Nations Unies A/AC.291/16

Assemblée générale

Distr. générale
7 novembre 2022
Français
Original : anglais

Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles
Quatrième session
Vienne, 9-20 janvier 2023

Document de négociation consolidé sur les dispositions générales, les dispositions relatives à l'incrimination 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

Note de la Présidente

1. Dans la perspective de la quatrième session du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, et conformément au plan de progression et mode de fonctionnement que le Comité spécial a approuvés à sa première session, la Présidente du Comité a établi, avec le concours du Secrétariat, un document de négociation consolidé basé sur les résultats de la première lecture des dispositions générales, des dispositions relatives à l'incrimination et des dispositions relatives aux mesures procédurales, à la détection et à la répression du projet de convention (voir annexe).

2. Plus précisément, le document de négociation consolidé fait fond sur des éléments tirés des propositions faites par les États Membres et rassemblées dans les documents A/AC.291/9, A/AC.291/9/Add.1, A/AC.291/9/Add.2 et A/AC.291/9/Add.3, ainsi que sur les déclarations prononcées par les États Membres et les vues qu'ils ont exprimées à la deuxième session. On s'est efforcé de proposer une formulation unique pour chaque disposition en intégrant des éléments tirés de différentes propositions ou déclarations. Certains termes ont été placés entre crochets afin de rendre compte des vues divergentes sur leur utilisation exprimées par certains États Membres aux sessions du Comité spécial.

3. Un deuxième document de négociation consolidé sera établi à partir des résultats de la première lecture du préambule, des dispositions relatives à la coopération internationale, à l'assistance technique, aux mesures préventives et au mécanisme d'application, ainsi que des dispositions finales de la convention, à laquelle le Comité spécial a procédé à sa troisième session, et il sera mis à la disposition de ce dernier pour qu'il l'examine avant sa cinquième session.

V.22-22551 (F) 051222 061222

Annexe

Document de négociation consolidé sur les dispositions générales, les dispositions relatives à l'incrimination 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

Chapitre I
Dispositions générales

Article premier. Objet

La présente Convention a pour objet de :

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

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

c) Proposer des mesures concrètes permettant d'améliorer l'assistance technique entre les États parties, 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] [la cybercriminalité], notamment au profit des pays en développement, ainsi que de renforcer et de promouvoir l'échange d'informations, de connaissances spécialisées, de données d'expérience et de bonnes pratiques.

Article 2. Terminologie

[*Compte tenu des déclarations faites par de nombreux États Membres à la deuxième session du Comité spécial, cette disposition devrait être traitée une fois arrêtés les principaux articles de fond de la convention*.]

Article 3. Champ d'application

1. La présente Convention s'applique, conformément à ses dispositions, à la prévention, à la détection, aux enquêtes et aux poursuites concernant [l'utilisation des technologies de l'information et des communications à des fins criminelles] [la cybercriminalité], y compris au gel, à la saisie, à la confiscation et à la restitution du produit des infractions établies conformément à la présente Convention.

2. La présente Convention s'applique également au recueil, à l'obtention, à la préservation et à la communication des preuves sous forme électronique [d'infractions visées par la présente Convention] [de toute infraction pénale] [d'infractions graves].

3. Aux fins de l'application de la présente Convention, il n'est pas nécessaire, sauf si celle-ci en dispose autrement, que les infractions qui y sont visées causent un dommage ou un préjudice aux personnes, y compris des personnes morales, aux biens ou à l'État.

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.

Article 5. Respect des droits humains

1. Les États parties font en sorte que l'exécution des obligations que leur impose la présente Convention soit conforme aux dispositions applicables du droit international des droits humains.

2. Les États parties s'efforcent de tenir compte des questions de genre et de prendre en considération la situation et les besoins particuliers des groupes vulnérables, en particulier des femmes, des enfants et des personnes âgées, dans les mesures prises pour prévenir et combattre [l'utilisation des technologies de l'information et des communications à des fins criminelles] [la cybercriminalité].

Chapitre II
Incrimination

AXE THÉMATIQUE 1[1]

Article 6. Accès illégal

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque l'acte a été commis intentionnellement, au fait d'accéder illicitement à tout ou partie d'un [système informatique] [système/dispositif électronique].

2. Un État partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des [données informatiques] [informations électroniques/numériques] ou dans une autre intention criminelle, ou soit en relation avec un [système informatique] [système/dispositif électronique] connecté à un autre [système informatique] [système/dispositif électronique].

3. Chaque État partie peut prévoir une aggravation de la peine lorsque cet accès :

a) Porte préjudice aux utilisateurs et utilisatrices et aux bénéficiaires ;

b) Conduit à l'obtention d'informations confidentielles provenant de sources officielles ;

c) Fait intervenir ou touche des infrastructures critiques.

Article 7. Interception illégale

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque l'acte a été commis intentionnellement, au fait d'intercepter illicitement, par des moyens techniques, des [données informatiques] [informations électroniques/numériques] lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un [système informatique] [système/dispositif électronique], y compris les émissions électromagnétiques provenant d'un [système informatique] [système/dispositif électronique] transportant de telles [données informatiques] [informations électroniques/numériques].

2. Un État partie peut exiger que l'infraction soit commise dans une intention criminelle ou soit en relation avec [un système informatique] [un système/dispositif

[1] L'organisation par thèmes a pour seul but de structurer les débats tenus lors des sessions formelles.

électronique] connecté à un autre [système informatique] [système/dispositif électronique].

