Nations Unies A/AC.291/9/Add.1

Assemblée générale

Distr. générale
21 avril 2022
Français
Original : anglais/arabe/espagnol/
français/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.22-02330 (F) 270522 300522

Merci de recycler

Table des matières

III. Dispositions générales

Angola

[Original : anglais]
[8 avril 2022]

Dispositions générales

Définitions : cybercriminalité, preuve électronique, interception, système informatique, données informatiques, métadonnées, données relatives au trafic, fournisseurs de services, programme informatique, réseau de communications électroniques, infrastructure critique, topographie, produit à semi-conducteur, souveraineté numérique.

Afin d'élaborer les concepts proposés ici, on pourra se fonder sur les instruments juridiques régionaux et internationaux mentionnés ci-dessus[1].

Australie

[Original : anglais]
[13 avril 2022]

Les dispositions générales devraient inclure :

- Une déclaration d'intention clairement axée sur la lutte contre la cybercriminalité ;
- Un champ d'application ciblé et bien défini ;
- Des définitions convenues, dont l'examen et l'adoption ne devraient avoir lieu qu'une fois arrêtés les articles de fond de la convention.

La nature du cyberespace, par opposition à l'espace physique, ajoute des difficultés à l'application et à l'interprétation des règles et principes du droit international, notamment du principe de la souveraineté des États, et à l'application de la compétence territoriale. L'Australie propose de poursuivre les débats sur la manière d'aborder ces questions juridiques dans la convention parallèlement à l'élaboration des dispositions de fond.

Brésil

[Original : anglais]
[8 avril 2022]

Chapitre I
Dispositions générales

Article premier
Objet[2]

La présente Convention a pour objet de prévenir et de combattre la cybercriminalité, en établissant :

[1] Note du secrétariat : il s'agit des instruments mentionnés sous un autre intertitre, à savoir : la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, la Convention sur la cybercriminalité du Conseil de l'Europe, la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention des Nations Unies contre la corruption.

[2] *Source* : Proposition originale présentée par le Brésil.

a) Des actes que les Parties sanctionnent en tant qu'infractions sur leurs territoires respectifs ;

b) Des pouvoirs de procédure permettant aux autorités nationales d'agir dans les meilleurs délais ; et

c) Des mesures de coopération internationale.

Article 2
Champ d'application[3]

1. La présente Convention s'applique :

a) À la prévention, à la détection et à la perturbation de la cybercriminalité, ainsi qu'aux enquêtes, aux poursuites et aux jugements s'y rapportant ;

b) À l'application de mesures visant à atténuer les conséquences de la cybercriminalité ; et

c) À toute forme de coopération internationale destinée à prévenir et à combattre la cybercriminalité.

2. Aux fins de l'application de la présente Convention, les infractions ne doivent pas nécessairement occasionner de dommage matériel pour être incriminées, sauf disposition contraire.

Article 3
Terminologie[4]

Aux fins de la présente Convention :

a) Le terme « personne touchée » s'entend de toute personne, fournisseur de services ou autre entité qui a été touché, ou est susceptible de l'être, dans ce rôle, par l'octroi d'une décision ;

b) Le terme « données informatiques » s'entend de toute représentation de données ou d'informations qui ont été, ou peuvent être stockées, transmises ou traitées d'une autre manière dans un système informatique. Elles comprennent les données relatives aux abonnés, au trafic et au contenu ;

c) Le terme « système informatique » s'entend de tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme ou d'un autre logiciel, le stockage ou la transmission de données informatiques, ou leur traitement d'une autre manière ;

d) Le terme « données relatives au contenu » s'entend de toutes données informatiques stockées par un fournisseur de services ou de toutes autres informations autres que des données relatives au trafic ou aux abonnés, par exemple du texte, de la voix, des vidéos, des images et du son, ou le contenu d'une communication ayant purement trait à la communication ;

e) Le terme « réseau de communications électroniques » s'entend des systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, des équipements de commutation ou de routage et des autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes et mobiles,

---

[3] Proposition présentée par la Chine et la Fédération de Russie, moyennant des modifications apportées par le Brésil.

[4] Réunion du groupe d'experts chargé d'actualiser la Loi type de l'Office des Nations Unies contre la drogue et le crime sur l'entraide judiciaire en matière pénale (processus en cours au 9 mars 2022), moyennant des modifications mineures apportées par le Brésil.

les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, quel que soit le type d'information transmise ;

f) Le terme « preuve électronique » s'entend de toute donnée ou information créée, stockée, transmise ou traitée d'une autre manière sous forme électronique qui peut servir à prouver ou infirmer un fait dans le cadre d'une procédure judiciaire ;

g) Le terme « surveillance électronique » s'entend :

i) Du suivi, de l'interception, de la reproduction ou de la manipulation de messages, de données ou de signaux qui ont été stockés ou transmis, ou sont en cours de transmission, par des moyens électroniques ; ou

ii) Du suivi ou de l'enregistrement d'activités par des moyens électroniques ;

h) Le terme « fournisseur de services » s'entend :

i) De toute personne, ou entité publique ou privée, qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, ou facilite d'une autre manière la communication sur un réseau de communications électroniques ; ou

ii) De toute autre personne, ou entité publique ou privée, qui stocke ou traite d'une autre manière des données informatiques pour ce service ou ses utilisateurs ;

i) Le terme « données relatives aux abonnés » s'entend de toutes données informatiques collectées par un fournisseur de services dans le cadre de l'activité normale de l'entreprise concernant le nom, la date de naissance, l'adresse postale ou géographique, les données de facturation et de paiement, les identifiants des appareils, le numéro de téléphone ou l'adresse électronique, ou toute autre information, par exemple l'adresse de protocole Internet utilisée au moment de la création du compte, qui peuvent servir à identifier l'abonné ou le client ainsi que le type de service fourni et la durée du contrat conclu avec le fournisseur de services, autres que des données relatives au trafic ou au contenu ;

j) Le terme « données relatives au trafic » s'entend de toutes données informatiques collectées par un fournisseur de services dans le cadre de l'activité normale de l'entreprise relatives :

i) Au type de service fourni et à sa durée, en ce qui concerne les données techniques et les données identifiant les mesures techniques liées ou les interfaces utilisées par l'abonné ou le client ou qui lui sont fournies, et les données relatives à la validation de l'utilisation du service, à l'exclusion des mots de passe ou d'autres moyens d'authentification utilisés à la place d'un mot de passe, fournis par un utilisateur ou créés à la demande d'un utilisateur ; ou

ii) Au début et à la fin d'une session d'accès utilisateur à un service, telle que la date et l'heure d'utilisation, ou la connexion et la déconnexion du service ; ou

iii) Aux métadonnées de communications traitées dans un réseau de communications électroniques à des fins de transmission, de distribution ou d'échange de contenu de communications électroniques, y compris des données permettant de remonter jusqu'à la source et la destination d'une communication et de les identifier, des données relatives à l'emplacement de l'équipement terminal traitées dans le cadre de la fourniture de services de communications, ainsi que la date, l'heure, la durée et le type de communication.

Burundi

[Original : français]
[8 avril 2022]

Chapitre I. Définitions

Au sens de la présente Convention, on entend par :

Accès illicite. Accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un réseau de communication électronique, d'un système d'information ou d'un équipement terminal.

Chiffrement. Toute technique consistant à transformer les données numériques en un format inintelligible en employant des moyens de cryptologie.

Cryptologie. Science relative à la protection et à la sécurité des informations.

Cybercriminalité. Tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou de tout autre réseau physique connexe ou en relation avec un système d'information.

Cyberespace. Ensemble de données numérisées constituant un univers d'informations et un milieu de communication liés à l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

Cybersécurité. Ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs.

Communication électronique. Toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de vidéos par voie électromagnétique, optique ou par tout autre moyen.

Données à caractère personnel. Toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

Données informatiques. Désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

Électromagnétique. Résultat de la vibration couplée d'un champ électrique et d'un champ magnétique variable dans le temps.

Fournisseur de services. Personne physique ou morale qui fournit un ou plusieurs services aux utilisateurs d'un système de télécommunication.

Information. Tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique ou autre.

Infrastructure critique. Infrastructure qui est essentielle aux services vitaux pour la sureté publique, la stabilité économique, la sécurité nationale, la stabilité internationale et pour la pérennité et la restauration du cyberespace critique.

Les infrastructures critiques de l'État sont constituées par les services de santé publique, de sécurité intérieure et extérieure, de défense, de finance et de transport connectés aux réseaux Internet.

Interception illégale. Accès sans en avoir le droit ou l'autorisation aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal.

Gateway internationale. Nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple, un réseau local et le réseau Internet.

Moyen de paiement électronique. Moyen permettant à son titulaire d'effectuer des opérations de paiement électronique en ligne.

Phishing/fishing. Forme d'escroquerie par e-mail qui consiste à prendre l'identité d'une entreprise connue et reconnue sur un e-mail pour inciter les destinataires à changer ou mettre à jour leurs coordonnées bancaires sur des pages Internet imitant celles de l'entreprise dont l'image a été utilisée pour l'escroquerie.

