre pour obtenir les données de trafic :

i) Tout en préservant la vie privée des autres utilisateurs, des clients et des tiers ; et

ii) Sans divulguer les données de trafic d'une partie non concernée par l'enquête.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que l'autorité de supervision indépendante puisse accorder le pouvoir de collecte en temps réel de données de trafic si elle est convaincue que :

a) L'étendue de l'interception est adaptée, proportionnée et nécessaire aux fins d'une enquête ou de poursuites pénales particulières ;

b) Des mesures seront prises pour faire exécuter le pouvoir tout en préservant la vie privée des autres utilisateurs, des clients et des tiers et sans divulguer de renseignements et de données d'une Partie non concernée par l'enquête ; et

c) L'enquête risque d'être entravée ou sérieusement compromise si le pouvoir de collecter en temps réel des données de trafic n'est pas autorisé.

5. Lorsqu'un État partie ne peut adopter, en raison des principes établis dans son ordre juridique interne, les mesures énoncées à l'alinéa a) du paragraphe 1, il peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données de contenu associées à des communications transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

6. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

7. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 23 et 24.

Article 30
Interception de données de contenu

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes, face à un éventail d'infractions graves à définir en droit interne, à :

a) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; et

b) Obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; ou

ii) Prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, des données de trafic associées à des communications transmises sur son territoire au moyen d'un système informatique.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que le pouvoir que confère le présent article ne soit obtenu que par une autorité compétente placée sous la supervision d'une entité indépendante, telle qu'une autorité judiciaire. Ces mesures garantissent que l'autorité compétente est tenue de convaincre l'autorité de supervision indépendante qu'il y a des motifs raisonnables pour autoriser l'interception de données de contenu liées à la personne ou aux locaux faisant l'objet d'une enquête, à l'une des fins suivantes :

a) Dans l'intérêt de la sécurité nationale ;

b) Pour prévenir ou détecter une infraction grave ;

c) Dans l'intérêt économique des citoyens, dans la mesure où il coïncide avec l'intérêt de la sécurité nationale ; ou

d) Pour donner effet à une demande d'entraide judiciaire.

3. Aux fins du paragraphe 2, l'autorité compétente :

a) Explique à l'autorité de supervision indépendante pourquoi elle pense que les données de contenu recherchées seront disponibles auprès :

i) De la personne sous le contrôle ou en la possession de laquelle se trouve le système informatique ;

ii) D'un fournisseur de services ;

b) Détermine et explique le type de données de contenu dont elle soupçonne qu'elles se trouvent dans le système informatique ou en la possession ou sous le contrôle du fournisseur de services ;

c) Définit et explique précisément les infractions au titre desquelles le pouvoir conféré par le présent article est demandé ;

d) Indique les mesures à prendre pour obtenir les données de contenu :

i) Tout en préservant la vie privée des autres utilisateurs, des clients et des tiers ; et

ii) Sans divulguer les données de trafic d'une partie non concernée par l'enquête.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que l'autorité de supervision indépendante puisse accorder le pouvoir d'interception de données de contenu si elle est convaincue que :

a) L'étendue de l'interception est adaptée, proportionnée et nécessaire aux fins d'une enquête ou de poursuites pénales particulières ;

b) Des mesures seront prises pour faire exécuter le pouvoir d'interception des données de contenu tout en préservant la vie privée des autres utilisateurs, des clients et des tiers et sans divulguer de renseignements et de données d'une partie non concernée par l'enquête ; et

c) L'enquête risque d'être entravée ou sérieusement compromise si l'interception n'est pas autorisée.

5. Lorsqu'une Partie ne peut adopter, en raison des principes établis dans son ordre juridique interne, les mesures énoncées à l'alinéa a) du paragraphe 1, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données de contenu relatives à des

communications transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

6. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

7. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 23 et 24.

Article 31
Conservation de données

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce qu'un fournisseur de services établi sur son territoire conserve :

a) Les renseignements sur l'abonné pendant au moins six ans ;

b) Les données de trafic pendant une période de 12 mois.

2. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 23 et 24.

3. Lorsqu'une Partie n'est pas en mesure, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, d'appliquer les mesures visées dans le présent article, elle peut se réserver le droit de ne pas le faire. Chaque Partie envisage de limiter une telle réserve de manière à permettre l'application la plus large possible desdites mesures.

Article 32
Confiscation et saisie

1. Chaque Partie adopte, dans toute la mesure possible dans le cadre de son système juridique interne, les mesures nécessaires pour permettre la confiscation :

a) Du produit du crime provenant d'infractions visées par la présente Convention ou de biens dont la valeur correspond à celle de ce produit ;

b) Des biens, des matériels et autres instruments utilisés ou destinés à être utilisés pour les infractions visées par la présente Convention.

2. Chaque Partie adopte les mesures nécessaires pour permettre l'identification, la localisation, le gel ou la saisie de tout ce qui est mentionné au paragraphe 3 du présent article aux fins de confiscation ultérieure.

3. Si le produit du crime a été transformé ou converti, en partie ou en totalité, en d'autres biens, ces derniers peuvent faire l'objet des mesures visées dans le présent article en lieu et place dudit produit.

4. Si le produit du crime a été mêlé à des biens acquis légitimement, ces biens, sans préjudice de tout pouvoir de gel ou de saisie, sont confiscables à concurrence de la valeur estimée du produit qui y a été mêlé.

5. Les revenus ou autres avantages tirés du produit du crime, des biens en lesquels le produit a été transformé ou converti ou des biens auxquels il a été mêlé peuvent aussi faire l'objet des mesures visées dans le présent article, de la même manière et dans la même mesure que le produit du crime.

6. Aux fins du présent article, chaque Partie habilite ses tribunaux ou autres autorités compétentes à ordonner la production ou la saisie de documents bancaires, financiers ou commerciaux. Les Parties ne peuvent invoquer le secret bancaire pour refuser de donner effet aux dispositions du présent paragraphe.

7. Chaque Partie peut envisager d'exiger que l'auteur d'une infraction établisse l'origine licite du produit présumé du crime ou d'autres biens confiscables, dans la

mesure où cette exigence est conforme aux principes de son droit interne et à la nature des procédures judiciaires et autres.

8. L'interprétation des dispositions du présent article ne doit en aucun cas porter atteinte aux droits des tiers de bonne foi.

9. Aucune disposition du présent article ne porte atteinte au principe selon lequel les mesures qui y sont visées sont définies et exécutées conformément aux dispositions du droit interne de chaque Partie et sous réserve de celles-ci.

Article 33
Compétence

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 5 à 20 de la présente Convention, lorsque l'infraction est commise :

a) Sur son territoire ;

b) À bord d'un navire qui bat son pavillon ;

c) À bord d'un aéronef immatriculé conformément à son droit interne ; ou

d) Par un de ses ressortissants, si elle est punissable pénalement là où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État.

2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux alinéas b) à d) du paragraphe 1 du présent article ou dans une partie quelconque de ces paragraphes.

3. Aux fins de l'article de la présente Convention relatif à l'extradition, chaque Partie adopte les mesures nécessaires pour établir sa compétence à l'égard des infractions établies conformément à ladite Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5. Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée établie conformément à la présente Convention, les Parties concernées se concertent, s'il y a lieu, afin de déterminer la mieux à même d'exercer les poursuites.

Iran (République islamique d')

[Original : anglais]
[8 avril 2022]

3. Mesures procédurales, détection et répression

Les criminels ont perpétuellement, et de plus en plus, recours à des services assurés par le secteur privé, notamment par les fournisseurs de services et les plateformes de mise en réseau des médias sociaux. Cela pose un problème de taille, qui exige des réponses concrètes. Compte tenu de l'importance fondamentale et cruciale que revêt la coopération des entités concernées avec les services de détection et de répression, dans le cadre des enquêtes et des poursuites engagées contre ce type d'infractions et dans les efforts visant à empêcher de telles utilisations abusives, il faudrait que la convention énonce précisément les obligations et réglementations applicables en ce qui concerne la coopération du secteur privé, des fournisseurs de services et d'autres entités similaires avec les services de détection et de répression,

en particulier pour les secteurs et les prestataires ayant une portée mondiale ou disposant d'une couverture importante à l'échelle internationale.

La mise en place de mesures permettant de s'assurer la coopération rapide et efficace de ces entités avec les services de détection et de répression et avec les autorités judiciaires devrait faire partie intégrante de la convention. À cette fin, la convention devrait inclure des sections spécifiquement consacrées à la question de la coopération entre les autorités nationales et des acteurs tels que les fournisseurs de services et le secteur privé, ainsi qu'à la définition de mesures concrètes devant notamment permettre d'assurer rapidement la préservation des données électroniques et leur divulgation aux services de détection et de répression.