Article 8. Atteinte à l'intégrité [de données informatiques] [d'informations électroniques/numériques]

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement, au fait d'introduire, de télécharger, de copier, d'endommager, de perturber, d'effacer, de détériorer, d'altérer ou de supprimer des [données informatiques] [informations électroniques/numériques] de manière illicite.

2. Un État partie peut exiger que le comportement décrit au paragraphe 1 entraîne un préjudice grave.

3. Chaque État partie peut prévoir une aggravation de la peine lorsque les actes décrits au paragraphe 1 font intervenir ou touchent des infrastructures critiques.

Article 9. Atteinte à l'intégrité d'un [système informatique] [système/dispositif électronique]

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement, au fait d'entraver gravement et illicitement le fonctionnement d'un [système informatique] [système/dispositif électronique] par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération, la perturbation ou la suppression [de données informatiques] [d'informations électroniques/numériques].

2. Chaque État partie peut prévoir une aggravation de la peine lorsque les actes décrits au paragraphe 1 font intervenir ou touchent des infrastructures critiques.

Article 10. Utilisation abusive de dispositifs et de programmes

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement et illicitement :

a) À la production, à la vente, à l'obtention pour utilisation, à l'importation, à la diffusion ou à d'autres formes de mise à disposition :

i) D'un dispositif, y compris un programme, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément à la présente Convention ; ou

ii) D'un mot de passe, de justificatifs d'accès ou [de données] [d'informations] similaires permettant d'accéder à tout ou partie d'un [système informatique] [système/dispositif électronique] ;

dans l'intention que ledit dispositif, ledit mot de passe, lesdits justificatifs d'accès ou lesdites [données] [informations] similaires soient utilisés afin de commettre l'une des infractions établies conformément à [l'article 6, sur l'accès illégal, l'article 7, sur l'interception illégale, l'article 8, sur l'atteinte à l'intégrité [de données informatiques] [d'informations électroniques/numériques] et l'article 9, sur l'atteinte à l'intégrité d'un [système informatique] [système/dispositif électronique], de la présente Convention] [la présente Convention] ; et

b) À la possession d'un élément visé aux alinéas a) i) ou ii) du paragraphe 1 du présent article, dans l'intention qu'il soit utilisé afin de commettre l'une des infractions établies conformément à [l'article 6, sur l'accès illégal, l'article 7, sur l'interception illégale, l'article 8, sur l'atteinte à l'intégrité [de données informatiques] [d'informations électroniques/numériques] et l'article 9, sur l'atteinte à l'intégrité d'un [système informatique] [système/dispositif électronique], de la

présente Convention] [la présente Convention]. Un État partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition ou la possession mentionnées au paragraphe 1 n'ont pas pour but de commettre une infraction établie conformément [à] [aux articles précédents de] la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un [système informatique] [système/dispositif électronique].

3. Chaque État partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la diffusion ou d'autres formes de mise à disposition des éléments mentionnés à l'alinéa a) ii) du paragraphe 1 du présent article.

AXE THÉMATIQUE 2

Article 11. Falsification [informatique] [au moyen des technologies de l'information et des communications]

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement et illicitement, à l'introduction, à l'altération, à l'effacement ou à la suppression [de données informatiques] [d'informations électroniques/numériques], engendrant des [données] [informations] non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles, d'une manière qui pourrait causer un préjudice.

2. Aux fins du présent article, un État partie peut exiger une intention frauduleuse ou une intention criminelle similaire pour que la responsabilité pénale soit engagée.

Article 12. Fraude [informatique] [au moyen des technologies de l'information et des communications]

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement et illicitement, au fait de frauder en tout ou en partie en ligne et de causer un préjudice patrimonial à une autre personne ou à une entité par la voie de :

a) Toute introduction, toute altération, tout effacement, tout blocage ou toute suppression de données informatiques ;

b) Toute forme d'atteinte au fonctionnement d'un [système informatique] [système/dispositif électronique] ;

c) Toute utilisation d'un [système informatique] [système/dispositif électronique] pour tromper une autre personne ou une entité ou l'inciter à faire ou à omettre de faire quelque chose qu'elle n'aurait autrement pas fait ou omis de faire ;

dans l'intention, frauduleuse ou criminelle, d'obtenir illicitement pour soi-même ou pour autrui :

i) Un bénéfice économique ; ou

ii) Des [données informatiques] [informations électroniques/numériques], y compris des [données] [informations] à caractère personnel qui ne seraient autrement pas mises à la disposition de l'auteur des faits.

2. Les actes de fraude comprennent, sans s'y limiter, les actes commis à l'intérieur des frontières nationales ou au-delà à l'aide d'Internet ou d'autres moyens [cyberdépendants] [numériques], par les méthodes suivantes :

a) Fraude par fausse déclaration ;

b) Fraude par défaut d'information ;

c) Fraude par abus de position, avec intention frauduleuse ou criminelle de causer une perte à autrui ou de réaliser un gain financier ou autre pour autrui.

Article 13. Vol [informatique] [au moyen des technologies de l'information et des communications]

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale au fait de voler des biens ou d'acquérir illégalement des titres y relatifs, au moyen de la destruction, du blocage, de la modification ou de la copie [de données informatiques] [d'informations électroniques/numériques] ou de toute autre forme d'immixtion dans des systèmes [informatiques] [électroniques].

2. Chaque État partie peut considérer le vol de biens ou l'acquisition illégale de titres y relatifs [par voie informatique] [au moyen des technologies de l'information et des communications] comme une circonstance aggravante de l'infraction de vol telle que définie dans son droit interne.