Pornographie infantile. Toute représentation visuelle d'un comportement sexuellement explicite, y compris toute photographie, film, vidéo ou image, qu'elle soit fabriquée ou produite par voie électronique, mécanique ou par d'autre moyens où :

1) La production de telles représentations visuelles implique un mineur ;

2) Les représentations visuelles sont une image numérique, une image d'un ordinateur ou une image générée par un ordinateur où un mineur est engagé dans un comportement sexuellement explicite ou lorsque des images de leurs organes sexuels sont produites ou utilisées à des fins principalement sexuelles et exploitées à l'insu de l'enfant ou non ;

3) La représentation visuelle a été créée, adaptée ou modifiée pour qu'un mineur s'engage dans un comportement sexuellement explicite.

Prestataires de services. Opérateurs mobiles, fournisseurs d'accès Internet et opérateurs d'infrastructures.

Programme informatique. Ensemble d'instructions exécutées par l'ordinateur pour obtenir les résultats escomptés.

Racisme et xénophobie en matière de TIC. Tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconisent ou encouragent la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion.

Spamming. Envoi généralement massif et non ciblé de messages commerciaux par e-mail avec l'intention de voler, à des individus n'ayant pas donné leur autorisation à l'émetteur pour la réception de tels messages.

Système informatique. Tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

TIC. Technologies de l'information et de la communication.

Canada[5]

[Original : anglais]
[9 avril 2022]

Dispositions générales

Objet

La présente Convention a pour objet de promouvoir la coopération de façon à améliorer l'efficacité de la prévention, des enquêtes et des poursuites en matière de cybercriminalité.

[5] Note du Secrétariat : le Canada a également communiqué une liste de définitions, disponible (en anglais) à l'adresse www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

Champ d'application

La présente Convention s'applique, sauf indication contraire et sous réserve de mesures de sauvegarde appropriées, aux fins suivantes :

a) Promouvoir et renforcer les mesures législatives et autres relatives à la prévention, aux enquêtes et aux poursuites concernant la cybercriminalité et les infractions graves fréquemment commises au moyen de systèmes informatiques établies par la présente Convention ;

b) Promouvoir, faciliter et appuyer la coopération et l'assistance internationales relatives à la prévention, aux enquêtes et aux poursuites concernant les infractions établies par la présente Convention ;

c) Promouvoir, faciliter et appuyer une entraide judiciaire efficiente et efficace concernant les preuves électroniques relatives aux infractions établies par la présente Convention et à toutes autres infractions pénales ; et

d) Promouvoir, faciliter et appuyer la fourniture d'une assistance technique en matière de prévention de la cybercriminalité et de lutte contre ce phénomène.

Conditions et mesures de sauvegarde

1. Chaque État partie veille à ce que l'instauration, la mise en œuvre et l'application des dispositions de la présente Convention soient soumises aux conditions et mesures de sauvegarde prévues par son droit interne, qui doit assurer la protection pleine et entière des droits humains et des libertés, en particulier des droits établis conformément aux obligations découlant du Pacte international relatif aux droits civils et politiques ou d'autres instruments internationaux applicables concernant les droits humains, et qui doit intégrer les principes de l'état de droit, de la légalité, de la nécessité et de la proportionnalité.

2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et mesures de sauvegarde 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. Chaque État partie applique des mesures destinées à permettre de mieux cerner les liens existant entre le genre et la cybercriminalité, notamment les incidences différenciées que peut avoir ce phénomène sur les femmes et les hommes. Ces mesures visent à promouvoir l'égalité des genres et l'autonomisation des femmes, notamment en intégrant ces éléments, dès que cela est pertinent, dans la législation, l'élaboration des politiques, la recherche, les projets et les programmes, selon qu'il convient et conformément aux principes fondamentaux du droit interne.

4. Les mesures énoncées dans la présente Convention ne doivent pas être interprétées et appliquées de manière à porter atteinte à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, sous forme orale, écrite, imprimée ou artistique, ou par tout autre moyen choisi à cette fin, ainsi que les droits applicables concernant le respect de la vie privée et la protection des données. L'interprétation et l'application de ces mesures doivent être conformes aux principes de non-discrimination internationalement reconnus.

Participation et tentative

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, conformément à son droit interne, au fait de participer à quelque titre que ce soit, par exemple comme complice, autre assistant ou instigateur, à une infraction établie conformément à la présente Convention.

2. Chaque État partie peut adopter les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, conformément à son droit interne, au fait de tenter de commettre une infraction établie conformément à la présente Convention.

3. Chaque État partie peut adopter les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, conformément à son droit interne, au fait de préparer une infraction établie conformément à la présente Convention.

Responsabilité des personnes morales

1. Chaque État partie adopte les mesures législatives et autres nécessaires, conformément à ses principes juridiques, pour établir la responsabilité des personnes morales qui participent à la commission des infractions établies par la présente Convention.

2. Sous réserve des principes juridiques de l'État partie, la responsabilité des personnes morales peut être pénale, civile ou administrative.

3. Cette responsabilité est sans préjudice de la responsabilité pénale des personnes physiques qui ont commis les infractions.

4. Chaque État partie veille, en particulier, à ce que les personnes morales tenues responsables conformément au présent article fassent l'objet de sanctions efficaces, proportionnées et dissuasives de nature pénale ou non pénale, y compris de sanctions pécuniaires.

Colombie

[Original : espagnol]
[9 avril 2022]

Dispositions générales

Les États parties s'attachent à prévenir et à combattre la cybercriminalité sous tous ses aspects en favorisant et en assurant le plein respect des droits des femmes et des filles, tout en accordant une attention spéciale aux questions de genre, en particulier à la violence fondée sur le genre, et notamment à la violence contre les femmes et les filles.

Les États parties s'attachent à prévenir et à combattre la cybercriminalité sous toutes ses manifestations en favorisant et en assurant le respect des droits humains et des libertés fondamentales. Toutes les dispositions de la présente Convention ou du présent instrument doivent être interprétées et appliquées conformément aux obligations internationales applicables en matière de droits humains.

Définitions

Conformément au consensus établi lors de la première phase de négociations quant à la nécessité de convenir de termes et de définitions technologiquement neutres, et à la lumière des observations formulées par l'équipe du Conseil de l'Europe pour la Convention de Budapest, les définitions énoncées dans ladite convention et son deuxième protocole sont pertinentes et suffisantes et susceptibles d'adaptation aux évolutions technologiques, et peuvent donc être proposées au Comité spécial.

En conséquence, les définitions proposées s'énoncent comme suit :

a) Système informatique : « tout dispositif isolé ou ensemble de dispositifs interconnectés […], qui assure […], en exécution d'un programme, un traitement automatisé de données » ;

b) Données informatiques : « toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction » ;

c) Fournisseur de services : « toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs » ;

d) Données relatives au trafic : « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent » ;

e) Autorité centrale : « autorité ou groupe d'autorités désignées en vertu d'un traité d'entraide ou d'un arrangement reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées, ou, à défaut, autorité ou groupe d'autorités désignées par une Partie [...] chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution » ;

f) Autorité compétente : « autorité judiciaire, administrative ou autre autorité chargée de l'application de la loi habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution de mesures [...] aux fins du recueil ou de la production de preuves concernant des enquêtes ou procédures pénales spécifiques » ;

g) Urgence : « situation présentant un risque grave et imminent pour la vie ou la sécurité d'une personne physique » ;

h) Données à caractère personnel : « informations relatives à une personne physique identifiée ou identifiable » ;

i) Partie transférante : « Partie qui transmet les données en réponse à une demande ou dans le cadre d'une équipe d'enquête commune, ou [...] Partie sur le territoire de laquelle se trouve un prestataire de services en mesure de transmettre ou une entité fournissant des services d'enregistrement de noms de domaine » ;

j) Données relatives aux abonnés : « toute information [...] 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 : [...] le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service [...], l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné [...], les données concernant la facturation et le paiement [...] et toute autre information relative à l'endroit où se trouvent les équipements de communication ».

Égypte

[Original: arabe]
[8 avril 2022]

Chapitre premier. Dispositions générales

Il est proposé que ce chapitre couvre l'objet de la Convention, les termes utilisés, la protection de la souveraineté et le champ d'application, comme indiqué ci-après :

Article premier : Objet

La présente Convention a pour objet de renforcer la coopération entre les États Membres de l'Organisation des Nations Unies en matière de lutte contre l'utilisation

des technologies de l'information et des communications à des fins criminelles. Elle vise à réprimer les actes de nature à menacer l'intégrité et la confidentialité des technologies de l'information et des communications, à incriminer l'utilisation abusive des technologies de l'information et des communications à des fins illégales, à faciliter les enquêtes et les poursuites visant les auteurs des actes concernés, et à mettre en œuvre des mesures destinées à éliminer les conséquences de ces infractions. Ces mesures comprennent la suspension des transactions portant sur des actifs obtenus par la commission d'un acte illégal visé par la présente Convention, et la confiscation et la restitution du produit de ces actifs. À cette fin, la présente Convention prévoit des pouvoirs suffisants pour lutter efficacement contre les infractions liées aux technologies de l'information et des communications, en établissant des accords de coopération internationale destinés à faciliter la détection de ces infractions et la conduite d'enquêtes s'y rapportant, la poursuite de leurs auteurs et l'extradition des délinquants.