Étant donné que les preuves électroniques constituent un élément indispensable pour les enquêtes et les poursuites ciblant des infractions commises au moyen des technologies de l'information et de la communication, il faudrait que la mise en place de procédures standard axées sur l'obtention, la gestion et la divulgation de preuves électroniques authentiques figure parmi les mesures énoncées dans la convention. La mise en place de procédures standard permet d'apporter aux infractions visées une réponse homogène et cohérente au niveau national, ce qui pourrait aussi garantir à l'échelle internationale une coopération plus efficace entre les services de détection et de répression et les autorités judiciaires pour ce qui est de préserver et de communiquer des preuves électroniques.

Le recouvrement et la restitution des avoirs et du produit du crime jouent un rôle important pour priver les criminels des avantages incitant à commettre des infractions et pour réduire la récidive, ainsi que pour indemniser les victimes. Par conséquent, les questions relatives à la saisie, au recouvrement et à la restitution rapides du produit du crime devraient constituer un élément essentiel de la convention. Dans cette dernière, les dispositions relatives à la détection et à la répression ainsi qu'aux mesures procédurales devraient confier aux autorités nationales des pouvoirs permettant de garantir le recouvrement rapide et sans heurts des avoirs et produits de la criminalité, en prévoyant dans ce domaine des mesures d'assistance et de coopération aussi larges que possible.

La lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles exige que les services de détection et de répression disposent de technologies modernes et qu'ils s'en servent dans le cadre des enquêtes et des poursuites pertinentes, afin d'apporter une réponse proportionnée à ce type d'infractions. Il faudrait donc promouvoir et appuyer l'utilisation de technologies modernes par les services de détection et de répression et les autorités judiciaires, notamment tout au long de l'application des mesures procédurales axées sur la prévention et la répression des infractions commises au moyen des technologies de l'information et des communications. Pour cela, il convient également de fournir aux services et autorités mentionnés le matériel et les moyens technologiques nécessaires, en leur prêtant une assistance technique fiable et politiquement neutre.

Japon

[Original : anglais]
[8 avril 2022]

3. Mesures procédurales, détection et répression

3.1 En ce qui concerne les mesures procédurales applicables aux enquêtes sur la cybercriminalité, il faudrait peut-être s'intéresser à la préservation, à la recherche et à la saisie rapides des données informatiques stockées, aux injonctions de produire et à la collecte en temps réel des données de trafic.

3.2 Nous pourrions envisager que ces dispositions procédurales s'appliquent aux enquêtes et procédures pénales visant les infractions pénales établies dans cette convention et d'autres infractions pénales commises au moyen d'un système

informatique, ainsi qu'à la collecte des preuves électroniques de toute infraction pénale.

3.3 En accordant les pouvoirs susmentionnés aux autorités compétentes des États Membres, il est nécessaire d'établir des dispositions confirmant que chaque État Membre doit veiller à ce que soient convenablement défendus les droits découlant des obligations prévues dans les traités relatifs aux droits humains et dans d'autres instruments, ainsi que d'autres droits de la personne et libertés, et à ce que soit appliquée une législation nationale incluant le principe de proportionnalité. La convention devrait rappeler cette idée générale dans le chapitre consacré aux mesures procédurales et aux activités de détection et de répression.

Mexique

[Original : anglais]
[13 avril 2022]

Mesures procédurales, détection et répression

Compte tenu de l'importance que revêtent les preuves numériques pour les enquêtes, les poursuites et les activités de détection et de répression, il est attendu que les États parties à la convention s'accordent sur des mesures procédurales de portée générale et bénéficiant d'une approbation minimale en ce qui concerne l'obtention, le traitement et la préservation de ce type de preuves. On pourrait envisager d'inclure la précision suivante : « Les États peuvent envisager et appliquer toutes les dispositions prévues dans les instruments internationaux existants, comme la Convention des Nations Unies contre la criminalité transnationale organisée, à des fins d'enquête ou/et pour la collecte de preuves et la préservation des preuves électroniques ».

En ce qui concerne les entités privées qui fournissent des services informatiques et des services de communication, le Mexique recommande d'inclure les articles suivants :

> « Les États parties s'engagent à faire en sorte que les entités privées qui fournissent des services informatiques et des services de communication, lorsqu'elles sont établies sur leur territoire ou que leurs activités sont soumises à la juridiction nationale, adoptent et mettent en œuvre des politiques et des procédures de diligence raisonnable pour éviter que tout dommage soit causé à des tiers. »
>
> « Les États parties s'engagent aussi à prendre des mesures appropriées pour que les entités privées qui sont établies sur leur territoire ou dont les activités sont soumises à la juridiction nationale n'enfreignent pas les lois d'autres États parties. »

Il serait également pertinent d'inclure un appel général à la responsabilité des entités privées qui fournissent des services informatiques et des services de communication, en les engageant à collaborer efficacement avec les services de détection et de répression et les autorités judiciaires du pays en ce qui concerne les enquêtes et les poursuites relatives à la cybercriminalité, dans le respect des réglementations applicables en matière de protection de la vie privée.

Nouvelle-Zélande

[Original : anglais]
[8 avril 2022]

Dispositions relatives aux mesures procédurales, à la détection et à la répression

10. Sous réserve de l'inclusion de garanties complètes en faveur de la protection des droits humains et des libertés fondamentales, du respect de l'État de droit et de

l'adhésion au principe de proportionnalité, la Nouvelle-Zélande est favorable à l'idée d'inclure dans cette convention des dispositions qui permettraient d'assurer rapidement la préservation et la mise à disposition des preuves numériques. Ces dispositions pourraient porter, par exemple, sur les aspects suivants :

- La perquisition et la saisie de données ciblées et pertinentes stockées dans des systèmes informatiques ;
- La collecte en temps réel de données informatiques ciblées et pertinentes ;
- L'interception de données informatiques ciblées et pertinentes ;
- La préservation de données informatiques ciblées et pertinentes ;
- Les injonctions de produire des données informatiques spécifiées qui se trouvent en la possession ou sous le contrôle d'une personne, et qui sont stockées dans un système informatique ou un support de stockage.

11. La Nouvelle-Zélande serait également favorable à l'idée d'inclure des dispositions qui permettent de s'assurer que les criminels ne tirent pas profit de leurs activités illicites, en prévoyant notamment la saisie et la confiscation du produit du crime, ainsi que des dispositions susceptibles de renforcer la coopération avec les services de détection et de répression.

Norvège

[Original : anglais]
[8 avril 2022]

Mesures procédurales, détection et répression

9. Le Comité spécial devrait s'inspirer de l'expérience de traités existants, comme la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention des Nations Unies contre la corruption. Dans le même temps, compte tenu du fait que la nouvelle convention s'attaquera aux défis de la cybercriminalité moderne, il devrait exiger des États Membres qu'ils prévoient des dispositions nationales concernant spécifiquement les preuves électroniques. En outre, le Comité spécial devrait garder à l'esprit que le temps et l'efficacité sont des aspects déterminants dans le cadre des enquêtes et des poursuites relatives à la cybercriminalité. La convention devrait autoriser la coopération aux fins de la collecte et de l'obtention de preuves électroniques pour tout type d'infractions, et non pas uniquement pour les actes de cybercriminalité.

10. Afin d'éviter toute répétition inutile des efforts, le Comité spécial devrait tirer parti des voies de communication et des réseaux qui existent déjà et qui fonctionnent bien, tout en les renforçant.

11. Le rôle clef du secteur privé doit être pris en compte.

12. Il faudrait s'intéresser à l'assistance et à la protection qu'il convient d'accorder aux victimes, ainsi qu'à la protection des témoins.

13. Les dispositions relatives aux mesures procédurales doivent être compatibles avec les garanties d'une procédure régulière ainsi qu'avec la protection des droits humains et des libertés fondamentales.

Fédération de Russie, également au nom du Bélarus, du Burundi, de la Chine, du Nicaragua et du Tadjikistan

[Original : russe]
[7 avril 2022]

Section 2

Procédure pénale et application de la loi

Article 31
Champ d'application des mesures du droit de procédure

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins de la prévention, de la détection, de la répression, de la mise au jour et de la poursuite des infractions et autres actes illégaux, ainsi que des procédures judiciaires engagées à leur sujet.

2. Sauf disposition contraire figurant à l'article 33 de la présente Convention, chaque État partie applique les pouvoirs et procédures visés au paragraphe 1 du présent article :

a) Aux infractions pénales et autres actes illégaux incriminés en application des articles 6 à 29 de la présente Convention ;

b) À toutes les autres infractions pénales et aux autres actes illégaux commis au moyen des technologies de l'information et des communications ;

c) À la collecte de preuves, y compris les preuves électroniques, de la commission d'infractions pénales ou autres actes illégaux.