Article 14. Utilisation illicite d'instruments de paiement électronique

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale aux actes suivants :

a) Le fait de confectionner, de fabriquer ou d'installer, par quelque moyen que ce soit, tout dispositif ou matériel facilitant la contrefaçon ou l'imitation de tout instrument de paiement électronique ;

b) Le fait de se procurer, d'utiliser ou de transmettre à autrui les [données] [informations] relatives à un instrument de paiement, ou de faciliter leur obtention par autrui ;

c) Le fait d'utiliser [un réseau informatique ou une technologie de l'information] [un système informatique] pour obtenir, sans autorisation, accès aux [données] [informations] se rapportant à un instrument de paiement ;

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

AXE THÉMATIQUE 3

Article 15. Violation des informations à caractère personnel

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement et illicitement, au fait de vendre, de fournir ou de mettre autrement à disposition tout matériel contenant des informations personnelles sur une personne, y compris des informations relatives à son compte bancaire, ou d'y accéder dans l'intention d'obtenir un avantage financier, et de communiquer ultérieurement ce matériel à autrui sans le consentement de la personne concernée.

Article 16. Infractions liées à l'identité

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement :

a) Au fait d'obtenir, de recevoir ou de diffuser sans droit des mots de passe ou des justificatifs d'accès à [un système informatique] [des données informatiques] ; et

b) Au fait d'utiliser de manière frauduleuse ou malhonnête la signature électronique, le mot de passe ou tout autre élément d'identification unique d'une autre personne.

AXE THÉMATIQUE 4

Article 17. Atteinte à la propriété intellectuelle

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque l'acte a été commis intentionnellement, au fait de porter atteinte à la propriété intellectuelle, telle que définie dans la législation de cet État partie, au moyen d'un [système informatique] [système/dispositif électronique], y compris au fait d'utiliser illicitement des programmes informatiques et des bases de données protégés par des droits d'auteur et au plagiat, conformément aux obligations qu'il a souscrites en application des conventions pertinentes et applicables, à l'exception de tout droit moral conféré par ces conventions, lorsqu'un tel acte a été commis délibérément et à une échelle commerciale.

2. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque l'acte a été commis intentionnellement, au fait de porter atteinte aux droits connexes, tels que définis dans la législation de cet État partie, au moyen d'un [système informatique] [système/dispositif électronique], conformément aux obligations qu'il a souscrites en application des conventions pertinentes et applicables, à l'exception de tout droit moral conféré par ces conventions, lorsqu'un tel acte a été commis délibérément, à une échelle commerciale et au moyen d'un [système informatique] [système/dispositif électronique].

3. Un État partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cet État partie.

AXE THÉMATIQUE 5

Article 18. Infractions relatives à des contenus en ligne montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement et illicitement, aux faits ci-après :

a) Produire ou reproduire des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants en vue de leur diffusion au moyen d'un [système informatique] [système/dispositif électronique] ;

b) Financer des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants ou y contribuer de toute autre manière au moyen d'un [système informatique] [système/dispositif électronique] ;

c) Contrôler, promouvoir, offrir, montrer publiquement ou mettre à disposition des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants, ou en faire la publicité, au moyen d'un [système informatique] [système/dispositif électronique] ;

d) Diffuser ou transmettre, au moyen d'un [système informatique] [système/dispositif électronique], des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants ;

e) Se procurer, au moyen d'un [système informatique] [système/dispositif électronique], des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants ;

f) Accéder en connaissance de cause à des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants, ou posséder de tels contenus, dans un [système informatique] [système/dispositif électronique] ou un [support de stockage de données informatiques] [dispositif électronique de stockage de données

numériques], ou visionner la transmission en direct de contenus montrant un enfant se livrant à un comportement sexuellement explicite ;

g) Participer à toute entreprise dont on sait ou dont on a des raisons de croire qu'elle est liée à des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants, ou recevoir des bénéfices d'une telle entreprise, au moyen d'un [système informatique] [système/dispositif électronique].

2. Aux fins du paragraphe 1, l'expression « contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants » désigne tout support visuel, y compris toute photographie, vidéo ou diffusion en direct, ainsi que tout dessins, tout support écrit et tout enregistrement audio, qui représente :

a) Un enfant se livrant à un comportement sexuellement explicite, réel ou simulé ;

b) Une personne qui a l'apparence d'un enfant se livrant à un comportement sexuellement explicite, réel ou simulé ;

c) Des images réalistes représentant un enfant se livrant à un comportement sexuellement explicite, réel ou simulé ;

d) Toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles ;

e) Une victime de torture ou d'autres peines ou traitements cruels, inhumains ou dégradants.

3. Aux fins du paragraphe 2, le terme « enfant » désigne toute personne âgée de moins de 18 ans.

4. Les États parties tiennent dûment compte de la nécessité, d'une part, d'éviter toute incrimination des enfants ayant produit eux-mêmes des contenus visés au paragraphe 2 et, d'autre part, de respecter les obligations qui leur incombent en vertu de la Convention relative aux droits de l'enfant et de ses protocoles.

5. Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les alinéas e) et f) du paragraphe 1 et les alinéas b) et c) du paragraphe 2.