Article 2 : Terminologie

Dans la présente Convention, les termes suivants sont employés avec le sens indiqué ci-après :

a) Technologie de l'information : tout moyen physique ou non corporel, ou groupe de moyens interconnectés ou non connectés, servant à stocker, classer, organiser, récupérer, traiter, élaborer et échanger des informations conformément aux ordres et instructions qui y sont stockés, y compris les données d'entrée et de sortie qui y sont associées, par voie filaire ou non filaire, au sein d'un système ou d'un réseau ;

b) Fournisseur de services : toute personne physique ou morale, publique ou privée, qui fournit à des abonnés des services leur permettant de communiquer à l'aide de technologies de l'information ou qui traite ou stocke des informations pour un service de communication ou ses utilisateurs ;

c) Données : toutes informations susceptibles d'être stockées, traitées, créées et transmises par des technologies de l'information, telles que des chiffres, lettres, symboles et autres éléments analogues ;

d) Système d'information : ensemble de programmes et d'outils destinés à traiter et à gérer des données et des informations ;

e) Réseau d'information : ensemble de deux systèmes d'information ou plus reliés entre eux aux fins de l'obtention ou de l'échange d'informations ;

f) Site : endroit où des informations sont mises à disposition sur un réseau d'information au moyen d'une adresse spécifique ;

g) Captage : visualisation ou obtention de données ou d'informations ;

h) Administrateur de site : personne chargée d'organiser, de gérer, de contrôler ou de tenir un ou plusieurs sites sur un réseau d'information, y compris les droits d'accès des différents utilisateurs du site, la conception du site, la création et l'organisation des pages ou du contenu du site, ou le site lui-même ;

i) Compte privé : ensemble d'informations relatives à une personne physique ou morale qui octroie à celle-ci le droit exclusif d'accéder aux services disponibles sur un site ou un système d'information, ou d'utiliser ces services ;

j) Courriel : moyen d'échange de messages électroniques à une adresse spécifique entre plus d'une personne physique ou morale par l'intermédiaire d'un réseau d'information ou d'un autre moyen électronique d'interconnexion, ordinateurs et appareils analogues ;

k) Interception : visualisation ou obtention de données ou d'informations pour les consulter secrètement, les désactiver, les stocker, les reproduire, les enregistrer, en modifier le contenu, en faire une utilisation abusive, les réacheminer ou les rediriger à des fins illégales ;

l) Pénétration : accès à un système d'information, à un ordinateur, à un réseau d'information ou à un dispositif analogue, sans autorisation, ou en violation des dispositions de la licence applicable, ou de manière illégale ;

m) Contenu : toutes données qui, par elles-mêmes ou associées à d'autres données ou informations, permettent de créer des informations ou d'identifier une tendance, une direction, un concept ou une signification, ou une référence à d'autres données ;

n) Preuve numérique : toute information électronique ayant force probante stockée sur un ordinateur, un réseau d'information ou un dispositif analogue ou transmise par son moyen, dont elle est extraite ou à partir duquel elle est obtenue, et pouvant être recueillie et analysée à l'aide de dispositifs technologiques, applications ou logiciels spéciaux ;

o) Trafic (données relatives au trafic) : données produites par un système d'information indiquant l'origine, la destination, l'expéditeur, le destinataire, l'itinéraire, l'heure, la date, la taille et la durée d'une communication ainsi que le type de service utilisé.

Article 3 : Protection de la souveraineté

1. Les États parties s'acquittent des obligations découlant de la présente Convention dans le respect de leur droit interne ou de leurs principes constitutionnels, de manière conforme aux principes de l'égalité souveraine des États et de la non-ingérence dans les affaires intérieures d'autres États.

2. La présente Convention ne permet pas à un État partie d'exercer, sur le territoire d'un autre État, une compétence et des fonctions qui sont du ressort exclusif des autorités de cet autre État en vertu de son droit interne.

Article 4. : Champ d'application.

1. Sauf disposition contraire, la présente Convention s'applique à la répression des infractions qui y sont prévues.

2. Aux fins de l'application de la présente Convention, les infractions ou autres actes illégaux qui y sont prévus ne doivent pas nécessairement occasionner de dommage matériel pour être incriminés, sauf disposition contraire.

3. Chaque État partie envisage de limiter ses réserves afin de permettre une large application des mesures susmentionnées.

El Salvador

[Original : espagnol]
[12 avril 2022]

Terminologie

De l'avis de notre gouvernement, il existe un certain nombre de définitions existantes qui devraient être incorporées dans le document, et ces définitions devraient être formulées de telle sorte que les traductions dans les six langues officielles de l'Organisation des Nations Unies transmettent les concepts corrects sans qu'il y ait le moindre doute quant au concept auquel il est fait référence. En conséquence, il est proposé que le Comité spécial examine les définitions déjà établies dans les instruments que les États Membres connaissent bien, tels que la Convention de Budapest et la Convention des Nations Unies contre la criminalité transnationale organisée, comme point de départ pour la rédaction des définitions.

En particulier, nous pensons que les définitions des expressions suivants devraient être ajoutées :

a) L'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure, ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;

b) L'expression « données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une action ;

c) L'expression « fournisseur de services » désigne toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;

d) L'expression « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Il convient d'ajouter une définition de l'expression « matériel à contenu pornographique mettant en scène des enfants » plutôt que de l'expression « pornographie mettant en scène des enfant », les mots clefs étant la production, la reproduction, la distribution, la publication, l'importation, l'exportation, l'offre, le financement, la vente, la commercialisation, la diffusion et la possession d'un tel contenu, et cette définition devrait inclure la participation d'une personne qui apparaît comme un mineur dans des actes sexuellement explicites ou des images réalistes d'un mineur participant à des actes sexuellement explicites ; elle devrait également viser non seulement la représentation d'enfants dans des actes sexuellement explicites, mais aussi les actes qui montrent des enfants et des adolescents nus.

Union européenne et ses États membres

[Original : anglais]
[6 avril 2022]

Chapitre premier. Dispositions générales

Article premier
Objet

Tout en garantissant un niveau élevé de protection des droits humains et des libertés fondamentales, la présente Convention a pour objet :

a) De promouvoir et renforcer les mesures visant à prévenir et combattre la cybercriminalité de manière plus efficace ;

b) De promouvoir et de faciliter la coopération internationale ;

c) De garantir un niveau élevé de protection des droits des victimes ; et

d) De soutenir le renforcement des capacités et l'assistance technique dans la lutte contre la cybercriminalité.

Article 2
Terminologie

Aux fins de la présente Convention :

a) L'expression « autorité centrale » désigne l'autorité ou plusieurs autorités chargées d'envoyer les demandes d'entraide judiciaire ou d'y répondre, de les exécuter ou de les transmettre aux autorités chargées de les exécuter ;

b) L'expression « cybercriminalité » désigne, aux fins de la présente Convention, les comportements tels que définis aux articles 5 à 10 de la présente Convention ;

c) L'expression « autorité compétente » désigne une autorité judiciaire, administrative ou autre autorité chargée de l'application de la loi habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution de mesures visées par la présente Convention concernant des enquêtes ou procédures pénales spécifiques ;

d) L'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;

e) L'expression « données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

f) L'expression « données à caractère personnel » désigne les informations relatives à une personne physique identifiée ou identifiable ;

g) L'expression « organisation régionale d'intégration économique » désigne toute organisation constituée par des États souverains d'une région donnée, à laquelle ses États membres ont transféré des compétences en ce qui concerne les questions régies par la présente Convention et qui a été dûment mandatée, conformément à ses procédures internes, pour signer, ratifier, accepter, approuver ladite Convention ou y adhérer; les références dans la présente Convention aux « États parties » sont applicables à ces organisations dans la limite de leur compétence ;

h) L'expression « fournisseur de services » désigne :

i) Toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ; et

ii) Toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;

i) L'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que les données relatives au trafic ou au contenu, et permettant d'établir :

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

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

iii) Toute autre information relative aux équipements de communication et à l'endroit où ils se trouvent, disponible sur la base d'un contrat ou d'un arrangement de services ;

j) L'expression « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;

k) L'expression « sans droit » désigne un comportement visé aux articles 5 à 10 de la présente Convention qui n'est pas autorisé par le propriétaire ou par un autre titulaire des droits sur le système informatique ou sur une partie de celui-ci, ou qui n'est pas autorisé en vertu du droit interne.

Article 3
Champ d'application

La présente Convention s'applique, sauf disposition contraire, à :

a) La prévention, l'instruction et la poursuite d'infractions pénales établies conformément aux articles 5 à 10 de la présente Convention ;

b) La collecte de preuves électroniques d'une infraction pénale établie conformément aux articles 5 à 10 de la présente Convention sur la base des mesures énoncées au chapitre III de la présente Convention ;

c) La fourniture d'une assistance technique et d'un appui pour le renforcement des capacités dans les domaines visés par la présente Convention.