3. a) Chaque État partie peut se réserver le droit de n'appliquer les mesures visées à l'article 38 de la présente Convention qu'aux infractions ou catégories d'infraction définies dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infraction ne soit pas plus réduit que celui des infractions auxquelles il applique les mesures visées à l'article 33. Chaque État partie envisage de limiter une telle réserve de manière à permettre l'application la plus large possible des mesures visées à l'article 38 ;

b) Si, du fait des limitations de la législation nationale en vigueur au moment de l'adoption de la présente Convention, un État partie ne peut appliquer les mesures visées aux articles 33 et 38 de la présente Convention aux informations transmises dans le système informatique d'un fournisseur de services, et que ce système

i) Est exploité au profit d'un groupe fermé d'utilisateurs ; et

ii) Ne recourt à aucun réseau d'information et de télécommunications et n'est pas relié à d'autres systèmes informatiques,

l'État partie concerné peut se réserver le droit de ne pas appliquer lesdites mesures à ces informations.

Article 32
Conditions et sauvegardes

1. Chaque État partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits humains et des libertés, en particulier des droits établis conformément aux obligations que l'État partie a souscrites en application du Pacte international relatif aux droits civils et politiques du 16 décembre 1966 ou d'autres instruments internationaux applicables en matière de droits humains.

2. Eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt général, en particulier à la bonne administration de la justice, chaque État partie examine l'effet des pouvoirs et procédures visés dans la présente section sur les droits, responsabilités et intérêts légitimes des tiers.

Article 33
Collecte d'informations transmises au moyen des technologies de l'information et des communications

1. Afin de lutter contre les infractions visées par la présente Convention et incriminées dans son droit interne, chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a) Collecter ou enregistrer à l'aide des moyens techniques appropriés, sur son territoire, des informations transmises au moyen des technologies de l'information et des communications ; et

b) Obliger un fournisseur de services, dans les limites de ses capacités techniques :

i) À collecter ou à enregistrer à l'aide des moyens techniques appropriés, sur son territoire, des données électroniques, y compris les données de contenu, transmises au moyen des technologies de l'information et des communications ; ou

ii) À prêter aux autorités compétentes de l'État partie concerné son concours et son assistance pour collecter ou enregistrer en temps réel, sur son territoire, des données électroniques, y compris les données de contenu, transmises au moyen des technologies de l'information et des communications.

2. Lorsqu'un État partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a) du présent article, il peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel de données électroniques, y compris les données de contenu, transmises au moyen de technologies de l'information et des communications sur son territoire, à l'aide des moyens techniques existant sur ce territoire.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 31 et 32 de la présente Convention.

Article 34
Préservation rapide d'informations électroniques accumulées

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la préservation rapide d'informations électroniques désignées expressément, y compris des données de trafic, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles d'être supprimées, copiées ou modifiées, y compris en raison de l'expiration de la période de conservation fixée par sa législation nationale ou par les conditions de service du fournisseur.

2. Lorsqu'un État partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne (y compris une personne morale) de préserver

certaines informations stockées se trouvant en sa possession ou sous son contrôle, il adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à préserver et à protéger l'intégrité desdites informations pendant une durée aussi longue que nécessaire, mais ne dépassant pas la durée prévue par la législation nationale de l'État partie, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Un État partie peut prévoir le renouvellement d'une telle injonction.

3. Chaque État partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour obliger le dépositaire des informations ou une autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 31 et 32 de la présente Convention.

Article 35
Préservation et divulgation rapides de données de trafic

1. Afin d'assurer la préservation des données de trafic, en application de l'article 34 de la présente Convention, chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour :

a) Veiller à ce que la préservation rapide des données de trafic soit possible indépendamment du nombre de fournisseur de services ayant participé à la transmission de ces informations ; et

b) Assurer la divulgation rapide aux autorités compétentes de l'État partie d'une quantité suffisante de données de trafic pour permettre à l'État partie d'identifier les fournisseurs de services et la voie par laquelle les informations ont été transmises.

2. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 31 et 32 de la présente Convention.

Article 36
Injonction de produire

1. Aux fins énoncées au paragraphe 1 de l'article 31 de la présente Convention, chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a) À une personne présente sur son territoire de communiquer des données électroniques désignées expressément, en sa possession ou sous son contrôle ;

b) À un fournisseur de services offrant des prestations sur le territoire de l'État partie de communiquer des renseignements en sa possession ou sous son contrôle sur les abonnés.

2. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 31 et 32 de la présente Convention.

3. Aux fins du présent article, l'expression « renseignements sur les abonnés » désigne toute information détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données de trafic ou de contenu, et permettant d'établir :

a) Le type de service d'information et de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b) L'identité, les adresses postales ou autres et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, y compris l'adresse de protocole Internet et les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c) Toute autre information relative à l'endroit où sont localisés les équipements informatiques correspondant au contrat ou à l'accord de prestation de services.

Article 37
Perquisition et saisie d'informations stockées ou traitées électroniquement

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à chercher à obtenir accès sur son territoire ou dans sa juridiction à :

a) Des appareils informatiques et aux informations qui y sont stockées ; et

b) Des supports de stockage d'informations où les informations électroniques recherchées sont susceptibles d'être stockées.

2. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que, lorsque ses autorités compétentes, dans le cadre d'une perquisition menée en application des dispositions du paragraphe 1 a), ont des raisons de penser que les informations recherchées sont stockées dans un autre appareil informatique situé sur son territoire, elles soient en mesure d'étendre rapidement la perquisition pour obtenir l'accès à cet autre appareil ou aux données qu'il contient.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire des informations électroniques sur son territoire ou dans sa juridiction. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un appareil ou système électronique utilisé pour stocker des informations ;

b) Réaliser et conserver une copie de ces données aux formats électronique et numérique ;

c) Préserver l'intégrité des informations stockées pertinentes ;

d) Enlever ces informations de l'appareil ou du système électronique consulté.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner, selon la procédure établie par son droit interne, à toute personne possédant une connaissance spécialisée du fonctionnement du système informatique en question, du réseau d'information et de télécommunications, ou de leurs éléments constitutifs, ou des mesures appliquées pour protéger les informations que contiennent ces dispositifs, de fournir toutes les informations ou l'assistance nécessaires pour permettre l'application des mesures visées aux paragraphes 1 à 3 du présent article.

5. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 31 et 32 de la présente Convention

Article 38
Collecte en temps réel de données de trafic

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a) Collecter ou enregistrer, à l'aide des moyens techniques appropriés, les données de trafic associées à l'utilisation de technologies de l'information et des communications sur son territoire ; et

b) Obliger les fournisseurs de services, dans les limites de leurs capacités techniques :

i) À collecter ou à enregistrer des données de trafic sur son territoire, à l'aide des moyens techniques appropriés ; ou

ii) À prêter à ses autorités compétentes leur concours et leur assistance pour collecter ou enregistrer, en temps réel, les données de trafic associées à des informations spécifiques transmises sur son territoire.

2. Lorsqu'un État partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a) du présent article, il peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données de trafic sur son territoire, à l'aide des moyens techniques existant sur ce territoire.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 31 et 32 de la présente Convention.

Article 39
Compétence

1. Chaque État partie adopte toutes les mesures qui sont nécessaires pour établir sa compétence à l'égard des infractions pénales et autres actes illégaux incriminés en application de la présente Convention, dans les cas suivants :

a) Lorsque l'infraction est commise sur son territoire ; ou

b) Lorsque l'infraction est commise à bord d'un navire battant son pavillon ou à bord d'un aéronef immatriculé conformément à son droit interne au moment de la commission de ladite infraction.

2. Sous réserve de l'article 3 de la présente Convention, un État partie peut également établir sa compétence à l'égard de l'une quelconque de ces infractions et autres actes illégaux dans les cas suivants :

a) Lorsque l'infraction est commise à l'encontre d'un de ses ressortissants, d'une personne apatride résidant de façon permanente sur son territoire, d'une personne morale établie ou ayant une représentation permanente sur son territoire, d'une de ses installations gouvernementales ou publiques, notamment les locaux d'une de ses missions diplomatiques ou d'un de ses postes consulaires ; ou

b) Lorsque l'infraction est commise par un de ses ressortissants ou par une personne apatride résidant habituellement sur son territoire ; ou

c) Lorsque l'infraction est commise à son encontre ; ou

d) Lorsque l'infraction est commise en tout ou en partie hors de son territoire mais a, sur son territoire, des effets qui constituent une infraction ou entraînent la commission d'une infraction.

3. Aux fins de l'article 47 de la présente Convention, chaque État partie adopte toutes les mesures qui sont nécessaires pour établir sa compétence à l'égard des infractions incriminées en application de la présente Convention lorsque l'auteur présumé se trouve sur son territoire et qu'il n'extrade pas cette personne aux seuls motifs qu'elle est un de ses ressortissants ou qu'il lui a accordé le statut de réfugié.

4. S'il n'extrade pas l'auteur présumé d'une infraction, l'État partie sur le territoire duquel se trouve cette personne doit, dans les cas prévus aux paragraphes 1 et 2 du présent article, sans aucune exception et que l'infraction ait été ou non commise sur son territoire, soumettre l'affaire sans retard à ses autorités compétentes pour l'exercice de l'action pénale selon une procédure conforme à sa législation.