Article 19. Facilitation, au moyen d'un [système informatique] [système/dispositif électronique], d'actes faisant intervenir des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale conformément à son droit interne, lorsque ces actes ont été commis intentionnellement et sans motif légal, au fait de créer, d'élaborer, de modifier, de maintenir, de contrôler ou de mettre à disposition un [système informatique] [système/dispositif électronique], de jouer un rôle d'animation ou d'assistance le concernant, ou d'en assurer la publicité ou la promotion, afin de faciliter la commission d'actes faisant intervenir des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants visés à l'article 18 de la présente Convention.

2. Aux fins du paragraphe 1, le terme « faciliter » couvre tout acte visé audit paragraphe ayant pour but de permettre à des personnes de produire des contenus montrant des violences sexuelles sur enfant ou l'exploitation sexuelle d'enfants ou d'y accéder, ou de transmettre, de diffuser, d'offrir ou de mettre à disposition de tels contenus pour elles-mêmes ou pour d'autres personnes.

Article 20. Manipulation psychologique d'un enfant ou fait de se procurer ou de procurer à autrui un enfant à des fins sexuelles au moyen d'un [système informatique] [système/dispositif électronique]

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis

intentionnellement, au fait de manipuler psychologiquement, de se procurer ou de procurer à autrui, de solliciter, de contraindre ou [d'attirer] [d'inciter] un enfant, de se mettre d'accord ou de s'entendre avec lui ou de lui faire une proposition afin de faciliter, d'encourager, d'offrir ou de solliciter un comportement sexuel illicite de la part d'un enfant ou d'une personne que l'on croit être un enfant, ou faisant intervenir un tel enfant ou une telle personne, ou de l'amener à assister ou à se livrer de toute autre manière à des activités sexuelles, au moyen d'un [système informatique] [système/dispositif électronique].

2. Aux fins du paragraphe 1, l'article 2 [x)] [portant sur la définition du terme « enfant » et la responsabilité pénale des enfants] s'applique. En outre, le terme « enfant » désigne également toute personne dont on croit qu'elle a moins de 18 ans.

3. La responsabilité pénale n'est pas établie si la personne a pris des mesures raisonnables pour s'assurer qu'elle n'avait pas affaire à un enfant.

Article 21. Cyberharcèlement d'un enfant

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement, au fait d'utiliser un [système informatique] [système/dispositif électronique] pour compiler, transmettre, publier, reproduire, acheter, vendre, recevoir, échanger ou diffuser le nom, le numéro de téléphone, l'adresse de courrier électronique, l'adresse de résidence, la photo, la description physique, les caractéristiques ou toute autre information permettant d'identifier un enfant, dans le but d'organiser une rencontre avec celui-ci en vue d'avoir des rapports sexuels, un comportement sexuellement explicite ou une activité sexuelle illicite.

AXE THÉMATIQUE 6

Article 22. Implication de personnes mineures dans la commission d'actes illégaux

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale au fait d'utiliser un [système informatique] [système/dispositif électronique] pour impliquer des personnes mineures dans la commission d'actes illégaux qui mettent leur vie ou leur santé physique ou mentale en danger, exception faite des actes visés à l'article [23] [, sur l'incitation ou la coercition au suicide,] de la présente Convention.

Article 23. Incitation ou contrainte au suicide

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale au fait d'inciter ou de contraindre autrui au suicide, y compris des enfants, par des pressions psychologiques ou d'autres formes de pressions exercées au moyen d'un [système informatique] [système/dispositif électronique].

AXE THÉMATIQUE 7

Article 24. Sextorsion

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement, au fait de menacer de diffuser ou de transmettre, par des moyens électroniques, une image intime d'une autre personne, dans l'intention spécifique :

a) De harceler, de menacer, de contraindre, d'intimider cette personne ou d'exercer une influence indue sur elle, notamment en vue d'obtenir un avantage financier ou un autre avantage matériel, y compris pour contraindre la victime à se livrer à une activité sexuelle non désirée ; ou

b) D'obtenir un avantage financier ou un autre avantage matériel, y compris pour contraindre la victime à se livrer à une activité sexuelle non désirée.

2. Aux fins du paragraphe 1, on entend par « image intime » un enregistrement visuel, y compris photographique, filmé ou vidéo, d'une personne, réalisé par quelque moyen que ce soit :

a) Dans lequel la personne figure nue, expose ses organes génitaux, sa région anale ou ses seins, ou se livre à une activité sexuelle explicite ;

b) Dans des circonstances où la personne, au moment de l'enregistrement, pouvait raisonnablement avoir certaines attentes en matière de protection de la vie privée ; et

c) Pour lequel la personne avait toujours ces attentes raisonnables en matière de protection de la vie privée au moment de la commission de l'infraction.

Article 25. Diffusion non consentie d'images intimes

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement et illicitement, au fait de publier, distribuer, transmettre, vendre, mettre à disposition une image intime d'une personne, ou d'en faire la publicité, au moyen d'un [système informatique] [système/dispositif électronique], [dans l'intention de provoquer une détresse émotionnelle grave] en sachant que la personne représentée sur l'image n'a pas donné son consentement à ce comportement, ou sans se soucier de savoir si elle a donné son consentement.

2. Aux fins du paragraphe 1, on entend par « image intime » un enregistrement visuel, y compris photographique, filmé ou vidéo, d'une personne, réalisé par quelque moyen que ce soit :

a) Dans lequel la personne figure nue, expose ses organes génitaux, sa région anale ou ses seins, ou se livre à une activité sexuelle explicite ;

b) Dans des circonstances où la personne, au moment de l'enregistrement, pouvait raisonnablement avoir certaines attentes en matière de protection de la vie privée ; et

c) Pour lequel la personne avait toujours ces attentes raisonnables en matière de protection de la vie privée au moment de la commission de l'infraction.