Article 4
Effets de la Convention

1. Si deux ou plusieurs États parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les États parties établiront leurs futures relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

2. En ce qui concerne les États parties qui sont membres d'une organisation d'intégration économique régionale, ces États parties peuvent, dans leurs relations mutuelles, appliquer les règles de cette organisation d'intégration économique régionale régissant les questions traitées dans la présente Convention.

3. Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie en vertu du droit international, en particulier du droit des droits humains.

Ghana

[Original : anglais]
[12 avril 2022]

Chapitre I
Dispositions générales

Article premier
Objet

L'objet de la présente Convention est de promouvoir et de faciliter la coopération internationale ainsi que de renforcer les mesures visant à prévenir et à combattre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Article 2
Terminologie

Aux fins de la présente Convention :

a) L'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;

b) L'expression « données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

c) L'expression « données relatives au contenu » désigne le contenu informatif de la communication, c'est-à-dire le sens de la communication, ou le message ou l'information véhiculés par la communication autre que les données relatives au trafic ;

d) Le terme « enfant » désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans ;

e) L'expression « infrastructures d'information critiques » désigne un ordinateur ou un système informatique identifié par un État Membre dans sa législation nationale comme étant essentiel pour la sécurité nationale ou le bien-être économique et social des citoyens ;

f) L'expression « images intimes et enregistrements visuels interdits » comprend :

i) Une image animée ou fixe qui représente :

a. La personne qui s'est livrée à une activité sexuelle intime qui ne se fait pas habituellement en public ; ou

b. La région génitale ou anale d'une personne, lorsque la région génitale ou anale est nue ou recouverte seulement par des sous-vêtements ; et

ii) Une image qui a été modifiée de manière à donner l'impression de montrer l'une des choses mentionnées au paragraphe i), même si la chose a été obscurcie numériquement, si la personne est représentée d'une manière sexuelle ;

g) L’expression « fournisseur de services » désigne :

i) Toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d’un système informatique ; et

ii) Toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;

h) Le terme « abonné » désigne un client ou un utilisateur d’un réseau de communications électroniques, d’un service de communications électroniques ou d’un service de radiodiffusion ;

i) L’expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que les données relatives au trafic ou au contenu, et permettant d’établir :

i) Le type de service de communication utilisé, la disposition technique prise à cet égard et la période de service ;

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

iii) 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 ;

j) L’expression « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu’élément de la chaîne de communication, indiquant l’origine, la destination, l’itinéraire, l’heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Article 3
Champ d’application

La présente Convention s’applique, conformément à ses dispositions, à :

a) La prévention, l’instruction et la poursuite d’infractions établies conformément à ses articles 5 à 20 ;

b) La collecte des preuves électroniques de toute infraction pénale ;

c) La fourniture d’une assistance technique et d’un appui pour le renforcement des capacités dans les domaines visés par la présente Convention ;

d) Le gel, la saisie, la confiscation et la restitution du produit d’infractions établies conformément à la présente Convention.

Article 4
Protection de la souveraineté

1. Les États Membres exécutent leurs obligations au titre de la présente Convention d’une manière compatible avec les principes de l’égalité souveraine et de l’intégrité territoriale des États et avec celui de la non-intervention dans les affaires intérieures d’autres États.

2. Aucune disposition de la présente Convention n’habilite un État Membre à exercer sur le territoire d’un autre État une compétence et des fonctions qui sont exclusivement réservées aux autorités de cet autre État par son droit interne.

Iran (République islamique d')

[Original : anglais]
8 avril 2022

1. Dispositions générales

Alors que les technologies de l'information et des communications offrent des possibilités exceptionnelles pour le développement des nations, les délinquants les utilisent de plus en plus souvent pour mener des activités illicites et réaliser des objectifs illégitimes. Les modes opératoires de ces délinquants sont de plus en plus diversifiés et sophistiqués et les multiples facettes de ces infractions évoluent considérablement. Les infractions commises au moyen de technologies de l'information et des communications transcendent souvent les frontières géographiques, constituant ainsi un défi sans précédent que les États Membres doivent relever d'urgence. À ce titre, une réponse collective renforcée et une coopération au niveau international dans un cadre juridique international solide sont plus que nécessaires.

Conformément à la résolution 74/247 de l'Assemblée générale, la raison d'être de la création du Comité spécial était de répondre à ce besoin urgent et d'élaborer un instrument juridique international à l'appui de mesures efficaces prises à différents niveaux pour lutter contre l'utilisation des technologies de l'information et des communications à des fins criminelles. À cet effet, les dispositions générales de la convention doivent énoncer les objectifs de la convention et en définir le champ d'application. Le respect des principes fondamentaux du droit international étant une pratique établie qui revêt une importance essentielle pour prévenir et combattre les infractions commises au moyen de technologies de l'information et des communications, une partie substantielle des dispositions générales devrait également être consacrée à ces principes. Définir les termes utilisés dans chaque partie de la convention est essentiel pour favoriser une interprétation commune des termes importants et, in fine, des dispositions de la convention.

1.1. Objectifs de la convention

Compte tenu de ce qui précède, la République islamique d'Iran souligne que la convention devrait avoir pour objet de consolider, de soutenir et de faciliter la coopération internationale visant à prévenir et à combattre l'utilisation des technologies de l'information et des communications à des fins criminelles, y compris pour le recouvrement d'avoirs, de renforcer les réponses nationales à ces infractions et d'aider les États parties, en particulier les pays en développement, à lutter contre ces infractions, notamment grâce au développement économique, à la fourniture d'une assistance technique et au transfert de technologie. À cet égard, une réponse technique devrait être apportée aux défis et aux obstacles, tels que les sanctions unilatérales et le sous-développement, qui compromettent la capacité des États de lutter efficacement contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Il convient également de tenir dûment compte de la responsabilité des fournisseurs de services et autres entités analogues en matière de coopération avec les autorités judiciaires et les services de détection et de répression, afin de garantir l'efficacité des mesures visant à prévenir et à combattre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Si une compréhension commune de cette criminalité et de l'évolution de ses formes est de la plus haute importance pour répondre efficacement aux infractions commises au moyen de technologies de l'information et des communications, la convention devrait également promouvoir et faciliter l'échange d'informations, de compétences techniques, de connaissances spécialisées, d'expériences et de bonnes pratiques.

Il sera possible d'atteindre ces objectifs en adoptant une stratégie qui privilégie un avenir commun dans le cyberespace pour tous les États Membres, fondé sur l'égalité des chances et la non-discrimination.

1.2. Champ d'application de la convention

La convention devrait couvrir les infractions qui dépendent des technologies de l'information et des communications, telles que les atteintes à la confidentialité et à l'intégrité des systèmes et données et les infractions commises contre l'infrastructure des technologies de l'information et des communications, ainsi que les infractions qui sont facilitées par ces technologies, par exemple, les insultes aux valeurs religieuses, l'incitation à la violence, l'incitation à commettre un homicide, la diffusion de contenus illicites et obscènes et l'exploitation sexuelle des enfants. Néanmoins, les infractions facilitées par les technologies de l'information et des communications peuvent requérir une approche au cas par cas qui tienne compte des différents facteurs entourant les diverses formes d'infractions et des éventuelles différences entre leurs éléments constitutifs. Dans certains cas, d'autres éléments peuvent également être nécessaires pour définir le champ d'application de la convention en fonction de la gravité des infractions ou en fonction des sanctions dont celles-ci sont assorties et selon que les infractions en question ont été perpétrées dans plus d'un État ou non.

1.3. Protection de la souveraineté

La République islamique d'Iran réaffirme que des dispositions visant expressément la protection de la souveraineté devraient être incluses dans les dispositions générales afin de garantir que les efforts et les mesures visant à prévenir et à combattre l'utilisation des technologies de l'information et des communications à des fins criminelles soient cohérents et conformes aux principes fondamentaux du droit international et aux principes énoncés dans la Charte des Nations Unies, en particulier l'égalité souveraine, l'intégrité territoriale des États et la non-ingérence. Il s'agit d'une pratique établie en matière d'élaboration de conventions visant à prévenir et à combattre la criminalité ; à titre d'exemple, le terme « protection de la souveraineté » a été utilisé dans des conventions telles que la Convention des Nations Unies contre la corruption.

La République islamique d'Iran reste circonspecte concernant les tentatives qui vont à l'encontre de cette pratique établie de la communauté internationale et qui visent à nier et à ignorer le rôle essentiel du respect de ces principes dans la lutte contre la criminalité.

Japon

[Original : anglais]
8 avril 2022

2. Dispositions générales

2.1. Objet

Nous sommes favorables aux trois objectifs décrits dans la proposition faite par la Présidente au cours de la première session du Comité spécial : a) promouvoir et renforcer les mesures visant à prévenir et à combattre la cybercriminalité ; b) promouvoir, faciliter et renforcer la coopération internationale ; et c) fournir des outils pratiques pour améliorer l'assistance technique et renforcer les capacités des autorités nationales.