5. Si un État partie qui exerce sa compétence en vertu du paragraphe 1 ou 2 du présent article est avisé, ou apprend de toute autre façon, que d'autres États parties mènent une enquête ou ont engagé des poursuites ou une procédure judiciaire

concernant le même acte, les autorités compétentes de ces États parties se consultent, selon qu'il convient, pour coordonner leurs actions.

6. Sans préjudice des normes du droit international général, la présente Convention n'exclut pas l'exercice de toute compétence pénale ou administrative établie par un État partie conformément à son droit interne.

Chapitre III. Mesures visant à prévenir et à combattre les infractions et autres actes illégaux commis dans le cyberespace

[…]

Article 45
Mesures de protection des témoins

Chaque État partie envisage d'adopter les mesures législatives qui peuvent se révéler nécessaires pour assurer une protection efficace aux personnes suivantes :

a) Les personnes qui, de bonne foi et pour des motifs raisonnables, fournissent des informations concernant des actes illégaux visés aux articles 6 à 28 de la présente Convention ou coopèrent d'une autre manière avec les services d'enquête ou les autorités judiciaires ;

b) Les personnes qui déposent en tant que témoins au sujet d'actes illégaux visés aux articles 6 à 28 de la présente Convention ou qui en sont victimes ;

c) Le cas échéant, les membres de la famille des personnes visées aux alinéas a) et b) du présent article.

Afrique du Sud

[Original : anglais]
[14 avril 2022]

Chapitre III. Mesures procédurales, détection et répression

Article 18
Dispositions procédurales

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans le présent article aux fins d'enquêtes ou de procédures pénales spécifiques.

2. Sauf disposition contraire figurant à l'article 32, chaque Partie applique les pouvoirs et procédures visés au paragraphe 1 du présent article :

a) Aux infractions pénales liées à l'utilisation des technologies de l'information et des communications établies conformément aux articles [...] à [...] de la présente Convention ;

b) À toutes les autres infractions pénales commises au moyen des technologies de l'information et des communications ; et

c) À la collecte de preuves sous forme électronique d'une infraction pénale liée à l'utilisation des technologies de l'information et des communications.

3. Chaque État partie peut se réserver le droit de n'appliquer les mesures visées à l'article 31 qu'aux infractions ou catégories d'infractions liées à l'utilisation des technologies de l'information et des communications spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles il applique les mesures visées à l'article 32. Chaque Partie envisage de limiter une telle réserve de manière à permettre l'application la plus large possible des mesures visées à l'article 31.

4. Lorsqu'en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, un État partie ne peut appliquer les mesures visées aux articles 31 et 32 aux communications transmises à l'aide des technologies de l'information et des communications mises à disposition par un fournisseur de services, et que le système concerné :

a) Est exploité au profit d'un groupe fermé d'utilisateurs ; et

b) N'emploie pas les réseaux publics de communications et n'est pas relié à d'autres technologies de l'information et des communications, qu'elles soient publiques ou privées, cette Partie peut se réserver le droit de ne pas appliquer lesdites mesures à ces communications. Chaque Partie envisage de limiter une telle réserve de manière à permettre l'application la plus large possible des mesures visées aux articles 31 et 32.

Article 19
Conditions et sauvegardes

1. Chaque État partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le présent article soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits humains et des libertés, notamment des droits et libertés fondamentales découlant des obligations qu'il a contractées au titre d'accords, de traités et d'instruments internationaux applicables relatifs aux droits humains, et qui doit intégrer le principe de la proportionnalité dans le respect de sa souveraineté.

2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt général, en particulier à la bonne administration de la justice, chaque État partie examine l'effet des pouvoirs et procédures visés dans le présent article sur les droits, responsabilités et intérêts légitimes des tiers.

Article 20
Préservation accélérée de données informatiques stockées

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une façon similaire la préservation accélérée de certaines données électroniques, y compris des données de trafic, qui ont été stockées au moyen des technologies de l'information et des communications, notamment lorsqu'il y a des raisons de penser que ces données sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'un État partie porte application du paragraphe 1 ci-dessus, au moyen d'une injonction adressée à une personne de préserver des données stockées se trouvant en sa possession ou sous son contrôle, il adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à préserver et protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, dans la limite de sept jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir le renouvellement d'une telle injonction.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 27 et 28.

Article 21
Perquisition et saisie de données informatiques stockées

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à accéder au moyen d'une perquisition ou d'une façon similaire :

a) À des technologies de l'information et des communications, à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b) À un support permettant de stocker des données informatiques sur son territoire.

2. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités accèdent au moyen d'une perquisition ou d'une façon similaire à des technologies de l'information et des communications, à des composantes de celles-ci, à un système informatique ou à une partie de celui-ci, conformément au paragraphe 1 a), et ont des raisons de penser que les données recherchées sont stockées dans d'autres technologies de l'information et des communications, dans des composantes de celles-ci, dans un autre système informatique ou dans une partie de celui-ci, lesquels étant situés sur son territoire, et que ces données sont légalement accessibles à partir du premier système ou disponibles pour celui-ci, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou le moyen similaire d'accéder à l'autre système.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire avec, s'il y a lieu, l'assistance des agents mandatés de la Partie étrangère ou de l'autre Partie, ou en leur présence, les données informatiques auxquelles elles ont accédé en application du paragraphe 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire des technologies de l'information et des communications ou des composantes de celles-ci, un système informatique ou une partie de celui-ci, ou un support de stockage de données informatiques ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées pertinentes ;

d) Rendre ces données informatiques inaccessibles ou les retirer du système informatique consulté ou des technologies de l'information et des communications avec lesquelles une connexion a été établie.

4. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement des technologies de l'information et des communications, de composantes de celles-ci, d'un système informatique ou des mesures appliquées pour protéger les données informatiques qu'ils contiennent de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées aux paragraphes 1 et 2.

5. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 27 et 28.

Article 22
Collecte en temps réel de données de trafic

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; et

b) Obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ; ou

ii) À prêter aux autorités compétentes son concours et son assistance pour la collecte ou l'enregistrement en temps réel de données de trafic associées à des communications transmises sur son territoire au moyen de technologies de l'information et des communications ou d'un système informatique.

Article 23
Interception de données de contenu

1. En ce qui concerne un éventail d'infractions graves à définir en droit interne, chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; et

b) Obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ; ou

ii) À prêter aux autorités compétentes son concours et son assistance pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications transmises sur son territoire au moyen de technologies de l'information et des communications ou d'un système informatique.

2. Lorsqu'un État partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a), il peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 27 et 28.

Article 24
Gel, saisie et confiscation

1. Nonobstant le fait que l'interprétation des dispositions du présent article ne doit en aucun cas porter atteinte aux droits des tiers de bonne foi et qu'aucune disposition du présent article ne porte atteinte au principe selon lequel les mesures qui y sont visées sont définies et exécutées conformément aux dispositions du droit interne de chaque État partie et sous réserve de celles-ci.

2. L'interprétation des dispositions du présent article ne doit en aucun cas porter atteinte aux droits des tiers de bonne foi.

3. Aucune disposition du présent article ne porte atteinte au principe selon lequel les mesures qui y sont visées sont définies et exécutées conformément aux dispositions du droit interne de chaque État partie et sous réserve de celles-ci.

4. Chaque État partie prend, dans toute la mesure possible dans le cadre de son système juridique interne, les mesures nécessaires pour permettre la confiscation :

a) Du produit du crime provenant d'infractions découlant de l'utilisation des technologies de l'information et des communications et établies conformément à la présente Convention ou de biens dont la valeur correspond à celle de ce produit, au profit de l'État partie lésé ;

b) Des biens, matériels ou autres instruments, y compris des technologies de l'information et des communications, utilisés ou destinés à être utilisés pour les infractions établies conformément à la présente Convention.

4. Chaque État partie prend les mesures nécessaires pour permettre l'identification, la localisation, le gel ou la saisie de tout ce qui est mentionné au paragraphe 1 du présent article aux fins de confiscation ultérieure.

5. Chaque État partie adopte, conformément à son droit interne, les mesures législatives et autres nécessaires pour réglementer l'administration par les autorités compétentes des biens gelés, saisis ou confisqués visés aux paragraphes 1 et 2 du présent article.

6. Si ce produit du crime a été transformé ou converti, en partie ou en totalité, en d'autres biens, ces derniers peuvent faire l'objet des mesures visées au présent article en lieu et place dudit produit.

7. Si ce produit du crime a été mêlé à des biens acquis légitimement, ces biens, sans préjudice de tout pouvoir de gel ou de saisie, sont confiscables à concurrence de la valeur estimée du produit qui y a été mêlé.

8. Les revenus ou autres avantages tirés de ce produit du crime, des biens en lesquels le produit a été transformé ou converti ou des biens auxquels il a été mêlé peuvent aussi faire l'objet des mesures visées au présent article, de la même manière et dans la même mesure que le produit du crime.

