Adoption de politiques harmonisées pour le marché des TIC dans les pays ACP

Crime informatique et cybercriminalité:

Loi type relative de la Communauté de développement de l'Afrique australe (SADC)

HIPSSA

Harmonisation des politiques en matière de TIC en Afrique Subsaharienne

Commission européenne

Adoption de politiques harmonisées pour le marché des TIC dans les pays ACP

Crime informatique et cybercriminalité :

Loi type relative de la Communauté de développement de l'Afrique australe (SADC)

HIPSSA

Harmonisation des politiques en matières de TIC en Afrique Subsaharienne

Avis de non-responsabilité

Le présent document a été réalisé avec l'aide financière de l'Union européenne. Les opinions exprimées dans les présentes ne reflètent pas nécessairement la position de l'Union européenne.

Les appellations utilisées et la présentation de matériaux, notamment des cartes, n'impliquent en aucun cas l'expression d'une quelconque opinion de la part de l'UIT concernant le statut juridique d'un pays, d'un territoire, d'une ville ou d'une région donnés, ou concernant les délimitations de ses frontières ou de ses limites. La mention de sociétés spécifiques ou de certains produits n'implique pas qu'ils sont agréés ou recommandés par l'UIT de préférence à d'autres non mentionnés d'une nature similaire.

La version française a été traduite au fin d'information uniquement et ne revêt aucun caractère officiel, seule la version anglaise fait foi.

Avant d'imprimer ce rapport, pensez à l'environnement.

Avant-propos

Les technologies de l'information et de la communication (TIC) sont à la base du processus de mondialisation. Conscients qu'elles permettent d'accélérer l'intégration économique de l'Afrique et donc, d'en renforcer la prospérité et la capacité de transformation sociale, les ministres responsables des communications et des technologies de l'information, réunis sous les auspices de l'Union africaine, ont adopté, en mai 2008, un cadre de référence pour l'harmonisation des politiques et réglementations des télécommunications/TIC, dont la mise en place se faisait d'autant plus nécessaire que les Etats étaient de plus en plus nombreux à adopter des politiques pour libéraliser ce secteur.

La coordination dans l'ensemble de la région est essentielle si l'on veut que les politiques, la législation et les pratiques résultant de la libéralisation dans chaque pays ne freinent pas, par leur diversité, le développement de marchés régionaux compétitifs.

Notre projet d'"Appui à l'harmonisation des politiques en matière de TIC en Afrique subsaharienne" (HIPSSA) cherche à remédier à ce problème potentiel en regroupant et accompagnant tous les pays de la région au sein du Groupe des Etats d'Afrique, des Caraïbes et du Pacifique (ACP). Ces pays formulent et adoptent des politiques, des législations et des cadres réglementaires harmonisés dans le domaine des TIC. Exécuté par l'Union internationale des télécommunications (UIT) sous la coprésidence de l'Union africaine, ce projet est entrepris en étroite collaboration avec les communautés économiques régionales (CER) et les associations régionales de régulateurs qui sont membres de son comité directeur. Un comité de pilotage global constitué de représentants du Secrétariat ACP et de la Direction générale du développement et de la coopération – EuropeAid (DEVCO, Commission européenne) supervise la mise en oeuvre du projet dans son ensemble.

Inscrit dans le cadre du programme ACP sur les technologies de l'information et de la communication (@CP-ICT), le projet est financé par le 9ème Fonds européen de développement (FED), principal vecteur de l'aide européenne à la coopération au service du développement dans les Etats ACP, et cofinancé par l'UIT. La finalité du programme @CT-ICT est d'aider les gouvernements et les institutions ACP à harmoniser leurs politiques dans le domaine des TIC, grâce à des conseils, des formations et des activités connexes de renforcement des capacités, fondés sur des critères mondiaux tout en étant adaptés aux réalités locales.

Pour tous les projets rassembleurs impliquant de multiples parties prenantes, l'objectif est double: créer un sentiment partagé d'appartenance et assurer des résultats optimaux pour toutes les parties. Une attention particulière est prêtée à ce problème, depuis les débuts du projet HIPSSA en décembre 2008. Une fois les priorités communes arrêtées, des groupes de travail réunissant des parties prenantes ont été créés pour agir concrètement. Les besoins propres aux régions ont ensuite été définis, de même que les pratiques régionales pouvant donner de bons résultats, qui ont été comparées aux pratiques et normes établies dans d'autres régions du monde.