2.2. Terminologie

Dans l'optique d'établir une convention effectivement applicable dans la durée, les termes utilisés dans cette convention doivent être clairement définis d'une façon

technologiquement neutre. Par exemple, il serait inapproprié d'arrêter des définitions pour des technologies en constante évolution, comme le « botnet ».

Il convient donc d'établir les définitions nécessaires de la manière la plus générale et claire possible, tout en se référant aux instruments internationaux existants tels que la Convention des Nations Unies contre la criminalité transnationale organisée. Nous estimons que ce point de vue s'applique également aux débats sur d'autres parties de la convention, telles que les dispositions sur l'incrimination.

2.3. Champ d'application

2.3.1. Le champ d'application de la convention doit être clairement énoncé, sur le modèle des dispositions de la Convention des Nations Unies contre la criminalité transnationale organisée et de la Convention des Nations Unies contre la corruption.

2.3.2. La cybersécurité et la gouvernance d'Internet ne devraient pas être abordées dans la convention. Par exemple, les mesures suivantes auraient un effet dissuasif sur les activités économiques légitimes, elles entraveraient le développement de la technologie et iraient au-delà du mandat du Comité spécial :

- Fixer des normes de sécurité dans le cadre de la convention ;
- Imposer aux personnes morales et aux particuliers l'obligation de se conformer à ces normes ou imposer des sanctions en cas de violation de ces normes ; ou
- Tenir pour responsables les personnes morales, leurs représentants ou les créateurs de logiciels qui participent involontairement à des actes de cybercriminalité commis par d'autres acteurs sans en avoir conscience.

Mexique

[Original : anglais]
[13 avril 2022]

Dispositions générales

Afin d'éviter d'éventuelles omissions et de prévenir le non-respect de l'application d'autres instruments juridiquement contraignants à venir, et conformément aux traités internationaux et régionaux antérieurs, le Mexique appuie l'inclusion de références générales tenant lieu de dispositions initiales, plutôt que de dispositions exhaustives et très détaillées.

En ce qui concerne la souveraineté, suivant l'exemple de la Convention-cadre des Nations Unies sur les changements climatiques, le Mexique recommande d'inclure dès le préambule une référence générale pour réaffirmer la souveraineté, comme suit : « Réaffirmant que le principe de la souveraineté des États doit présider à la coopération internationale destinée à lutter contre l'utilisation des technologies de l'information et des communications à des fins criminelles ».

Le Mexique recommande aussi d'inclure dans le préambule un alinéa réaffirmant la Charte des Nations Unies, l'applicabilité du droit international, la Déclaration universelle des droits de l'homme et d'autres obligations internationales relatives aux droits humains, comme suit : « Réaffirmant les buts et principes énoncés dans la Charte des Nations Unies, le droit international, la Déclaration universelle des droits de l'homme et d'autres instruments pertinents relatifs aux droits humains ».

Il est également recommandé d'inclure une disposition générale sur l'importance, pour les États, de prendre des mesures appropriées pour protéger les personnes, en particulier les groupes vulnérables : « A décidé de prendre des mesures destinées à favoriser la prévention, les interventions, l'atténuation, les enquêtes et les poursuites visant à protéger efficacement les personnes, en particulier les groupes

vulnérables, de l'utilisation des technologies de l'information et des communications à des fins criminelles ».

Comme indiqué dans la recommandation ci-dessus, il est essentiel, pour le Gouvernement mexicain, d'inclure dans la convention des mesures destinées à favoriser la prévention, les interventions, l'atténuation, les enquêtes et les poursuites.

Lors du processus de négociation de la convention, il importera de reconnaître la pertinence des instruments internationaux juridiquement contraignants antérieurs, en particulier la Convention des Nations Unies contre la criminalité transnationale organisée, en partageant des expériences concrètes qui pourraient aider à améliorer l'efficacité de la coopération internationale en matière de lutte contre la cybercriminalité. Il faut en outre prévoir une disposition générale visant à promouvoir la cohérence de l'action du système des Nations Unies.

Le Mexique recommande en outre d'inclure également dans le préambule une reconnaissance explicite des possibilités et des avantages qu'offrent les technologies de l'information et des communications, afin d'indiquer clairement qu'elles ne sont pas intrinsèquement liées à la criminalité et utilisées uniquement à des fins illicites : « Reconnaissant que les technologies de l'information et des télécommunications offrent des possibilités de favoriser le développement, de remédier aux inégalités et de promouvoir l'inclusion, le bien-être, la justice et l'exercice des droits humains, et reconnaissant qu'il importe de promouvoir l'accès universel à ces technologies et de protéger les avantages qu'elles offrent ».

De plus, le Mexique souhaite éviter l'écueil d'un recours excessif à des garanties, qui pourrait alors devenir une contrainte, contraire à l'esprit de coopération internationale qui devrait être le moteur de ce processus.

« L'objet de la présente Convention est de promouvoir la coopération bilatérale et multilatérale et l'entraide judiciaire, notamment la coopération multisectorielle, en vue de favoriser la prévention, les interventions, l'atténuation, les enquêtes et les poursuites eu égard à l'utilisation des technologies de l'information et des communications à des fins criminelles ».

Le Mexique considère que d'autres dispositions générales doivent être ajoutées sur les points suivants : définir des procédures de règlement des conflits ; créer un mécanisme d'examen de l'application ; garantir la participation et la collaboration des autres parties prenantes concernées pour soutenir les efforts menés par les États parties pour prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles ; reconnaître la nature publique d'Internet et la pertinence du principe de neutralité d'Internet aux fins de la Convention.

Nouvelle-Zélande

[Original : anglais]
[8 avril 2022]

Dispositions générales

8. De notre point de vue, les dispositions générales devraient être les suivantes :

- *Objet.* Le meilleur moyen d'élaborer un traité efficace est d'adopter une approche cohérente, réaliste et ciblée pour définir nos objectifs. Pour la Nouvelle-Zélande, l'objectif devrait être d'établir un cadre mondial harmonisé, moderne et efficace de coopération et de coordination entre les États pour qu'ils s'attaquent à la menace croissante que la cybercriminalité représente pour les particuliers, les entreprises et les gouvernements. Il s'agit notamment de fournir un soutien et une assistance technique afin que tous les États puissent acquérir les capacités et les moyens de faire face à ces problèmes.

- *Champ d'application*. Le champ d'application devrait être lui-aussi ciblé et clairement défini. La proposition de la Présidente figurant dans le document de séance A/AC.291/CRP.8/Rev.1 constitue un bon point de départ pour déterminer le champ d'application de la convention.
- *Définitions convenues.* Les définitions doivent être précises, univoques, adaptées aux évolutions futures et, dans la mesure du possible, fondées sur les instruments internationaux et régionaux pertinents existants.
- Un instrument complet doit aussi inclure une disposition générale qui rappelle l'importance de la protection des droits humains et des libertés fondamentales et du respect de l'état de droit, compte tenu en particulier des perspectives des femmes, des enfants, des peuples autochtones et des groupes vulnérables.

9. Un certain nombre d'États ont indiqué qu'il était important pour eux d'inclure une disposition sur la souveraineté des États. Nous souhaitons faire observer que l'application d'une telle disposition dans le cadre de la présente convention doit tenir compte de plusieurs caractéristiques qui distinguent le cyberespace du monde matériel, en particulier : a) le cyberespace comporte un élément virtuel qui n'a pas de lien territorial clair ; et b) les activités menées dans le cyberespace peuvent s'appuyer sur des cyberinfrastructures fonctionnant simultanément dans plusieurs territoires et pays disparates.

Annexe II
Définitions

L'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure, ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

L'expression « données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

L'expression « contenus montrant l'exploitation sexuelle d'enfants » désigne tout contenu, y compris sous forme d'images, de vidéos et de flux en direct, représentant un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation d'un enfant à des fins principalement sexuelles.

Le terme « biens » désigne tous les types d'avoirs, y compris les actifs numériques, corporels ou incorporels, meubles ou immeubles, tangibles ou intangibles, ainsi que les actes juridiques ou documents attestant la propriété de ces avoirs ou les droits y relatifs

Norvège

[Original : anglais]
[8 avril 2022]

Dispositions générales

1. La convention devrait inclure des dispositions fortes de protection des droits humains et des libertés fondamentales, notamment le droit à la vie privée et la protection des données personnelles. Nous devons garantir la pleine compatibilité d'une future convention des Nations Unies sur la cybercriminalité avec les obligations au regard du droit international.

2. Pour être efficace, cet instrument doit fournir les garanties nécessaires, y compris en matière de proportionnalité, de légalité et de nécessité des mesures de détection et de répression.

3. L'accent devrait être mis sur la coopération internationale aux fins de la prévention et de la lutte contre la cybercriminalité.