9. Aux fins du présent article et de l'article […] de la présente Convention, [relatif à la coopération internationale,] chaque État partie habilite ses tribunaux ou autres autorités compétentes à ordonner la production ou la saisie de documents bancaires, financiers ou commerciaux. Un État partie ne peut invoquer le secret bancaire pour refuser de donner effet aux dispositions du présent paragraphe.

10. Les États parties peuvent envisager d'exiger que l'auteur d'une infraction établisse l'origine licite du produit présumé du crime ou d'autres biens confiscables, dans la mesure où cette exigence est conforme aux principes fondamentaux de leur droit interne et à la nature des procédures judiciaires et autres.

Article 25
Disposition du produit du crime ou des biens confisqués

1. Un État partie qui confisque le produit du crime ou des biens en application du paragraphe 3 de l'article 33 de la présente Convention en dispose conformément à son droit interne et à ses procédures administratives.

2. Lorsque les États parties agissent à la demande d'un autre État partie en application de l'article 39 de la présente Convention, ils doivent, dans la mesure où leur droit interne le leur permet et si la demande leur en est faite, envisager à titre prioritaire de restituer le produit du crime ou les biens confisqués à l'État partie requérant, afin que ce dernier puisse indemniser les victimes de l'infraction ou restituer ce produit du crime ou ces biens à leurs propriétaires légitimes.

3. Lorsqu'un État partie agit à la demande d'un autre État partie en application de l'article 41 de la présente Convention, il peut envisager spécialement de conclure des accords ou arrangements prévoyant :

a) De verser la valeur de ce produit ou de ces biens, ou les fonds provenant de leur vente, ou une partie de ceux-ci, au compte établi en application de l'article […] de la présente Convention et à des organismes intergouvernementaux spécialisés dans la lutte contre la criminalité organisée ;

b) De partager avec d'autres États parties, systématiquement ou au cas par cas, ce produit ou ces biens, ou les fonds provenant de leur vente, conformément à son droit interne ou à ses procédures administratives.

Article 26
Antécédents judiciaires

Chaque État partie peut adopter les mesures législatives ou autres nécessaires pour tenir compte, dans les conditions et aux fins qu'il juge appropriées, de toute condamnation dont l'auteur présumé d'une infraction aurait antérieurement fait l'objet dans un autre État, afin d'utiliser cette information dans le cadre d'une procédure pénale relative à une infraction découlant de l'utilisation des technologies de l'information et des communications et établie conformément à la présente Convention.

Article 27
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 des groupes criminels organisés :

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 les activités des groupes criminels organisés, ou le lieu où ils se trouvent ;

ii) Les liens, y compris à l'échelon international, avec d'autres groupes criminels organisés ;

iii) Les infractions que les groupes criminels organisés ont commises ou pourraient commettre ;

b) À fournir une aide factuelle et concrète aux autorités compétentes, qui pourrait contribuer à priver les groupes criminels organisés de leurs 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, de bonne foi, coopère de manière substantielle à l'enquête ou aux poursuites relatives à une infraction 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, de bonne foi, coopère de manière substantielle à l'enquête ou aux poursuites relatives à une infraction liée à l'utilisation des technologies de l'information et des communications et visée par la présente Convention.

4. La protection de ces personnes est assurée comme le prévoit l'article 34 de la présente Convention.

5. Lorsqu'une personne qui est visée au paragraphe 1 du présent article et se trouve dans un État partie peut, de bonne foi, 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 28
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 liées à l'utilisation des technologies de

l'information et des communications et visées par la présente Convention. En particulier, chaque État partie adopte des mesures efficaces pour :

a) Renforcer les voies de communication entre leurs autorités, organismes et fournisseurs d'accès à Internet compétents et, si nécessaire, en établir afin de faciliter l'échange sûr et rapide d'informations concernant tous les aspects des infractions liées à l'utilisation des technologies de l'information et des communications et 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 liées à l'utilisation des technologies de l'information et des communications et 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) Faciliter une coordination efficace entre leurs autorités, organismes et fournisseurs d'accès à Internet 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 ;

e) Échanger, avec d'autres États parties, des informations sur les moyens et procédés spécifiques employés par les groupes criminels organisés, y compris, s'il y a lieu, sur les itinéraires et les moyens de transport ainsi que sur l'usage de fausses identités, de documents modifiés ou falsifiés ou d'autres moyens de dissimulation de leurs activités à l'aide des technologies de l'information et des communications ;

f) Échanger des informations et coordonner les mesures administratives et autres prises, comme il convient, pour détecter au plus tôt les infractions liées à l'utilisation des technologies de l'information et des communications et visées par la présente Convention.

2. Afin de donner effet à la présente Convention, les États parties envisagent de conclure des accords ou 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 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 faire face à la criminalité transnationale organisée perpétrée au moyen des technologies de l'information et des communications.

Article 29
Enquêtes conjointes

Les États parties envisagent de conclure des accords ou des arrangements bilatéraux ou multilatéraux en vertu desquels, pour les affaires qui font l'objet d'enquêtes, de poursuites ou de procédures judiciaires dans un ou plusieurs États, les

autorités compétentes concernées peuvent établir des instances d'enquête conjointes. En l'absence de tels accords ou arrangements, des enquêtes conjointes peuvent être décidées au cas par cas. Les États parties concernés veillent à ce que la souveraineté de l'État partie sur le territoire duquel l'enquête doit se dérouler soit pleinement respectée.

Article 30
Techniques d'enquête spéciales

1. Afin de combattre efficacement l'utilisation des technologies de l'information et des communications à des fins criminelles, chaque État partie, dans la mesure où les principes fondamentaux de son système juridique interne le permettent et conformément aux conditions prescrites par son droit interne, prend, dans la limite de ses moyens, les mesures nécessaires pour permettre l'utilisation, sur son territoire, de techniques d'enquête spéciales, telles que la surveillance électronique ou d'autres formes de surveillance et les opérations d'infiltration, et pour que les preuves recueillies au moyen de ces techniques soient admissibles devant ses tribunaux, sans compromettre la cybersécurité et la confidentialité des renseignements de chaque État partie.

2. Aux fins des enquêtes sur les infractions liées à l'utilisation des technologies de l'information et des communications et 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 aux techniques d'enquête spéciales dans le cadre de la coopération internationale. Ces accords ou arrangements sont conclus et appliqués dans le plein respect du principe de l'égalité souveraine des États et des libertés et droits humains fondamentaux et ils sont 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, les décisions de recourir à des techniques d'enquête spéciales au niveau international sont prises au cas par cas et peuvent, si nécessaire, tenir compte d'ententes et d'arrangements financiers quant à l'exercice de leur compétence par les États parties concernés.

Article 31
Restitution et disposition des avoirs

1. Un État partie ayant confisqué des biens en application de l'article 33 ou 34 de la présente Convention en dispose, y compris en les restituant à leurs propriétaires légitimes antérieurs, en application du paragraphe 3 du présent article et conformément aux dispositions de la présente Convention et à son droit interne.

2. Chaque État partie adopte, conformément aux principes fondamentaux de son droit interne, les mesures législatives et autres nécessaires pour permettre à ses autorités compétentes de restituer les biens confisqués, lorsqu'il agit à la demande d'un autre État partie, conformément à la présente Convention, et compte tenu des droits des tiers de bonne foi.

3. Conformément aux paragraphes 1 et 2 du présent article, l'État partie requis :

a) Dans les cas de lutte contre l'utilisation des technologies de l'information et des communications visée par la présente Convention, lorsque la confiscation a été exécutée conformément à l'article […] et sur la base d'un jugement définitif rendu dans l'État partie requérant, exigence à laquelle il peut renoncer, restitue les biens confisqués à l'État partie requérant ;

b) Dans le cas du produit de toute autre infraction liée à l'utilisation des technologies de l'information et des communications et visée par la présente Convention, lorsque la confiscation a été exécutée conformément à l'article […] de la présente Convention et sur la base d'un jugement définitif dans l'État partie requérant, exigence à laquelle il peut renoncer, restitue les biens confisqués à l'État partie requérant, lorsque ce dernier fournit des preuves raisonnables de son droit de

propriété antérieur sur lesdits biens à l'État partie requis ou lorsque ce dernier reconnaît un préjudice à l'État partie requérant comme base de restitution des biens confisqués ;

c) Dans tous les autres cas, envisage à titre prioritaire de restituer les biens confisqués à l'État partie requérant, de les restituer à ses propriétaires légitimes antérieurs ou de dédommager les victimes de l'infraction.

4. S'il y a lieu, et sauf si les États parties en décident autrement, l'État partie requis peut déduire des dépenses raisonnables engagées pour les enquêtes, poursuites ou procédures judiciaires ayant abouti à la restitution ou à la disposition des biens confisqués en application du présent article.