Ces évaluations détaillées, qui tiennent compte des spécificités de la sous-région et de chaque pays, ont servi de point de départ à l'élaboration de modèles de politiques et de textes législatifs constituant un cadre législatif dont l'ensemble de la région peut être fier. Il ne fait aucun doute que ce projet servira d'exemple pour les parties prenantes qui cherchent à mettre le rôle de catalyseur joué par les TIC au service de l'accélération de l'intégration économique et du développement socio-économique.

Avant-propos

Je saisis cette occasion pour remercier la Commission européenne et le Secrétariat ACP pour leur soutien financier. Je remercie également la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO), l'Union économique et monétaire ouest-africaine (UEMOA), la Communauté économique des Etats de l'Afrique centrale (CEEAC), la Communauté économique et monétaire de l'Afrique centrale (CEMAC), la Communauté d'Afrique de l'Est (CAE), le Marché commun de l'Afrique orientale et australe (COMESA), la Communauté de développement de l'Afrique australe (SADC), l'Autorité intergouvernementale pour le développement (IGAD) l'Association des régulateurs des communications de l'Afrique australe (CRASA), l'Association des régulateurs de télécommunications d'Afrique centrale (ARTAC), la Commission économique des Nations Unies pour l'Afrique (CEA) et l'Assemblée des régulateurs des télécommunications de l'Afrique de l'Ouest (ARTAO) d'avoir contribué à la réalisation du projet. Sans la volonté politique des pays bénéficiaires, les résultats auraient été bien maigres. Aussi, je tiens à exprimer ma profonde gratitude à tous les gouvernements des pays ACP pour leur détermination, qui a assuré le grand succès de ce projet.

Brahima Sanou
Directeur du BDT

Remerciements

Le présent document constitue l'un des résultats d'une activité régionale organisée dans le cadre du projet HIPSSA ("Appui à l'harmonisation des politiques dans le secteur des TIC en Afrique subsaharienne"), officiellement lancé en décembre 2008 à Addis-Abeba.

En réponse à la fois aux défis et aux possibilités qu'offrent les technologies de l'information et de la communication (TIC) en termes de développement politique, social, économique et environnemental, l'Union internationale des télécommunications (UIT) et la Commission européenne (CE) ont uni leurs forces et signé un accord (projet UIT-CE) destiné à fournir un "Appui pour l'établissement de politiques harmonisées sur le marché des TIC dans les pays ACP", dans le cadre du Programme "ACP-Technologies de l'information et de la communication" (@CP-TIC) financé par le 9ème Fonds européen de développement (FED). Il s'agit du projet UIT-CE-ACP.

Ce projet global UIT-CE-ACP est mené à bien dans le cadre de trois sous-projets distincts adaptés aux besoins spécifiques de chaque région: l'Afrique subsaharienne (HIPSSA), les Caraïbes (HIPCAR) et les Etats insulaires du Pacifique (ICB4PAC).

En tant que membres de la Commission de direction du projet HIPSSA – coprésidée par la Commission de l'Union africaine et l'UIT – le Secrétariat de la Communauté de développement de l'Afrique australe (SADC) et celui de la Communication Regulators' Association of Southern Africa (CRASA) ont fourni conseils et assistance aux consultants, le Professeur Marco Gercke et Mme Judith Tembo, qui ont préparé le projet de document. Ce dernier a été révisé, examiné et validé, avec un large consensus, par les participants lors de l'atelier organisé en collaboration avec les Secrétariats de la CRASA et de la SADC, qui s'est déroulé à Gaborone (Botswana) du 27 février au 3 mars 2012. Il devrait être adopté par les Ministres des pays de la SADC chargés des télécommunications, des postes et des TIC, lors de la réunion qu'ils tiendront à Maurice en novembre 2012.

L'UIT souhaite remercier les délégués des ateliers issus des ministères chargés des TIC et des télécommunications des pays de la SADC, les régulateurs des pays de la CRASA, le milieu universitaire, la société civile, les opérateurs et les organisations régionales, pour l'excellent travail qu'ils ont fourni et l'engagement dans l'élaboration du rapport final, dont ils ont fait preuve afin de produire le contenu. Nous remercions également très sincèrement les Secrétariats de la SADC et de la CRASA pour leurs contributions.