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

[Original : russe]
[7 avril 2022]

Chapitre premier. Dispositions générales

Article premier : Objets

La présente Convention a pour objets :

a) De promouvoir et de renforcer les mesures visant à prévenir et à combattre de manière effective les infractions et autres actes illégaux liés à l'utilisation des technologies de l'information et des communications ;

b) D'empêcher les atteintes à la confidentialité, à l'intégrité et à la disponibilité des technologies de l'information et des communications, ainsi que l'usage illégal de ces technologies, en incriminant les actes visés dans la présente Convention, en donnant des pouvoirs suffisants pour qu'il soit possible de lutter efficacement contre ces actes, en facilitant la détection et les enquêtes et poursuites auxquels ils donnent lieu aux niveaux national et international, et en mettant au point des dispositifs de coopération internationale ;

c) D'améliorer l'efficacité de la coopération internationale et de développer celle-ci, notamment au moyen de la formation et de la prestation d'une assistance technique dans le but de prévenir et de combattre les infractions liées aux technologies de l'information et des communications.

Article 2 : Champ d'application

1. La présente Convention s'applique, conformément à ses dispositions, à la prévention, à la détection et à la répression des actes incriminés en application de ses articles 6 à 29, aux enquêtes et aux poursuites auxquels ils donnent lieu, ainsi qu'à la mise en œuvre de mesures visant à éliminer les conséquences de tels actes, notamment la suspension des opérations concernant des avoirs obtenus au moyen de la perpétration de tout acte incriminé en application de la présente Convention, et la saisie, la confiscation et la restitution du produit de telles infractions.

2. Aux fins de l'application de la présente Convention, les actes visés ne doivent pas nécessairement occasionner de préjudice important pour être incriminés, sauf disposition contraire.

Article 3 : Protection de la souveraineté

1. Les États parties s'acquittent des obligations découlant de la présente Convention dans le respect des principes de la souveraineté des États, de l'égalité souveraine des États et de la non-ingérence dans les affaires intérieures d'autres États.

2. Sauf disposition contraire, la présente Convention n'habilite les autorités compétentes d'aucun État partie à exercer sur le territoire d'un autre État partie une compétence ou des fonctions qui sont exclusivement réservées aux autorités de cet autre État par son droit interne.

Article 4 : Terminologie et définitions

Aux fins de la présente Convention :

a) On entend par « saisie de biens » l'interdiction temporaire du transfert, de la conversion, de la disposition ou du mouvement de biens, ou le fait d'assumer

temporairement le contrôle de biens sur décision d'un tribunal ou d'une autre autorité compétente ;

b) On entend par « botnet » deux appareils électroniques ou plus sur lesquels un logiciel malveillant a été installé et qui sont contrôlés de manière centralisée à l'insu des utilisateurs ;

c) On entend par « logiciel malveillant » un logiciel dont l'objet est la modification, la destruction, la copie ou le blocage non autorisés de l'information, ou la neutralisation de logiciels utilisés pour sécuriser des données numériques ;

d) « Pornographie mettant en scène des enfants » s'entend dans l'acception qui en est donnée à l'article 2, paragraphe c), 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 les enfants, du 25 mai 2000 ;

e) On entend par « produit » tout bien provenant directement ou indirectement de la commission d'un acte incriminé en application de la présente Convention ou obtenu directement ou indirectement en le commettant, ainsi que les revenus ou autres avantages tirés de ce produit, des biens en lesquels le produit a été transformé ou converti ou des biens auxquels il a été mêlé ;

f) On entend par « technologies de l'information et des communications » les processus et les méthodes utilisés aux fins de la production, du traitement et de la diffusion d'informations, ainsi que les moyens employés pour les mettre en œuvre ;

g) On entend par « réseaux d'information et de télécommunications » l'ensemble des dispositifs techniques conçus pour contrôler les processus technologiques au moyen de l'informatique et des télécommunications ;

h) On entend par « biens » tous les types d'avoirs, corporels ou incorporels, meubles ou immeubles, tangibles ou intangibles, y compris l'argent placé sur un compte bancaire, les actifs financiers numériques et les monnaies numériques, notamment les cryptomonnaies, ainsi que les actes juridiques ou documents attestant la propriété intégrale ou partielle de ces avoirs ;

i) On entend par « information » toute donnée (message, enregistrement), indépendamment de la forme sous laquelle elle se présente ;

j) On entend par « confiscation » la dépossession de biens sous la contrainte et sans compensation sur décision d'un tribunal ou d'une autre autorité compétente ;

k) On entend par « attaque informatique » le fait de porter délibérément atteinte, à l'aide de logiciels et/ou de logiciels et de matériel informatique, à des systèmes informatiques ou à des réseaux d'information et de télécommunications dans l'objectif d'en perturber ou d'en interrompre le fonctionnement, ou de menacer la sécurité des informations traitées par de telles installations ;

l) On entend par « donnée numérique » toute donnée (enregistrements), indépendamment de la forme et des caractéristiques sous lesquelles elle se présente, contenue et traitée dans des appareils, systèmes et réseaux d'information et de télécommunications ;

m) On entend par « infrastructure d'information critique » l'ensemble d'infrastructures d'information critiques et de réseaux de télécommunications utilisés pour interconnecter de telles infrastructures ;

n) On entend par « infrastructures essentielles » les systèmes informatiques et les réseaux d'information et de télécommunications des pouvoirs publics et les systèmes informatiques et dispositifs de contrôle des processus automatiques utilisés dans les secteurs de la défense, de la santé, de l'éducation, du transport, des communications, de l'énergie et des finances ainsi que dans le secteur bancaire, dans le domaine nucléaire et dans d'autres domaines essentiels à la vie de l'État et de la société ;

o) On entend par « fournisseur de services » :

i) Toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen des technologies de l'information et des communications ; ou

ii) Toute autre entité traitant ou stockant des informations électroniques pour le compte d'une entité visée au sous-alinéa i) ci-dessus ou des utilisateurs des services fournis par cette entité ;

p) On entend par « donnée relative au trafic » toute information électronique (à l'exclusion du contenu des données transférées) portant sur le transfert de données au moyen des technologies de l'information et des communications et indiquant, en particulier, l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée d'une communication ou le type de service en réseau sous-jacent ;

q) On entend par « appareil ou système électronique » l'ensemble (le regroupement) d'éléments de matériel utilisés ou conçus aux fins du traitement, de l'entreposage et du transfert automatiques d'informations électroniques ;

r) On entend par « preuve électronique » toute information probante stockée ou transmise sous forme numérique (sur un support électronique).

Le terme « préjudice important » revêt le sens qui lui est donné dans le droit interne de l'État partie requis.

Afrique du Sud

[Original : anglais]
[14 avril 2022]

Chapitre premier. Dispositions générales

Article premier. Énoncé des objectifs

Les objectifs de la Convention sont les suivants :

a) Promouvoir et renforcer les mesures visant à prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles et la cybercriminalité, tout en protégeant les utilisateurs de ces technologies contre cette forme de criminalité ;

b) Promouvoir et renforcer les mesures visant à prévenir et combattre efficacement les infractions pénales et autres commises dans le domaine des technologies de l'information et des communications ;

c) Promouvoir, faciliter et appuyer la coopération internationale visant à prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles et la cybercriminalité ;

d) Fournir des outils pratiques permettant d'améliorer l'assistance technique entre les États parties et de renforcer les capacités dont sont dotées les autorités nationales pour prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles et la cybercriminalité, et renforcer les mesures visant à promouvoir l'échange d'informations, de données d'expérience et de bonnes pratiques.

Article 2. Terminologie

Aux fins de la présente Convention :

a) Le terme « objet » s'entend :

i) De données ;

ii) D'un programme informatique ;

iii) D’un support de stockage de données informatiques ; ou

iv) D’un système informatique ;

qui :

a. Ont, ou sont présumés avoir, sur la base de soupçons raisonnables, un lien avec la commission, soupçonnée ou avérée ;

b. Peuvent constituer une preuve de la commission, soupçonnée ou avérée ; ou

c. Sont destinés, ou présumés être destinés, sur la base de soupçons raisonnables, à être utilisés pour la commission :

i. D’une infraction au sens de la présente Convention ;

ii. De toute autre infraction causée au moyen de technologies de l’information et des communications ; ou

iii. D’une infraction dans un État étranger qui est en grande partie similaire à une infraction visée par la présente Convention ;

b) Le terme « contenus montrant des abus sexuels sur enfant » s’entend de toute image, quelle que soit la manière dont elle a été créée, ou toute description ou présentation – photographie, film, vidéo, image – fabriquée ou produite par des moyens électroniques, mécaniques ou autres, d’un comportement sexuellement explicite, lorsque :

i) La production de cette représentation visuelle fait intervenir une personne mineure ;

ii) Cette représentation visuelle est une image numérique ou générée par ordinateur qui montre une personne mineure se livrant à un comportement sexuellement explicite, ou encore une image des organes sexuels d’une personne mineure, qui est produite ou utilisée à des fins principalement sexuelles et exploitée à l’insu ou non de l’enfant ; et

iii) Cette représentation visuelle a été créée, adaptée ou modifiée pour sembler montrer une personne mineure se livrant à un comportement sexuellement explicite ;

c) Le terme « ordinateur » s’entend de tout dispositif électronique programmable utilisé, soit en tant que tel, soit en tant que partie d’un système informatique ou de tout autre dispositif ou équipement, pour exécuter des opérations arithmétiques, logiques, de routage, de traitement ou de stockage prédéterminées conformément à des instructions définies, et qui comprend des données, un programme informatique ou un support de stockage de données informatiques qui sont liés à un tel dispositif, connectés à celui-ci ou utilisés avec celui-ci ;