5. S'il y a lieu, les États parties peuvent aussi, conformément à leur droit interne, envisager en particulier de conclure, au cas par cas, des accords ou des arrangements mutuellement acceptables pour la disposition définitive des biens confisqués.

Suisse

[Original : anglais]
[8 avril 2022]

2.3 Dispositions relatives aux mesures procédurales, à la détection et à la répression

Section 1

Dispositions communes

Champ d'application des mesures du droit de procédure

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2. Chaque Partie applique les pouvoirs et procédures visés au paragraphe 1 du présent article :

a) Aux infractions pénales établies conformément aux dispositions de la présente Convention relatives à l'incrimination ;

b) À toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c) À la collecte de preuves sous forme électronique d'une infraction pénale.

3. a) Chaque Partie peut se réserver le droit de n'appliquer les mesures relatives à la collecte en temps réel des données de trafic qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures relatives à l'interception de données de contenu. Chaque Partie envisage de limiter une telle réserve de manière à permettre l'application la plus large possible des mesures relatives à la collecte en temps réel des données de trafic ;

b) Lorsqu'en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, une Partie ne peut appliquer les mesures relatives à la collecte en temps réel des données de trafic et à l'interception de données de contenu aux communications transmises dans le système informatique d'un fournisseur de services, et que ce système :

i) Est exploité au profit d'un groupe fermé d'utilisateurs ; et

ii) N'emploie pas les réseaux publics de communications et n'est pas relié à un autre système informatique, qu'il soit public ou privé,

cette Partie peut se réserver le droit de ne pas appliquer lesdites mesures à ces communications. Chaque Partie envisage de limiter une telle réserve de manière à permettre l'application la plus large possible des mesures relatives à la collecte en temps réel des données de trafic et à l'interception de données de contenu.

Conditions et sauvegardes

1. Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits humains et des libertés, notamment des droits découlant des obligations qu'elle a contractées au titre du Pacte international relatif aux droits civils et politiques et d'autres instruments internationaux et régionaux applicables relatifs aux droits humains, et qui doit intégrer le principe de la proportionnalité.

2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt général, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures visés dans la présente section sur les droits, responsabilités et intérêts légitimes des tiers.

Préservation accélérée de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une façon similaire la préservation accélérée de données électroniques, y compris des données de trafic, qui ont été stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie porte application du paragraphe 1 ci-dessus, au moyen d'une injonction adressée à une personne de préserver des données stockées se trouvant en sa possession ou sous son contrôle, elle adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à préserver et protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, dans la limite de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir le renouvellement d'une telle injonction.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les dispositions de la présente Convention relatives au champ d'application des mesures du droit de procédure et aux conditions et sauvegardes.

Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a) À une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et

b) À un fournisseur de services assurant des prestations sur son territoire de communiquer des renseignements en sa possession ou sous son contrôle sur des abonnés à de tels services.

2. Les pouvoirs et procédures visés dans le présent article sont régis par les dispositions de la présente Convention relatives au champ d'application des mesures du droit de procédure et aux conditions et sauvegardes.

3. Aux fins du présent article, l'expression « renseignements sur l'abonné » s'entend de toute information détenue par un fournisseur de services sous forme de données informatiques ou sous toute autre forme, se rapportant aux abonnés de ses services, autres que des données de trafic ou de contenu, et permettant d'établir :

a) Le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b) L'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c) Toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à accéder au moyen d'une perquisition ou d'une façon similaire :

a) À un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b) À un support permettant de stocker des données informatiques sur son territoire.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités accèdent au moyen d'une perquisition ou d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire et qu'elles sont légalement accessibles à partir du premier système ou disponibles pour celui-ci, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou le moyen similaire d'accéder à l'autre système.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques auxquelles elles ont accédé en application du paragraphe 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage de données informatiques ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées pertinentes ;

d) Rendre ces données informatiques inaccessibles ou les retirer du système informatique consulté.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées aux paragraphes 1 et 2.

5. Les pouvoirs et procédures visés dans le présent article sont régis par les dispositions de la présente Convention relatives au champ d'application des mesures du droit de procédure et aux conditions et sauvegardes.

Section 2

Compétence

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux dispositions de la présente Convention relatives à l'incrimination, lorsque l'infraction est commise :

a) Sur son territoire ; ou

b) À bord d'un navire qui bat son pavillon ou à bord d'un aéronef immatriculé selon ses lois ; ou

c) Par un de ses ressortissants, si l'infraction est punissable en vertu du droit de l'État où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.

2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1 b) à 1 d) du présent article ou dans une partie quelconque de ces paragraphes.

3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction établie conformément aux dispositions de la présente Convention relatives à l'incrimination lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition, à condition que l'infraction soit punissable 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.

4. Une Partie peut également établir sa compétence à l'égard de toute infraction pénale établie conformément aux dispositions de la présente Convention relatives à l'incrimination, lorsque l'infraction est commise :

a) Contre l'un de ses ressortissants ;

b) Contre cette Partie.

5. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

6. Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée établie conformément à la présente Convention, les Parties concernées se concertent, s'il y a lieu, afin de déterminer laquelle est la mieux à même d'exercer les poursuites.

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

[Original : anglais]
[12 avril 2022]

Chapitre III. Mesures procédurales, détection et répression

Article 16
Conditions et sauvegardes

1. Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection

adéquate des droits humains et des libertés, notamment des droits découlant des obligations qu'elle a contractées au titre du Pacte international relatif aux droits civils et politiques et d'autres dispositions du droit international des droits de l'homme s'appliquant, et qui doit intégrer les principes de la proportionnalité.

2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans la présente section sur les droits, responsabilités et intérêts légitimes des tiers.

Article 17
Portée d'application des mesures du droit de procédure, y compris une utilisation plus large du droit procédural pour toutes les infractions

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2. Sauf disposition contraire, chaque Partie applique les pouvoirs et procédures visés au paragraphe 1 du présent article :

a) Aux infractions pénales établies conformément aux infractions définies dans la présente Convention ;

b) À toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c) À la collecte des preuves électroniques de toute infraction pénale.

Article 18
Conservation rapide

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une façon similaire la préservation accélérée de données électroniques, y compris des données de trafic, qui ont été stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie porte application du paragraphe 1 ci-dessus, au moyen d'une injonction adressée à une personne de préserver des données stockées se trouvant en sa possession ou sous son contrôle, elle adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à préserver et protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, dans la limite de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction sera renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures visés dans le présent article sont régis par des garanties relatives aux droits humains.

Article 19
Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a) À une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et

b) À un fournisseur de services assurant des prestations sur son territoire de communiquer des renseignements en sa possession ou sous son contrôle sur des abonnés à de tels services.

c) Les pouvoirs et procédures visés dans le présent article sont régis par des garanties relatives aux droits humains.

2. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

a) Le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b) L'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c) Toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Article 20
Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a) À un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b) À un support permettant de stocker des données informatiques sur son territoire.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent un système informatique ou une partie de celui-ci ou y accèdent d'une façon similaire, conformément à l'alinéa a) du paragraphe 1, et qu'elles ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique situé sur son territoire, ou une partie de celui-ci, et qu'elles sont légalement accessibles à partir du premier système ou disponibles pour celui-ci, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou le moyen similaire d'accéder à l'autre système.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques auxquelles elles ont accédé en application du paragraphe 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage de données informatiques ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées voulues ;

d) Rendre ces données informatiques inaccessibles ou les retirer du système informatique consulté.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5. Les pouvoirs et procédures visés dans le présent article sont régis par des garanties relatives aux droits humains.

République-Unie de Tanzanie

[Original : anglais]
[8 avril 2022]

5. Mesures procédurales

Les lois sur la cybercriminalité fixent des normes de comportement acceptable pour les personnes utilisant les technologies de l'information et des communications, prévoient des sanctions sociojuridiques pour les infractions relevant de la cybercriminalité et protègent les personnes utilisant les technologies de l'information et des communications, en général, et atténuent et/ou préviennent les dommages causés aux personnes, aux données, aux systèmes, aux services et aux infrastructures. La République-Unie de Tanzanie propose que les aspects ci-après soient pris en compte dans la Convention, à la section relative aux mesures procédurales :

Préservation et divulgation rapides de données électroniques

La Convention devrait comporter une disposition permettant aux États Membres d'inclure dans leur législation nationale, selon que de besoin, les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

Lorsqu'une Partie, ordonne au moyen d'une injonction à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, elle adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction sera renouvelée par la suite.

La Convention devrait comporter une disposition permettant aux États parties d'adopter les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou toute autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

Injonction de produire

La Convention devrait comporter une disposition permettant de prendre les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à une personne se trouvant sur son territoire de soumettre des données informatiques spécifiques en la possession ou sous le contrôle de cette

personne, qui sont stockées dans un système informatique ou sur un support de stockage de données informatiques.