Sans la participation active de l'ensemble de ces parties prenantes, il aurait été impossible d'élaborer un tel document, qui reflète les exigences et les conditions générales de la région de la SADC tout en décrivant les meilleures pratiques internationales.

Les activités ont été mises en œuvre par Mme Ida Jallow, chargée de la coordination des activités en Afrique subsaharienne (Coordonnatrice principale du projet HIPSSA), et M. Sandro Bazzanella, chargé de la gestion de l'ensemble du projet couvrant l'Afrique subsaharienne, les Caraïbes et le Pacifique (Directeur du projet UIT-CE-ACP), avec l'appui de Mme Hiwot Mulugeta, Assistante du projet HIPSSA, et de Mme Silvia Villar, Assistante du projet UIT-CE-ACP. Le travail a été réalisé sous la direction générale de M. Cosmas Zavazava, Chef du Département de l'appui aux projets et de la gestion des connaissances. Le document a été établi sous la supervision directe de M. Jean-François Le Bihan, qui était alors Coordonnateur principal du projet, et ses auteurs ont bénéficié des commentaires de la Division de l'environnement réglementaire et commercial (RME) et de la Division des initiatives spéciales (SIS) du Bureau de développement des télécommunications (BDT) de l'UIT, ainsi que de la Division des applications TIC et de la cybersécurité (CYB) de l'UIT. L'équipe du Service de composition des publications de l'UIT a été chargée de la publication.

Table des matières

Pages

Table des matières

Titre I

TITRE I: PRÉLIMINAIRE

Titre abrégé

1. La présente loi peut être désignée sous le titre "Loi relative au crime informatique et à la cybercriminalité" et entrera en vigueur [le xxx/après sa publication au *Journal officiel*].

Objectif

2. L'objectif d'une loi sur le crime informatique et la cybercriminalité en [indiquer le nom d'un pays] est de criminaliser les crimes liés à l'informatique et aux réseaux et d'enquêter sur ceux-ci.

Définitions

3. (1) "Accès", en relation avec l'Article 4, signifie entrer dans un système informatique.

(2) "Fournisseur d'accès" désigne toute personne physique ou morale qui fournit un service de transmission électronique de données en transmettant des informations fournies par ou à un utilisateur du service dans un réseau de communication, ou qui fournit un accès à un réseau de communication.

(3) "Fournisseur de cache" désigne toute personne physique ou morale fournissant un service de transmission électronique de données par stockage automatique, intermédiaire et temporaire des informations, dans le seul but de rendre plus efficace la transmission des informations aux autres utilisateurs du service à leur demande.

(4) "Enfant" désigne toute personne de moins de dix-huit (18) ans.

(5) "Système d'information" (ou "système informatique") désigne un dispositif ou un groupe de dispositifs interconnectés ou reliés qui, au moyen d'un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions.

(6) "Données informatiques" désigne toute représentation de faits, de concepts, d'informations (textes, sons, vidéos ou images), de codes ou d'instructions lisibles par une machine, dans un format permettant d'être traité par un système informatique, notamment un programme pouvant faire exécuter une fonction à un système informatique.

(7) "Moyen de stockage de données informatiques" désigne tout objet ou support (par exemple, une disquette) à partir duquel les informations peuvent être reproduites, avec ou sans l'aide d'un autre objet ou dispositif.

(8) "Pédopornographie" ou "pornographie infantile" se réfère à tout matériel pornographique décrivant, présentant ou représentant:

(a) un enfant se livrant à des comportements sexuellement explicites;

(b) une personne qui paraît être un enfant se livrant à des comportements sexuellement explicites; ou

(c) des images représentant un enfant se livrant à des comportements sexuellement explicites.

Un pays peut restreindre la criminalisation en n'appliquant pas les cas (b) et (c).

(9) "Infrastructures critiques" désigne les systèmes informatiques, les dispositifs, les réseaux, les programmes informatiques, les données informatiques d'une importance tellement vitale pour le pays que toute incapacité, destruction ou atteinte à l'intégrité de ces systèmes et actifs porterait atteinte à la sécurité, à la sécurité nationale ou économique, à la santé et à la sûreté publiques nationales, ou toute combinaison de ces éléments.