d) Le terme « données informatiques » s’entend de toute représentation de faits, d’informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu’un système informatique exécute une fonction ;

e) Le terme « support de stockage de données informatiques » s’entend de tout dispositif à partir duquel des données ou un programme informatique peuvent être reproduits ou sur lequel des données ou un programme informatique peuvent être stockés au moyen d’un système informatique, que ce dispositif soit connecté physiquement ou non audit système ;

f) Le terme « programme informatique » s’entend de données représentant des instructions ou des commandes qui, une fois exécutées dans un système informatique, permettent à celui-ci d’exécuter une fonction ;

g) Le terme « système informatique » s’entend :

i) D’un ordinateur ; ou

ii) De plusieurs ordinateurs interconnectés ou apparentés, capables :

a. D'échanger entre eux des données ou toute autre fonction ; ou

b. D'échanger des données ou toute autre fonction avec un autre ordinateur ou système informatique ;

h) Le terme « confiscation » s'entend de la dépossession permanente de biens sur décision d'un tribunal ou d'une autre autorité compétente ;

i) Le terme « criminalité cyberdépendante » s'entend d'infractions qui ne peuvent être commises qu'à l'aide d'un ordinateur, de réseaux informatiques ou d'autres types de technologies de l'information et des communications ;

j) Le terme « criminalité facilitée par Internet » s'entend d'infractions pénales qui ne dépendent pas de l'utilisation d'ordinateurs ou de réseaux mais qui ont été transposées à une autre échelle ou transformées à l'aide d'Internet et de techniques de communication ;

k) Le terme « message de données » s'entend de données générées, envoyées, reçues ou stockées par des moyens électroniques, dont toute restitution se présente sous une forme intelligible ;

l) Le terme « information numérique » s'entend de toute donnée (enregistrements), indépendamment de la forme et des caractéristiques sous lesquelles elle se présente, contenue et traitée dans des dispositifs, systèmes et réseaux d'information et de communication ;

m) Le terme « preuve électronique » s'entend de toute information ayant force probante stockée ou transmise sous forme numérique (sur un support électronique) ;

n) Le terme « gel des avoirs » s'entend de l'interdiction temporaire du transfert, de la conversion, de la disposition ou du mouvement de biens, ou du fait d'assumer à titre temporaire la garde ou le contrôle de biens sur décision d'un tribunal ou d'une autre autorité compétente ;

o) Le terme « biens » s'entend de tous les types d'avoirs, corporels ou incorporels, meubles ou immeubles, tangibles ou intangibles, ainsi que les actes juridiques ou documents attestant la propriété de ces avoirs ou les droits y relatifs ;

p) Le terme « produit du crime » s'entend de tout bien provenant directement ou indirectement de la commission d'une infraction ou obtenu directement ou indirectement en la commettant ;

q) Le terme « infraction principale » s'entend de toute infraction par suite de laquelle est généré un produit qui est susceptible de devenir l'objet d'une infraction définie à l'article 23 de la présente Convention et de la législation nationale de l'État partie ou État Membre ;

r) Le terme « saisie des avoirs » s'entend du fait de prendre le contrôle permanent de biens ou d'assumer à titre permanent la garde ou le contrôle de biens sur décision d'un tribunal ou d'une autre autorité compétente ;

s) Le terme « fournisseur de services » s'entend de toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, ou de toute autre entité traitant ou stockant des données informatiques pour le compte de ce service de communication ou de ses utilisateurs ;

t) Le terme « données de trafic » s'entend des données ayant trait à une communication, indiquant l'origine, la destination, l'itinéraire, le format, l'heure, la date, la taille et la durée de cette communication ou le type de service sous-jacent.

Article 3. Champ d'application

La présente Convention s'applique, conformément à ses dispositions, à la prévention, aux enquêtes et aux poursuites concernant des infractions relevant de la

criminalité cyberdépendante ou facilitée par Internet causées par l'utilisation des technologies de l'information et des communications à des fins criminelles, ainsi qu'au gel, à la saisie, à la confiscation et à la restitution du produit des infractions visées par la Convention.

Article 4. Protection de la souveraineté

1. Les États parties exécutent leurs obligations au titre de la présente Convention d'une manière compatible avec les principes de l'égalité souveraine et de l'intégrité territoriale des États et avec celui de la non-intervention dans les affaires intérieures d'autres États.

2. Aucune disposition de la présente Convention n'habilite un État partie à exercer sur le territoire d'un autre État une compétence et des fonctions qui sont exclusivement réservées aux autorités de cet autre État par son droit interne.

Suisse

[Original : anglais]
[8 avril 2022]

2.1. Dispositions générales

Objet

La présente Convention a pour objet :

a) De promouvoir et renforcer les mesures visant à [prévenir et combattre] la cybercriminalité de manière efficace ;

b) De promouvoir, faciliter et appuyer la coopération internationale et l'assistance technique visant à prévenir et combattre la cybercriminalité.

Respect et protection des droits humains et des libertés fondamentales

Les États parties exécutent leurs obligations au titre de la présente Convention d'une manière compatible avec les obligations que leur impose le droit international des droits de l'homme.

Terminologie

Le terme « système informatique » s'entend de tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure, ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

Le terme « données informatiques » s'entend de toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

Le terme « fournisseur de services » s'entend :

a) De toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ; et

b) De toute autre entité traitant ou stockant des données informatiques pour le compte de ce service de communication ou de ses utilisateurs.

Le terme « données de trafic » s'entend de toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Champ d'application

La présente Convention s'applique, sauf disposition contraire, à la prévention, aux enquêtes et aux poursuites concernant les infractions établies conformément à ses dispositions relatives à l'incrimination.

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

[Original : anglais]
[12 avril 2022]

Chapitre. Dispositions générales

Article premier. Objet

La présente Convention a pour objet de promouvoir la coopération internationale et l'assistance technique visant à prévenir et combattre la cybercriminalité.

Article 2. Définitions

Aux fins de la présente Convention :

a) Le terme « système informatique » s'entend de tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure, ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;

b) Le terme « données informatiques » s'entend de toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

c) Le terme « fournisseur de services » s'entend :

i) De toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ; et

ii) De toute autre entité traitant ou stockant des données informatiques pour le compte de ce service de communication ou de ses utilisateurs ;

d) Le terme « données de trafic » s'entend de toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Article 3. Champ d'application

1. La présente Convention s'applique, sauf disposition contraire, à la prévention, aux enquêtes et aux poursuites concernant les infractions établies conformément à ses dispositions.

2. La présente Convention peut également s'appliquer, lorsqu'elle en dispose ainsi, à la collecte de preuves sous forme électronique d'une infraction pénale.

Article 4. Protection des droits humains

Chaque Partie fait en sorte que l'exécution des obligations que lui impose la présente Convention est conforme au droit international des droits de l'homme.

Observations supplémentaires

Le Royaume-Uni estime qu'il peut également être utile que le chapitre relatif aux dispositions générales traite de la manière dont la présente Convention se rapporte à d'autres instruments de justice pénale des Nations Unies et les complète, et qu'il prévoie un engagement à prendre en compte les questions de genre dans l'application des dispositions de la Convention.

République-Unie de Tanzanie

[Original : anglais]
[8 avril 2022]

3. Dispositions générales

L'objet de la Convention devrait être de promouvoir la coopération en matière de lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Le monde virtuel étant en perpétuelle évolution, il existe une grande variété de termes utilisés à ce jour dans le domaine des technologies de l'information et de la communication. Il est impératif que la Convention définisse des termes qui soient appliqués universellement dans le domaine des technologies de l'information et des communications afin d'éviter toute ambiguïté ou tout malentendu.

3.1. Définition des termes

La République-Unie de Tanzanie estime que la Convention devrait énoncer des définitions neutres et techniques afin de tenir compte de l'évolution rapide des technologies. Les termes à définir devraient être les éléments suivants :

a) Accès ;

b) Fournisseur d'accès ;

c) Fournisseur de mise en cache ;

d) Enfant ;

e) Pédopornographie ;

f) Système informatique ;

g) Données informatiques ;

h) Confiscation ;

i) Contrebande ;

j) Cryptographie ;

k) Cyberterrorisme ;

l) Données ;

m) Message de données ;

n) Support de stockage de données ;

o) Données électroniques ;

p) Gel ;

q) Entraver (en relation avec un système informatique) ;

r) Système de messagerie interactive ;

s) Interception (en relation avec une fonction de l'ordinateur) ;

t) Interconnexion ;

u) Auteur ;

v) Contenus racistes et xénophobes

w) Saisie ;

x) Fournisseur de services (en relation avec les technologies de l'information et des communications) ;

y) Données de trafic.

3.2. Compétence

La Convention devrait prévoir des mesures législatives et autres nécessaires pour que chaque État partie établisse sa compétence à l'égard des infractions établies conformément à ses dispositions lorsque :

a) L'infraction est commise sur son territoire ;

b) 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 ;

c) L'infraction est dirigée contre un système, un dispositif ou des données informatiques ou une personne situés sur son territoire ;

d) L'infraction est commise par ou à l'encontre d'un de ses ressortissants.