3. La responsabilité pénale n'est pas établie si le partage non consenti a un but légitime.

4. Un enfant ne peut consentir à la publication d'une image intime dont il est le sujet.

AXE THÉMATIQUE 8

Article 26. Incitation à la conduite d'activités subversives ou armées

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, conformément à son droit interne, à tout appel, émis au moyen des technologies de l'information et des communications, à la conduite d'activités subversives ou armées destinées à renverser par la violence le régime d'un autre État.

Article 27. Infractions liées à l'extrémisme

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale au fait de distribuer, au moyen d'un [système informatique] [système/dispositif électronique], des contenus incitant à la commission d'actes illégaux motivés par la haine politique, idéologique, sociale, raciale, ethnique ou religieuse, ainsi que de défendre et de justifier de tels actes et de fournir un accès à de tels contenus par ce moyen.

Article 28. Négation, approbation, justification ou réhabilitation du génocide ou de crimes contre la paix et l'humanité

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 diffuser de manière intentionnelle, [par voie informatique] [au moyen des technologies de l'information et des communications], tout contenu tendant à nier, à approuver, à justifier ou à réhabiliter des actes pouvant être assimilés au génocide ou aux crimes contre la paix et l'humanité incriminés par le Tribunal militaire international créé en application de l'Accord de Londres du 8 août 1945.

AXE THÉMATIQUE 9

Article 29. Infractions liées au terrorisme

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque ces actes ont été commis au moyen des technologies de l'information et des communications, au fait de commettre des actes terroristes, d'inciter, de recruter ou de participer sous toute autre forme à des activités terroristes, de promouvoir et de justifier le terrorisme ou la collecte ou la fourniture de fonds destinés à son financement, d'entraîner à des actes terroristes, de faciliter la communication entre les organisations terroristes et leurs membres, y compris par la création, la publication ou l'utilisation d'un site Web ou la fourniture d'un appui logistique aux auteurs d'actes terroristes, de diffuser des informations relatives aux méthodes de fabrication d'explosifs employées, notamment, dans le cadre d'actes terroristes et d'inciter au conflit, à la sédition, à la haine ou au racisme.

Article 30. Infractions liées à la distribution de stupéfiants et de substances psychotropes

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque cet acte a été commis intentionnellement, au fait de se livrer au trafic illicite, au moyen d'un [système informatique] [système/dispositif électronique], de stupéfiants et de substances psychotropes et des matériels nécessaires à leur fabrication.

Article 31. Infractions liées au trafic d'armes

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque cet acte a été commis intentionnellement, au fait de se livrer au trafic illicite, au moyen des technologies de l'information et des communications, d'armes, de munitions, d'engins explosifs et de matières explosibles.

Article 32. Distribution illégale de médicaments et de produits médicaux contrefaits

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale au fait de distribuer de manière intentionnelle et illégale, au moyen des technologies de l'information et des communications, des médicaments et des produits médicaux contrefaits.

AXE THÉMATIQUE 10

Article 33. Blanchiment d'argent

1. Chaque État partie adopte, conformément aux principes fondamentaux de son droit interne, les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque l'acte a été commis intentionnellement :

a) i) À la conversion ou au transfert de biens, y compris de monnaies virtuelles, dont celui qui s'y livre sait qu'ils sont le produit du crime, dans le but de dissimuler ou de déguiser l'origine illicite desdits biens ou d'aider toute personne qui

est impliquée dans la commission de l'infraction principale à échapper aux conséquences juridiques de ses actes ;

ii) À la dissimulation ou au déguisement de la nature véritable, de l'origine, de l'emplacement, de la disposition, du mouvement ou de la propriété de biens ou de droits y relatifs dont l'auteur sait qu'ils sont le produit du crime ;

b) Sous réserve des concepts fondamentaux de son système juridique :

i) À l'acquisition, à la détention ou à l'utilisation de biens dont celui qui les acquiert, les détient ou les utilise sait, au moment où il les reçoit, qu'ils sont le produit du crime ;

ii) À la participation à l'une des infractions établies conformément au présent article ou à toute association, entente, tentative ou complicité par fourniture d'une assistance, d'une aide ou de conseils en vue de sa commission.

2. Aux fins de l'application du paragraphe 1 du présent article :

a) Chaque État partie s'efforce d'appliquer le paragraphe 1 du présent article à l'éventail le plus large d'infractions principales ;

b) Chaque État partie inclut dans les infractions principales les infractions pertinentes établies conformément à la présente Convention. S'agissant des États parties dont la législation contient une liste d'infractions principales spécifiques, ceux-ci incluent dans cette liste, au minimum, un éventail complet d'infractions liées à [l'utilisation des technologies de l'information et des communications à des fins criminelles] [la cybercriminalité].

c) Aux fins de l'alinéa b), les infractions principales incluent les infractions commises à l'intérieur et à l'extérieur du territoire relevant de la compétence de l'État partie en question. Toutefois, une infraction commise à l'extérieur du territoire relevant de la compétence d'un État partie ne constitue une infraction principale que lorsque l'acte correspondant est une infraction pénale en vertu du droit interne de l'État où il a été commis et constituerait une infraction pénale en vertu du droit interne de l'État partie appliquant le présent article s'il avait été commis sur son territoire ;

d) Chaque État partie remet au Secrétaire général de l'Organisation des Nations Unies une copie de ses lois qui donnent effet au présent article ainsi qu'une copie de toute modification ultérieurement apportée à ces lois ou une description de ces lois et modifications ultérieures ;

e) Lorsque les principes fondamentaux du droit interne d'un État partie l'exigent, il peut être disposé que les infractions énoncées au paragraphe 1 du présent article ne s'appliquent pas aux personnes qui ont commis l'infraction principale.