(10) "Dispositifs" désigne, sans s'y limiter:

(a) couper l'alimentation électrique d'un système informatique; et

(b) les éléments de stockage, tels que les disques durs, les cartes mémoire, les disques compacts et les bandes;

(c) les périphériques d'entrée, tels que les claviers, les souris, les pavés tactiles, les scanners et les appareils photo numériques;

(d) les périphériques de sortie, tels que les imprimantes et les écrans.

(11) "Communication électronique" désigne un transfert de signes, de signaux ou de données informatiques de toute nature, transmis en tout ou en partie par câble, par radiocommunication, par ondes électromagnétiques ou par un système de photographie électronique ou à fibres optiques.

(12) "Entraver", en relation avec un système informatique, signifie, sans s'y limiter:

(a) couper l'alimentation électrique d'un système informatique; et

(b) provoquer des interférences électromagnétiques dans un système informatique; et

(c) corrompre un système informatique par quelque moyen que ce soit; et

(d) introduire, transmettre, endommager, effacer, détériorer, altérer ou supprimer des données informatiques.

(13) "Hébergeur" désigne toute personne physique ou morale qui fournit un service de transmission électronique de données en stockant les informations fournies par l'utilisateur du service.

(14) "Lien hypertexte" désigne une caractéristique ou une propriété d'un élément tel qu'un symbole, un mot, une phrase ou une image qui contient des informations sur une autre source et qui renvoie à et affiche un autre document lorsqu'elle est exécutée.

(15) "Fournisseur de liens hypertextes" désigne toute personne physique ou morale qui fournit un ou plusieurs liens hypertexte.

(16) "Interception" inclut, sans s'y limiter, l'acquisition, la visualisation et la capture de toute communication de données informatiques, que ce soit de manière câblée, sans fil, électronique, optique, magnétique, orale ou par tout autre moyen durant la transmission, à l'aide d'un dispositif technique.

(17) "Courriers électroniques multiples" désigne tout message électronique, notamment courriel et messagerie instantanée, envoyé à plus de [mille] destinataires.

(18) "Contenu raciste et xénophobe" désigne tout contenu, y compris, sans s'y limiter, toute image, tout enregistrement audio-vidéo ou toute autre représentation d'idées ou de théories qui préconisent, promeuvent ou encouragent la haine, la discrimination ou la violence contre tout individu ou groupe d'individus, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments.

(19) "Outil de criminalistique à distance" désigne un outil d'enquête (y compris logiciel ou équipement) installé ou lié à l'ensemble ou une partie d'un système informatique et utilisé pour effectuer des tâches incluant, sans s'y limiter, l'enregistrement des frappes ou la transmission d'une adresse IP.

(20) "Saisir" signifie:

(a) activer tout système informatique et moyen de stockage des données informatiques sur site;

(b) faire et conserver une copie des données informatiques, en utilisant notamment l'équipement sur site;

(c) maintenir l'intégrité de ces données informatiques stockées;

(d) rendre inaccessible ou retirer les données informatiques du système informatique auquel on a accédé;

(e) sortir sur imprimante les données informatiques; ou

(f) saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un moyen de stockage des données informatiques.

(21) "Fournisseur de services Internet" désigne toute personne physique ou morale qui fournit aux utilisateurs les services mentionnés aux Articles 28-33 des présentes.

(22) "Données relatives au trafic" désigne les données informatiques:

(a) ayant trait à une communication passant par un système informatique; et

(b) générées par un système informatique en tant qu'éléments de la chaîne de communication; et

(c) indiquant l'origine, la destination, l'itinéraire, l'heure, la taille et la durée de la communication, ou le type de services sous-jacents.

(23) "Objet" désigne, sans s'y limiter:

(a) un système informatique ou une partie d'un système informatique;

(b) un autre système informatique, si

  (i) les données informatiques de ce système informatique sont disponibles sur le premier système informatique perquisitionné, et

  (ii) il existe des motifs raisonnables de croire que les données informatiques

(c) un moyen de stockage de données informatiques.

(24) "Utiliser" désigne:

(a) le développement d'un logiciel de criminalistique à distance;

(b) l'adoption d'un logiciel de criminalistique à distance; et

(c) l'achat d'un logiciel de criminalistique à distance.