Perquisition et saisie de données informatiques stockées

La Convention doit impérativement imposer aux États Membres l'obligation de prévoir dans leur législation des dispositions et autres mesures qui se révèlent nécessaires pour habiliter leurs autorités compétentes à fouiller un système informatique dans lequel des données informatiques peuvent être stockées sur son territoire ou une partie de celui-ci, à y accéder et à s'en saisir, ainsi que les données informatiques qui y sont stockées.

Protection des lanceurs d'alerte et des témoins

La Convention devrait obliger les Parties à prévoir des mesures de protection des dénonciateurs, des témoins et des victimes de cybercrimes, selon les affaires.

Il est par ailleurs proposé que la Convention exige que chaque État Membre prenne, dans la limite de ses moyens, des mesures appropriées pour assurer une protection efficace contre des actes éventuels de représailles ou d'intimidation aux lanceurs d'alerte et aux témoins qui, dans le cadre de procédures pénales, font un témoignage concernant les infractions visées par la présente Convention et, le cas échéant, à leurs parents et à d'autres personnes qui leur sont proches, conformément à leurs lois internes. Ces mesures ne doivent pas porter atteinte aux droits du défendeur, y compris le droit à une procédure régulière.

6. Détection et répression

La bonne gestion de la cybercriminalité et des infractions connexes fait appel à plusieurs types d'interventions, qui sont la prévention, la détection et la lutte. Ces interventions, qui incombent par la loi aux services de détection et de répression, doivent être reconnues. Par conséquent, la République-Unie de Tanzanie est d'avis que la Convention devrait couvrir les aspects suivants en matière de détection et de répression.

Formation, assistance technique et échange de compétences

Pour prévenir et combattre efficacement l'utilisation des technologies de l'information et des communications à des fins criminelles, il est essentiel de fournir une assistance technique aux pays en développement et de renforcer l'échange d'informations. L'assistance technique et l'échange de compétences devraient être axés sur les points suivants :

a) Détection, prévention des infractions visées par la Convention et lutte contre celles-ci ;

b) Techniques employées par les personnes soupçonnées d'être impliquées dans des infractions visées par la Convention, et mesures de lutte appropriées ;

c) Surveillance du mouvement des produits de contrebande ;

d) Détection et surveillance du produit du crime, des biens, des matériels ou des autres instruments, et méthodes de transfert, de dissimulation ou de déguisement de ce produit et de ces autres instruments, ainsi que les méthodes de lutte contre la cybercriminalité ;

e) Rassemblement des éléments de preuve ;

f) Matériels et techniques modernes de détection et de répression, y compris l'utilisation de nouveaux logiciels et les opérations d'infiltration ;

g) Méthodes utilisées pour combattre les actes de cybercriminalité perpétrés au moyen de systèmes informatiques, de réseaux de télécommunication ou d'autres techniques modernes ;

h) Planification et mise en œuvre de programmes de recherche et de formation destinés à échanger les compétences sur la protection du cyberespace.

Enquêtes conjointes

La cybercriminalité ne connaît pas de frontières et peut concerner plus d'un pays. La Convention devrait prévoir l'obligation pour les États parties de prendre des dispositions concernant les affaires qui font l'objet d'enquêtes, de poursuites ou de procédures judiciaires dans un ou plusieurs États. Les autorités compétentes peuvent constituer des organes d'enquête conjoints. Les États parties concernés sont priés de veiller à ce que la souveraineté de l'État partie sur le territoire duquel l'enquête doit se dérouler soit pleinement respectée.

Appui financier

La Convention devrait comporter une disposition imposant aux États développés et aux organismes des Nations Unies de fournir un appui financier aux pays en développement afin qu'ils puissent mettre en œuvre des stratégies de détection, de prévention et de lutte contre la cybercriminalité.

États-Unis d'Amérique

[Original : anglais]
[8 avril 2022]

Mesures procédurales, détection et répression

Mesures du droit de procédure

Portée d'application des mesures du droit de procédure

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2. Sauf disposition contraire figurant à l'article relatif à l'interception des données, chaque État partie applique les pouvoirs et procédures visés au paragraphe 1 du présent article :

a) Aux infractions pénales établies conformément au chapitre de la présente Convention relative à l'incrimination ;

b) À toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c) À la collecte de preuves sous forme électronique d'une infraction pénale.

Préservation accélérée de données informatiques stockées

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une façon similaire la préservation accélérée de données électroniques, y compris des données de trafic, qui ont été stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'un État partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cet État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de 90 jours, afin de permettre aux autorités compétentes

d'obtenir leur divulgation. Un État partie peut prévoir le renouvellement d'une telle injonction.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

Injonction de produire

1. Chaque État partie adopte des mesures législatives et autres qui se révèlent nécessaires pour habiliter les autorités compétentes à ordonner à une personne se trouvant sur son territoire de soumettre des données informatiques spécifiques en la possession ou sous le contrôle de cette personne, qui sont stockées dans un système informatique ou sur un support de stockage de données informatiques.

Perquisition et saisie de données informatiques stockées

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a) À un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b) À un support permettant de stocker des données informatiques sur son territoire.

2. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage de données informatiques ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées voulues ;

d) Rendre ces données informatiques inaccessibles ou les retirer du système informatique consulté.

4. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

Collecte en temps réel de données de trafic

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; et

b) Obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; ou

ii) Prêter aux autorités compétentes son concours et son assistance pour la collecte ou l'enregistrement en temps réel de données de trafic associées à des communications transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'un État partie en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a), il peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données de trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

Interception de données de contenu

1. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes, en ce qui concerne un éventail d'infractions graves à définir en droit interne, à :

a) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b) Obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i) Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; ou

ii) Prêter aux autorités compétentes son concours et son assistance pour la collecte ou l'enregistrement en temps réel de données de trafic associées à des communications transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'un État partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1 a), il peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données de contenu associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

Juridiction[17]

1. Chaque État partie adopte les mesures nécessaires pour établir sa compétence à l'égard des infractions établies conformément à la présente Convention dans les cas suivants :

a) Lorsque l'infraction est commise sur son territoire ; ou

b) Lorsque l'infraction est commise à bord d'un navire qui bat son pavillon ou à bord d'un aéronef immatriculé conformément à son droit interne au moment où ladite infraction est commise.

2. Sous réserve de l'article relatif à la souveraineté de la présente Convention, un État partie peut également établir sa compétence à l'égard de l'une quelconque de ces infractions dans les cas suivants :

a) Lorsque l'infraction est commise à l'encontre d'un de ses ressortissants ; ou

b) Lorsque l'infraction est commise par l'un de ses ressortissants ou par une personne apatride résidant habituellement sur son territoire ; ou

c) L'infraction est l'une de celles établies conformément à l'article [article sur le blanchiment d'argent] de la présente Convention et est commise hors de son territoire en vue de la commission d'une infraction établie conformément à l'article [article sur le blanchiment d'argent] de la présente Convention sur son territoire ; ou

d) Lorsque l'infraction est commise à son encontre.

3. Aux fins de l'article relatif à l'extradition de la présente Convention, chaque État partie prend les mesures nécessaires pour établir sa compétence à l'égard des infractions établies conformément à la présente Convention lorsque l'auteur présumé se trouve sur son territoire et qu'il n'extrade pas cette personne au seul motif qu'elle est l'un de ses ressortissants.

4. Chaque État partie peut également prendre les mesures nécessaires pour établir sa compétence à l'égard des infractions établies conformément à la présente Convention lorsque l'auteur présumé se trouve sur son territoire et qu'il ne l'extrade pas.

5. Si un État partie qui exerce sa compétence en vertu du paragraphe 1 ou 2 du présent article a été avisé, ou a appris de toute autre façon, que d'autres États parties mènent une enquête ou ont engagé des poursuites ou une procédure judiciaire concernant le même acte, les autorités compétentes de ces États parties se consultent, selon qu'il convient, pour coordonner leurs actions.

6. Sans préjudice des normes du droit international général, la présente Convention n'exclut pas l'exercice de toute compétence pénale établie par un État partie conformément à son droit interne.

Confiscation et saisie[18]

1. Les États parties adoptent, dans toute la mesure possible dans le cadre de leurs systèmes juridiques nationaux, les mesures nécessaires pour permettre la confiscation :

a) Du produit du crime provenant d'infractions visées par la présente Convention ou de biens dont la valeur correspond à celle de ce produit ;

b) Biens, des matériels et autres instruments utilisés ou destinés à être utilisés pour les infractions visées par la présente Convention.

---

[17] Convention des Nations Unies contre la corruption, art. 42, et Convention des Nations Unies contre la criminalité transnationale organisée, art. 15.

[18] Convention contre la criminalité organisée, art. 12.

2. Les États parties adoptent les mesures nécessaires pour permettre l'identification, la localisation, le gel ou la saisie de tout ce qui est mentionné au paragraphe 1 du présent article aux fins de confiscation éventuelle.