Article 34. Entrave à la justice

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale, lorsque les actes ont été commis intentionnellement :

a) Au fait de recourir à la force physique, à des menaces ou à l'intimidation ou de promettre, d'offrir ou d'accorder un avantage indu pour obtenir un faux témoignage ou empêcher un témoignage ou la présentation d'éléments de preuve dans une procédure en rapport avec la commission d'infractions visées par la présente Convention ;

b) Au fait de recourir à la force physique, à des menaces ou à l'intimidation pour empêcher un agent de la justice ou un agent des services de détection et de répression d'exercer les devoirs de leur charge lors de la commission d'infractions visées par la présente Convention. Rien dans le présent alinéa ne porte atteinte aux droits des États parties de disposer d'une législation destinée à protéger d'autres catégories d'agents publics.

AXE THÉMATIQUE 11

Article 35. 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 pour des infractions établies par la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé :

a) Sur un pouvoir de représentation de la personne morale ;

b) Sur une autorité pour prendre des décisions au nom de la personne morale ;

c) Sur une autorité pour exercer un contrôle au sein de la personne morale.

2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque État partie adopte les mesures nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission d'une infraction pénale établie conformément à la présente Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité explicite ou implicite.

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

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

5. 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.

6. La responsabilité des personnes morales n'est pas engagée en cas d'actes commis ou omis de bonne foi :

a) Dans l'accomplissement effectif ou recherché d'un devoir imposé par la présente Convention ou au titre de la présente Convention ; ou

b) Dans l'exercice effectif ou recherché d'une fonction ou d'un pouvoir conféré par la présente Convention ou au titre de la présente Convention.

Article 36. 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 ou encore associé, à une infraction établie conformément à la présente Convention, ou au fait d'organiser une telle infraction ou de donner des instructions à d'autres personnes pour qu'elles commettent cette infraction.

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

4. Chaque État partie adopte les mesures législatives et autres nécessaires pour renforcer la responsabilité en cas d'infraction commise en groupe, y compris par des groupes criminels organisés.

5. Chaque État partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 37. Connaissance, intention et motivation en tant qu'éléments d'une infraction

La connaissance, l'intention ou la motivation nécessaires en tant qu'éléments d'une infraction établie conformément à la présente Convention peuvent être déduites de circonstances factuelles objectives.

Article 38. Prescription

Lorsqu'il y a lieu, chaque État partie fixe, dans le cadre de son droit interne, un long délai de prescription dans lequel des poursuites peuvent être engagées du chef d'une des infractions établies conformément à la présente Convention et fixe un délai plus long ou suspend la prescription lorsque l'auteur présumé de l'infraction s'est soustrait à la justice.

Article 39. Poursuites judiciaires, jugement et sanctions

1. Chaque État partie rend la commission d'une infraction établie conformément à la présente Convention passible de sanctions qui tiennent compte de la gravité de cette infraction.

2. Chaque État partie peut imposer une aggravation de la peine pour les infractions établies conformément à la présente Convention, y compris, mais sans s'y limiter, lorsque la commission des infractions :

a) Porte atteinte à des infrastructures critiques ;

b) Débouche sur l'obtention d'informations confidentielles provenant de sources officielles ;

c) Cause un préjudice, y compris des dommages physiques ou psychologiques, à des personnes.

3. Chaque État partie prend les mesures nécessaires pour établir ou maintenir, conformément à son système juridique et à ses principes constitutionnels, un équilibre approprié entre toutes immunités ou tous privilèges de juridiction accordés à ses agents publics dans l'exercice de leurs fonctions, et la possibilité, si nécessaire, de rechercher, de poursuivre et de juger effectivement les infractions établies conformément à la présente Convention.

4. Chaque État partie s'efforce de faire en sorte que tout pouvoir judiciaire discrétionnaire conféré par son droit interne et afférent aux poursuites judiciaires engagées contre des individus pour des infractions établies conformément à la présente Convention soit exercé de façon à optimiser l'efficacité des mesures de détection et de répression de ces infractions, compte dûment tenu de la nécessité d'exercer un effet dissuasif en ce qui concerne leur commission.

5. Chaque État partie veille à ce que toute personne poursuivie pour une infraction établie conformément à 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 et applicables du droit international des droits humains, y compris le droit à un procès équitable et les droits de la défense.

6. S'agissant d'infractions établies conformément à la présente Convention, chaque État partie prend les mesures appropriées conformément à son droit interne et compte dûment tenu des droits de la défense, pour faire en sorte que les conditions auxquelles sont subordonnées les décisions de mise en liberté dans l'attente du jugement ou de la procédure d'appel tiennent compte de la nécessité d'assurer la présence de la partie défenderesse lors de la procédure pénale ultérieure.

7. Chaque État partie prend en compte la gravité des infractions concernées lorsqu'il envisage l'éventualité d'une libération anticipée ou conditionnelle de personnes reconnues coupables de ces infractions.