Titre II

TITRE II: INFRACTIONS

Accès illégal

4. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, accède intentionnellement à l'ensemble ou à une partie d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Présence illégale

5. (1) Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, reste intentionnellement connectée à l'ensemble ou une partie d'un système informatique, ou qui continue d'utiliser un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

(2) Un pays peut décider de ne pas criminaliser la connexion non autorisée si d'autres recours efficaces existent. Un pays peut également imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête.

Interception illégale

6. (1) Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, intercepte intentionnellement, par des moyens techniques:

(a) toute transmission non publique vers, de ou au sein d'un système informatique; ou

(b) des émissions électromagnétiques provenant d'un système informatique,

commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

(2) Un pays peut décider qu'il y a infraction si elle est commise dans une intention malhonnête, ou en rapport avec un système informatique connecté à un autre système informatique, ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique.

Atteinte à l'intégrité des données

7. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, réalise intentionnellement l'un des actes suivants:

(a) endommagement ou détérioration de données informatiques; ou

(b) suppression de données informatiques; ou

(c) altération de données informatiques; ou

(d) fait de rendre les données informatiques dénuées de sens, inutiles ou inopérantes; ou

(e) obstruction, interruption ou interférence avec l'utilisation légale des données informatiques; ou

(f) obstruction, interruption ou interférence avec toute personne dans l'utilisation légale de données informatiques; ou

(g) refus de l'accès aux données informatiques à toute personne ayant le droit d'y accéder,

commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Espionnage des données

8. (1) Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, obtient intentionnellement, pour elle-même ou un tiers, des données informatiques qui ne lui sont pas destinées et qui sont spécialement protégées contre l'accès non autorisé, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

(2) Un pays peut limiter la criminalisation à certaines catégories de données informatiques.

Atteinte à l'intégrité du système

9. (1) Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime:

(a) entrave ou porte atteinte au fonctionnement d'un système informatique; ou

(b) entrave ou porte atteinte à une personne qui utilise ou exploite légalement un système informatique,

commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

(2) Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, entrave ou porte atteinte intentionnellement à un système informatique exclusivement réservé aux opérations des infrastructures critiques ou, s'il n'est pas exclusivement réservé aux opérations des infrastructures critiques, un système utilisé dans les opérations des infrastructures critiques, de sorte que cela affecte cette utilisation ou lesdites infrastructures, est passible d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Dispositifs illégaux

10 (1) Une personne commet une infraction si:

(a) sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, elle produit, vend, obtient pour utilisation, importe, exporte, distribue ou rend autrement disponible:

(i) un dispositif, notamment un programme informatique, conçu ou adapté pour commettre l'une des infractions définies par d'autres dispositions du Titre II de la présente loi; ou

(ii) un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'il soit utilisé par quiconque pour commettre une infraction définie par d'autres dispositions du Titre II de la présente loi; ou

(b) cette personne a en sa possession un élément mentionné à l'alinéa (i) ou (ii) avec l'intention qu'il soit utilisé par un tiers pour commettre une infraction telle que définie par d'autres dispositions du Titre II de la

présente loi, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.

(2) Cette disposition ne saurait être interprétée 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 aux autres dispositions du Titre II de la présente loi, comme dans le cas de tests autorisés ou de protection d'un système informatique.

(3) Un pays peut décider de pas criminaliser les dispositifs illégaux ou de limiter la criminalisation aux dispositifs énumérés dans un tableau.

Falsification informatique

11. (1) Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, introduit, altère, efface ou supprime des données informatiques de manière intentionnelle et engendre ainsi des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques, que ces données soient directement lisibles et intelligibles ou non, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

(2) Si l'infraction susmentionnée est commise en envoyant des courriers électroniques multiples à partir ou au moyen de systèmes informatiques, la sanction sera une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Fraude informatique

12. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque intentionnellement la perte d'un bien pour un tiers d'une des manières suivantes:

(a) introduction, altération, effacement ou suppression des données informatiques;

(b) atteinte au fonctionnement d'un système informatique,

dans l'intention frauduleuse ou malhonnête d'obtenir, sans qu'elle n'y ait droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Pédopornographie ou pornographie infantile

13. (1) Une personne qui, de manière intentionnelle et sans motif ou justification légitime:

(a) produit de la pornographie mettant en scène des enfants à des fins de diffusion par l'intermédiaire d'un système informatique;