3. Si le produit du crime a été transformé ou converti, en partie ou en totalité, en d'autres biens, ces derniers peuvent faire l'objet des mesures visées au présent article en lieu et place dudit produit.

4. Si le produit du crime a été mêlé à des biens acquis légitimement, ces biens, sans préjudice de tous pouvoirs de gel ou de saisie, peuvent être confisqués à concurrence de la valeur estimée du produit qui y a été mêlé.

5. Les revenus ou autres avantages tirés du produit du crime, des biens en lesquels le produit a été transformé ou converti ou des biens auxquels il a été mêlé peuvent aussi faire l'objet des mesures visées au présent article, de la même manière et dans la même mesure que le produit du crime.

6. Aux fins du présent article et de l'article relatif à la coopération internationale aux fins de la confiscation de la présente Convention, chaque État partie habilite ses tribunaux ou autres autorités compétentes à ordonner la production ou la saisie de documents bancaires, financiers ou commerciaux. Les États parties ne peuvent invoquer le secret bancaire pour refuser de donner effet aux dispositions du présent paragraphe.

7. Les États parties peuvent envisager d'exiger que l'auteur d'une infraction établisse l'origine licite du produit présumé du crime ou d'autres biens pouvant faire l'objet d'une confiscation, dans la mesure où cette exigence est conforme aux principes de leur droit interne et à la nature de la procédure judiciaire et des autres procédures.

8. L'interprétation des dispositions du présent article ne doit en aucun cas porter atteinte aux droits des tiers de bonne foi.

9. Aucune disposition du présent article ne porte atteinte au principe selon lequel les mesures qui y sont visées sont définies et exécutées conformément aux dispositions du droit interne de chaque État partie et sous réserve de celles-ci.

Disposition du produit du crime ou des biens confisqués[19]

1. Le produit du crime ou les biens confisqués par un État partie en vertu de l'article relatif à la confiscation et à la saisie et [tout article sur la coopération internationale aux fins de confiscation] de la présente Convention sont éliminés par cet État partie conformément à son droit interne et à ses procédures administratives.

2. Lorsque les États parties agissent à la demande d'un autre État partie en application de l'article de [tout article relatif à la coopération internationale aux fins de la confiscation] de la présente Convention, ils doivent, dans la mesure où leur droit interne le leur permet et si la demande leur en est faite, envisager à titre prioritaire de restituer le produit du crime ou les biens confisqués à l'État partie requérant, afin que ce dernier puisse indemniser les victimes de l'infraction ou restituer ce produit du crime ou ces biens à leurs propriétaires légitimes.

3. Lorsqu'il donne suite à la demande d'un autre État partie conformément à l'article sur la confiscation et la saisie et [tout type de coopération internationale aux fins de confiscation] de la présente Convention, un État partie peut, après avoir dûment pris en considération l'indemnisation des victimes, accorder une attention particulière à la conclusion d'accords ou d'arrangements tendant à :

a) Verser la valeur de ce produit ou de ces biens, ou les fonds provenant de leur vente, ou une partie de ceux-ci, au compte établi en application de [tout article

[19] Convention contre la criminalité organisée, art. 14.

relatif à l'assistance technique] de la présente Convention et à des organismes intergouvernementaux spécialisés dans la lutte contre la cybercriminalité ;

b) Partager avec d'autres États parties, systématiquement ou au cas par cas, ce produit ou ces biens, ou les fonds provenant de leur vente, conformément à son droit interne ou à ses procédures administratives.

Établissement des antécédents judiciaires[20]

Chaque État partie peut adopter les mesures législatives ou autres qui sont nécessaires pour tenir compte, dans les conditions et aux fins qu'il juge appropriées, de toute condamnation dont l'auteur présumé d'une infraction aurait antérieurement fait l'objet dans un autre État, afin d'utiliser cette information dans le cadre d'une procédure pénale relative à une infraction visée par la présente Convention.

Protection des témoins[21]

1. Chaque État partie prend, dans la limite de ses moyens, des mesures appropriées pour assurer une protection efficace contre des actes éventuels de représailles ou d'intimidation aux témoins qui, dans le cadre de procédures pénales, font un témoignage concernant les infractions visées par la présente Convention et, le cas échéant, à leurs parents et à d'autres personnes qui leur sont proches.

2. Les mesures envisagées au paragraphe 1 du présent article peuvent consister notamment, sans préjudice des droits du défendeur, y compris du droit à une procédure régulière :

a) À établir, pour la protection physique de ces personnes, des procédures visant notamment, selon les besoins et dans la mesure du possible, à leur fournir un nouveau domicile et à permettre, le cas échéant, que les renseignements concernant leur identité et le lieu où elles se trouvent ne soient pas divulgués ou que leur divulgation soit limitée ;

b) À prévoir des règles de preuve qui permettent aux témoins de déposer d'une manière qui garantisse leur sécurité, notamment à les autoriser à déposer en recourant à des techniques de communication telles que les liaisons vidéo ou à d'autres moyens adéquats.

3. Les États parties envisagent de conclure des accords ou arrangements avec d'autres États en vue de fournir un nouveau domicile aux personnes mentionnées au paragraphe 1 du présent article.

4. Les dispositions du présent article s'appliquent également aux victimes lorsqu'elles sont témoins.

Octroi d'une assistance et d'une protection aux victimes[22]

1. Chaque État partie prend, dans la limite de ses moyens, des mesures appropriées pour prêter assistance et accorder protection aux victimes d'infractions visées par la présente Convention, en particulier dans les cas de menace de représailles ou d'intimidation.

2. Chaque État partie établit des procédures appropriées pour permettre aux victimes d'infractions visées par la présente Convention d'obtenir réparation.

3. Chaque État partie, sous réserve de son droit interne, fait en sorte que les avis et préoccupations des victimes soient présentés et pris en compte aux stades appropriés de la procédure pénale engagée contre les auteurs d'infractions d'une manière qui ne porte pas préjudice aux droits de la défense.

---

[20] Convention contre la criminalité organisée, art. 22.

[21] Convention sur la criminalité organisée, art. 24, et Convention contre la corruption, art. 32.

[22] Convention contre la criminalité organisée, art. 25.

Mesures propres à renforcer la coopération avec les services de détection et de répression[23]

1. Chaque État partie prend des mesures appropriées pour encourager les personnes qui participent ou ont participé à des infractions établies par la présente Convention :

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, l'emplacement ou les activités des personnes participant aux infractions établies par la présente Convention ;

ii) Les liens, y compris les liens internationaux, avec d'autres personnes participant aux infractions établies par la présente Convention ;

iii) Les infractions que les personnes participant aux infractions établies dans la présente Convention ont commises ou peuvent commettre ;

b) À fournir une aide factuelle et concrète aux autorités compétentes, qui pourrait contribuer à priver les [personnes participant à des infractions établies par la présente Convention] de leurs 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 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 établie conformément à la présente Convention.

4. La protection de ces personnes est assurée comme cela est prévu dans l'article relatif à la protection des témoins de la présente Convention.

5. Lorsqu'une personne qui est visée au paragraphe 1 du présent article et se trouve dans un État partie 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.

Venezuela (République bolivarienne du)

[Original : espagnol]
[13 avril 2022]

6. Mesures procédurales, détection et répression

Concernant les procédures pénales, la détection et la répression, il est proposé, de manière générale, que la future convention établisse des mécanismes portant sur les aspects suivants :

- La coopération en matière de collecte et de partage de preuves et lors des autres phases d'enquête ;
- La détermination des responsabilités des acteurs non étatiques et la mise en place de cadres réglementaires définissant la portée de leurs obligations dans le cadre des processus liés à l'application du droit national et international ;

[23] Convention contre la criminalité organisée, art. 26.

- L'établissement de la compétence pour ce qui est de l'utilisation des technologies de l'information et des communications, dans une optique de coopération et sans préjudice de la souveraineté des États dans le contexte des enquêtes pénales.

Viet Nam

[Original : anglais]
[12 avril 2022]

Chapitre III. Mesures procédurales, détection et répression

8. Compétence

1. Tout État Membre prend les mesures nécessaires pour établir sa compétence aux fins de connaître des infractions visées aux articles [...] dans les cas suivants :

a) Quand l'infraction a été commise sur tout territoire sous la juridiction dudit État ou à bord d'aéronefs ou de navires immatriculés dans cet État ;

b) Lorsque l'auteur présumé de l'infraction a la nationalité dudit État ;

c) Quand la victime a la nationalité dudit État et que ce dernier le juge approprié.

2. La présente Convention n'exclut aucune compétence pénale exercée par un État conformément à son droit interne.

9. Pouvoirs des autorités compétentes

Les États Membres :

a) Prennent les mesures nécessaires pour prévenir et repérer les infractions pénales visées par la présente Convention, et mener des enquêtes, des poursuites et des procédures judiciaires les concernant ;

b) Recueillent des preuves relatives aux infractions visées par la présente Convention, notamment sous forme de données numériques, en veillant à protéger la souveraineté des autres États Membres.