8. Aucune disposition de la présente Convention ne porte atteinte au principe selon lequel la définition des infractions établies conformément à celle-ci et des moyens juridiques de défense applicables ainsi que d'autres principes juridiques régissant la légalité des incriminations relève exclusivement du droit interne d'un État partie et selon lequel lesdites infractions sont poursuivies et punies conformément au droit de cet État partie.

9. Les États parties s'efforcent de promouvoir la réinsertion dans la société des personnes reconnues coupables d'infractions établies conformément à la présente Convention.

Chapitre III
Mesures procédurales et détection et répression

AXE THÉMATIQUE 1

Article 40. Compétence

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

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

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

2. Sous réserve de l'article 4 de la présente Convention, un État partie peut également établir sa compétence à l'égard de l'une quelconque de ces infractions dans les cas suivants :

a) Lorsque l'infraction est commise contre l'un ou l'une de ses ressortissants ou l'une de ses personnes morales ; ou

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

c) Lorsque l'infraction est commise hors de son territoire en vue de la commission, sur son territoire, d'une infraction établie conformément à la présente Convention ;

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

e) Lorsque l'infraction concerne les [données informatiques] [informations électroniques/numériques] de ses ressortissantes et ressortissants, quel que soit le lieu où elles sont physiquement stockées, traitées ou triées.

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

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

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

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

Article 41. Champ d'application des mesures procédurales

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

2. Sauf disposition contraire figurant à l'article 48 de la présente Convention, chaque État partie applique les pouvoirs et procédures visés au paragraphe 1 du présent article :

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

b) Aux autres infractions pénales commises au moyen d'un [système informatique] [système/dispositif électronique] ; et

c) Au recueil, sous forme électronique, de preuves [des infractions visées par la présente Convention] [de toute infraction pénale] [des infractions graves].

3. a) Chaque État partie peut se réserver le droit de n'appliquer les mesures visées à l'article 47 de la présente Convention qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions pénales auxquelles il applique les mesures visées à l'article 48. Chaque État partie envisage de limiter une telle réserve de manière à permettre l'application la plus large possible des mesures relatives à la collecte en temps réel des données de trafic.

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

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

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

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

Article 42. Conditions et sauvegardes

1. Chaque État partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le présent chapitre soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits humains et des libertés, notamment des droits et libertés fondamentales découlant de ses obligations au titre du droit international des droits humains, et qui doit intégrer les principes de la proportionnalité, de la nécessité et de la légalité ainsi que la protection de la vie privée et des données à caractère personnel.

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

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

AXE THÉMATIQUE 2

Article 43. Préservation accélérée [de données informatiques stockées] [d'informations électroniques/numériques accumulées]

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

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

3. Chaque État partie adopte les mesures législatives et autres nécessaires pour obliger le gardien des [données informatiques] [informations électroniques/ numériques] ou une autre personne chargée de préserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par sa législation nationale.

4. Les pouvoirs et procédures visés dans le présent article sont régis par les articles 41 et 42 de la présente Convention.

Article 44. Préservation et divulgation partielle accélérées de données de trafic

1. Afin d'assurer la préservation des données de trafic en application de l'article sur la préservation accélérée de [données informatiques] [d'informations électroniques/numériques] stockées, chaque État partie adopte les mesures législatives et autres nécessaires :

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

b) Pour veiller à la divulgation accélérée à son autorité compétente, ou à une personne désignée par cette autorité, d'une quantité suffisante de données de trafic pour pouvoir identifier les fournisseurs de services et la voie par laquelle la communication ou les informations indiquées ont été transmises.

2. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 41 et 42.

Article 45. Injonction de produire

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes, lorsque l'on peut raisonnablement penser qu'il y a ou qu'il y a eu commission d'une infraction pénale, à ordonner :

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

b) À un fournisseur de services offrant des prestations sur son territoire, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 41 et 42.

3. Aux fins du présent article, le terme « données relatives aux abonnés » désigne toute information détenue par un fournisseur de services sous forme [de données informatiques] [d'informations électroniques/numériques] ou sous toute autre forme, se rapportant aux abonnés de ses services, autres que des données de trafic ou de contenu, et permettant d'établir :

a) Le type de service de technologies de l'information et des communications utilisé, les dispositions techniques appliquées à cet égard et la période de service ;

b) L'identité, l'adresse postale ou géographique et le numéro de téléphone de la personne titulaire de l'abonnement, 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 ;

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

Article 46. Perquisition et saisie [d'informations stockées ou traitées électroniquement/numériquement] [de données informatiques stockées]

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes, lorsque l'on peut raisonnablement penser qu'il y a ou qu'il y a eu commission d'une infraction pénale, à perquisitionner ou à accéder d'une façon similaire sur son territoire ou dans sa juridiction :

a) À un [système/dispositif électronique] [système informatique] ou à une partie de celui-ci ainsi qu'aux [données informatiques] [informations électroniques/numériques] qui y sont stockées ; et

b) À un support de stockage [de données informatiques] [d'informations électroniques/numériques] dans lequel pourraient être stockées les [données informatiques] [informations électroniques/numériques] recherchées.

2. Chaque État partie adopte les mesures législatives et autres nécessaires pour que, lorsque ses autorités compétentes, dans le cadre d'une perquisition menée en application des dispositions de l'alinéa a) du paragraphe 1, ont des motifs raisonnables de penser que des [données informatiques] [informations électroniques/numériques] recherchées sont stockées dans un autre [système/dispositif électronique] [système informatique] situé sur son territoire, et que ces [données] [informations] sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, elles soient en mesure d'étendre rapidement la perquisition pour obtenir l'accès à cet autre [système/dispositif électronique] [système informatique] ou aux [données] [informations] qu'il contient.

3. Chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire, sur son

territoire ou dans sa juridiction, des [données informatiques] [informations électroniques/numériques] auxquelles il a été accédé conformément aux paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a) Saisir ou obtenir d'une autre façon un [système/dispositif électronique] [système informatique], ou une partie de celui-ci, ou un support servant à stocker des [données informatiques] [informations électroniques/numériques] ;

b) Réaliser et conserver une copie de ces [données informatiques] [informations électroniques/numériques] au format électronique/numérique ;

c) Préserver l'intégrité des [données informatiques] [informations électroniques/numériques] stockées concernées ;

d) Rendre ces [données informatiques] [informations électroniques/numériques] inaccessibles ou les retirer du [système informatique] [système/dispositif électronique] consulté.

4. Chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne possédant une connaissance spécialisée du fonctionnement du [système/dispositif électronique] [système informatique] en question, du réseau d'information et de télécommunications, ou de leurs éléments constitutifs, ou des mesures appliquées pour protéger les [données informatiques] [informations électroniques/numériques] que contiennent ces dispositifs, de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 à 3 du présent article.

5. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 41 et 42.

Article 47. Collecte en temps réel des données de trafic

1. Chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes, lorsque l'on peut raisonnablement penser qu'il y a ou qu'il y a eu commission d'une infraction pénale, à prendre les mesures suivantes relativement aux données de trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un [système informatique] [système/dispositif électronique] :

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

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

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

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

lesdites données associées à des communications spécifiques transmises sur son territoire.

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

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

4. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 41 et 42.

Article 48. Interception de données de contenu

1. En ce qui concerne un éventail d'infractions graves à définir en droit interne, chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes à prendre les mesures suivantes relativement [aux données de contenu] [aux informations électroniques/numériques, y compris les données de contenu, transmises au moyen de technologies de l'information et des communications] de communications spécifiques transmises sur son territoire au moyen d'un [système informatique] [système/dispositif électronique] :

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

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

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

ii) À prêter aux autorités compétentes son concours et son assistance pour procéder à la collecte ou à l'enregistrement en temps réel ;

de ces [données] [informations].

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

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

4. Les pouvoirs et procédures visés dans le présent article sont conformes aux articles 41 et 42.

Article 49. Admissibilité des preuves électroniques/numériques

Les preuves électroniques/numériques issues ou extraites de dispositifs, d'équipements, de supports électroniques/numériques, de systèmes ou programmes informatiques ou de toutes autres technologies de l'information et des communications ont, dans les procédures pénales, la même valeur probante que les preuves matérielles scientifiques, dès lors qu'elles remplissent les conditions techniques imposées par la législation des États parties concernés.

AXE THÉMATIQUE3

Article 50. Gel, saisie et confiscation du produit du crime

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

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

b) Des biens, matériels ou autres instruments utilisés ou destinés à être utilisés pour les infractions établies conformément à la présente Convention.

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

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

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

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

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

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

8. Chaque État partie peut envisager d'exiger que l'auteur d'une infraction établisse l'origine licite du produit présumé du crime ou d'autres biens confiscables, dans la mesure où cette exigence est conforme aux principes de son droit interne et à la nature des procédures judiciaires et autres.

9. Les dispositions du présent article ne doivent pas être interprétées comme portant atteinte aux droits des tiers de bonne foi.

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

Article 51. Établissement des antécédents judiciaires

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

Article 52. Protection des témoins

1. Chaque État partie prend, dans la limite de ses moyens, des mesures appropriées pour assurer une protection efficace contre des actes éventuels de représailles ou d'intimidation aux témoins qui font un témoignage ou qui, de bonne foi et pour des motifs raisonnables, fournissent des informations concernant des infractions établies conformément à la présente Convention ou coopèrent d'une autre manière avec les services d'enquête ou les autorités judiciaires, et, le cas échéant, à leurs parents et à d'autres personnes qui leur sont proches.

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

a) À établir, pour la protection physique de ces personnes, des procédures visant notamment, selon les besoins et dans la mesure du possible, à leur fournir un

nouveau domicile et à permettre, s'il y a lieu, que les renseignements concernant leur identité et le lieu où elles se trouvent ne soient pas divulgués ou que leur divulgation soit limitée ;

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

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

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

Article 53. Octroi d'une assistance et d'une protection aux victimes

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

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

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

Article 54. Réparation du préjudice

Chaque État partie prend les mesures nécessaires, conformément aux principes de son droit interne, pour donner aux entités ou personnes qui ont subi un préjudice du fait [de l'utilisation des technologies de l'information et des communications à des fins criminelles] [de la cybercriminalité] le droit d'engager une action en justice à l'encontre des responsables dudit préjudice en vue d'obtenir réparation.

Article 55. Mesures propres à renforcer la coopération avec les services de détection et de répression

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

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

i) L'identité, la nature, la composition, la structure, l'emplacement ou les activités des personnes participant aux infractions établies conformément à la présente Convention ;

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

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

b) À fournir une aide factuelle et concrète aux autorités compétentes, qui pourrait contribuer à priver les personnes participant à des infractions établies conformément à la présente Convention de leurs ressources ou du produit du crime.

2. Chaque État partie envisage de prévoir la possibilité, dans les cas appropriés, d'alléger la peine dont est passible un prévenu qui coopère de manière substantielle à

l'enquête ou aux poursuites relatives à une infraction établie conformément à la présente Convention.

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

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

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