États-Unis d'Amérique

[Original : anglais]
[8 avril 2022]

Terminologie

Le terme « enfant » s'entend de toute personne âgée de moins de 18 ans.

Le terme « contenus montrant des abus sexuels sur enfant » s'entend de toute représentation visuelle éventuellement transmise en direct : a) d'un enfant se livrant à un comportement sexuellement explicite, réel ou simulé ; ou b) d'une personne adulte se livrant à un comportement sexuel explicite, réel ou simulé, avec un enfant associé intentionnellement à cette représentation visuelle éventuellement transmise en direct. Il n'est pas nécessaire que l'enfant soit conscient de la nature de ce comportement sexuellement explicite ou capable d'en apprécier la nature[6].

Le terme « données informatiques » s'entend de toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un ordinateur exécute une telle fonction.

Le terme « système informatique » s'entend de tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure, ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

Le terme « confiscation » s'entend de la dépossession permanente de biens sur décision d'un tribunal ou d'une autre autorité compétente[7].

Le terme « cybercriminalité » s'entend des infractions établies conformément à la présente Convention.

[6] Adapté de l'article 2 c) 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.

[7] Convention contre la criminalité organisée, art. 2 g).

Les termes « gel » ou « saisie » s'entendent de l'interdiction temporaire du transfert, de la conversion, de la disposition ou du mouvement de biens, ou du fait d'assumer à titre temporaire la garde ou le contrôle de biens sur décision d'un tribunal ou d'une autre autorité compétente[8].

Le terme « infraction principale » s'entend de toute infraction par suite de laquelle est généré un produit qui est susceptible de devenir l'objet d'une infraction définie dans l'article de la présente Convention relatif à l'incrimination du blanchiment du produit de la cybercriminalité[9].

Le terme « produit du crime » s'entend de tout bien provenant directement ou indirectement de la commission d'une infraction ou obtenu directement ou indirectement en la commettant[10].

Le terme « biens » s'entend de tous les types d'avoirs, corporels ou incorporels, meubles ou immeubles, tangibles ou intangibles, ainsi que les actes juridiques ou documents attestant la propriété de ces avoirs ou les droits y relatifs[11].

Le terme « organisation d'intégration économique régionale » s'entend d'une organisation constituée par des États souverains d'une région donnée, à laquelle ses États membres ont transféré des compétences au titre des questions régies par la présente Convention et qui a été dûment autorisée, conformément à ses procédures internes, à signer, ratifier, accepter, approuver ladite Convention ou à y adhérer ; dans la présente Convention, les références aux « États parties » s'appliquent à ces organisations dans la limite de leur compétence[12].

Le terme « fournisseur de services » s'entend : a) de toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ; et b) de toute autre entité traitant ou stockant des données informatiques pour le compte de ce service de communication ou de ses utilisateurs.

Le terme « comportement sexuellement explicite » s'entend d'au moins l'un des comportements réels ou simulés suivants : a) relations sexuelles – y compris génito-génitales, oro-génitales, ano-génitales ou oro-anales – entre des enfants ou entre une personne adulte et un enfant ; b) zoophilie ; c) masturbation ; d) violences sadomasochistes dans un contexte sexuel ; ou e) exhibition lascive des parties génitales ou de la région pubienne d'un enfant, vêtu ou nu.

Le terme « données de trafic » s'entend de toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Champ d'application

La présente Convention s'applique, sauf disposition contraire, à la prévention, aux enquêtes et aux poursuites concernant les infractions établies conformément à ses dispositions, ainsi qu'à la collecte, à l'obtention et au partage de preuves électroniques.

Protection des droits humains et des libertés fondamentales et état de droit

1. Les États parties exécutent leurs obligations au titre de la présente Convention dans le plein respect des droits humains et des libertés fondamentales, et de l'état de droit.

---

[8] Ibid., art. 2 f).
[9] Ibid., art. 2 h).
[10] Ibid., art. 2 e).
[11] Ibid., art. 2 d).
[12] Ibid., art. 2 j).

2. Aucune disposition de la présente Convention ne doit être interprétée comme modifiant les autres droits et obligations des États et des individus au titre du droit international, y compris de la Charte des Nations Unies et du droit international des droits de l'homme.

3. Toute personne placée en détention ou contre laquelle toute autre mesure est prise ou une procédure est engagée en application de la présente Convention bénéficie de tous les droits et garanties prévus par la législation de l'État sur le territoire duquel elle se trouve et par les dispositions pertinentes du droit international des droits de l'homme, y compris du Pacte international relatif aux droits civils et politiques.

Protection de la souveraineté[13]

1. Les États parties exécutent leurs obligations au titre de la présente Convention d'une manière compatible avec les principes de l'égalité souveraine et de l'intégrité territoriale des États et avec celui de la non-intervention dans les affaires intérieures d'autres États.

2. Aucune disposition de la présente Convention n'habilite un État partie à exercer sur le territoire d'un autre État une compétence ou des fonctions qui sont exclusivement réservées aux autorités de cet autre État par son droit interne.

Venezuela (République bolivarienne du)

[Original : espagnol]
[13 avril 2022]

4. Dispositions générales

Dans ce contexte, les dispositions générales de la Convention doivent être conformes aux principes fondamentaux du droit international public qui, tels qu'ils sont consacrés par la Charte des Nations Unies, feront partie intégrante du futur instrument, notamment la reconnaissance de la souveraineté et de la compétence territoriale prévues par la législation nationale des États, y compris l'application au cyberespace du principe de souveraineté, la non-ingérence dans les affaires intérieures des autres États, le respect de l'intégrité territoriale des autres États et le règlement pacifique des différends.

La Convention doit établir le principe de complémentarité avec d'autres instruments internationaux, tant multilatéraux que régionaux, relatifs à la criminalité transnationale, tels que la Convention des Nations Unies contre la corruption et la Convention des Nations Unies contre la criminalité transnationale organisée, ainsi que le respect des responsabilités découlant du droit international des droits de l'homme, notamment des conventions relatives aux droits humains.

À cet égard, la République bolivarienne du Venezuela souligne que, à l'instar d'autres instruments juridiques internationaux, cet instrument ne doit pas créer de conflit artificiel entre les concepts de souveraineté nationale et de droits humains, qui sont intrinsèquement complémentaires.

Ce chapitre doit inclure les définitions des termes et expressions clefs employés dans la Convention.

[13] Convention contre la criminalité organisée et Convention contre la corruption, art. 4.

Viet Nam

[Original : anglais]
[12 avril 2022]

Chapitre premier. Dispositions générales

1. Objectifs

a) Promouvoir et renforcer les mesures visant à prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles ;

b) Promouvoir, faciliter et appuyer la coopération internationale et l'assistance technique visant à prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles, notamment par le recouvrement d'avoirs, conformément aux principes fondamentaux du droit international et dans le respect des droits humains.

2. Champ d'application

La présente Convention s'applique à la prévention, aux enquêtes et aux poursuites concernant l'utilisation des technologies de l'information et des communications à des fins criminelles.

3. Protection de la souveraineté

a) Les États Membres exécutent leurs obligations au titre de la présente Convention d'une manière compatible avec les principes de l'égalité souveraine et de l'intégrité territoriale des États, du refus de la menace de recours ou du recours à la force, et de la non-intervention dans les affaires intérieures d'autres États ;

b) Aucune disposition de la présente Convention n'autorise un État Membre à exercer sur le territoire d'un autre État une compétence et des fonctions qui sont exclusivement réservées aux autorités de cet autre État Membre par son droit interne.

4. Définitions

a) Le terme « cyberespace » s'entend d'un réseau d'infrastructures informatiques qui comprend des réseaux de télécommunications, Internet, des réseaux informatiques, des systèmes de communication, des systèmes de traitement et de contrôle de l'information et des bases de données ;

b) Le terme « système d'information » s'entend d'une combinaison de matériel, de logiciels et de bases de données conçus pour la création, la transmission, la collecte, le traitement et le stockage d'informations dans le cyberespace ;

c) Le terme « cyberattaque » s'entend de l'utilisation du cyberespace, de technologies de l'information ou de dispositifs électroniques pour saboter ou interrompre le réseau de télécommunications, Internet, les réseaux informatiques, les systèmes de communication, les systèmes de traitement et de contrôle de l'information, les bases de données ou les dispositifs électroniques ;

d) Le terme « cyberterrorisme » s'entend d'un acte de terrorisme ou de financement du terrorisme qui implique l'utilisation du cyberespace, de technologies de l'information ou de dispositifs électroniques ;

e) Le terme « informations personnelles » s'entend des informations associées à l'identification d'une personne physique ;

f) Le terme « données numériques » s'entend de signaux, lettres, chiffres, images, sons ou éléments similaires créés, stockés et transmis ou acquis par des moyens électroniques ;

g) Le terme « infrastructure du cyberespace » s'entend d'un système d'infrastructures destiné à la création, à la transmission, à la collecte, au traitement et au stockage d'informations et de données dans le cyberespace.