(b) offre ou met à disposition, via un système informatique, des contenus pédopornographiques;

(c) diffuse ou transmet via un système informatique des contenus pédopornographiques;

(d) se procure et/ou obtient des contenus pédopornographiques pour elle-même ou un tiers, via un système informatique;

(e) possède des contenus pédopornographiques sur un système informatique ou un moyen de stockage des données informatiques; et

(f) obtient en connaissance de cause l'accès, via les technologies de l'information et de la communication, à des contenus pédopornographiques,

commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

(2) Si la personne prouve que les contenus pornographiques servent uniquement à des fins de répression, cela constitue une décharge face à une accusation formulée au titre des paragraphes (1)(b) à (1)(f).

Pornographie

14. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, met intentionnellement des contenus pornographiques à disposition d'un ou de plusieurs enfants, via un système informatique, ou facilite l'accès des enfants à des contenus pornographiques via un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Infractions liées à l'identité

15. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime, ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Contenu raciste et xénophobe

16. Une personne qui, de manière intentionnelle, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime:

(a) produit des contenus racistes et xénophobes à des fins de diffusion par l'intermédiaire d'un système informatique;

(b) offre ou met à disposition, via un système informatique, des contenus racistes et xénophobes;

(c) diffuse ou transmet, via un système informatique, des contenus racistes et xénophobes,

commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Insulte à caractère raciste et xénophobe

17. Une personne qui, de manière intentionnelle et sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, insulte publiquement, via un système informatique:

(a) des personnes au motif qu'elles appartiennent à un groupe se distinguant par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments; ou

(b) un groupe de personnes se distinguant par l'une ou l'autre de ces caractéristiques,

commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Négation du génocide et des crimes contre l'humanité

18. Une personne qui, de manière intentionnelle et sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, diffuse ou met autrement à disposition du public des contenus qui nient, minimisent ouvertement, approuvent ou justifient des actes constituant un génocide ou un crime contre l'humanité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

SPAM

19. (1) Une personne qui, de manière intentionnelle et sans motif ou justification légitime:

(a) déclenche intentionnellement la transmission de courriers électroniques multiples à partir ou via un système informatique; ou

(b) utilise un système informatique protégé pour relayer ou retransmettre des courriers électroniques multiples, dans l'intention de tromper ou d'induire en erreur, quant à l'origine de ces messages, les destinataires, ou tout prestataire de services de courrier électronique ou de services Internet; ou

(c) falsifie matériellement les informations se trouvant dans les en-têtes des messages électroniques multiples et déclenche intentionnellement la transmission de ces messages,

commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

(2) Un pays peut restreindre la criminalisation concernant la transmission de courriers électroniques multiples dans le cadre de relations clients ou commerciales.

Divulgation des détails d'une enquête

20. Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue, ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle:

(a) le fait qu'une injonction ait été émise; ou

(b) toute action réalisée aux termes de l'injonction; ou

(c) toute donnée collectée ou enregistrée aux termes de l'injonction,

commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

Refus d'autoriser l'assistance

21. (1) Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux Articles 25 à 27, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée], ou d'une amende maximale de [montant], ou les deux.

(2) Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.

Harcèlement au moyen de communications électroniques

22. Toute personne qui initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.

Titre III

TITRE III: JURISDICTION

Jurisdiction

23. La présente loi s'applique à tout acte (infraction) ou omission commis:

(a) sur le territoire de [État prenant les dispositions]; ou

(b) sur un bateau ou un avion immatriculé en [État prenant les dispositions]; ou

(c) par un citoyen de [Etat prenant les dispositions] en dehors de la juridiction de tout pays; ou

(d) par un citoyen de [Etat prenant les dispositions] en dehors du territoire de [Etat prenant les dispositions], si le comportement de la personne constitue également une infraction aux termes de la loi du pays dans lequel ladite infraction est commise.

TITRE IV: PREUVE ÉLECTRONIQUE

Recevabilité des preuves électroniques

24. Dans les procédures relatives à une infraction à une loi de [État prenant les dispositions], le fait que la preuve ait été générée par un système informatique n'empêche pas en soi que cette preuve soit admissible.

Titre V

TITRE V: DROIT PROCÉDURAL

Perquisition et saisie

25. (1) Si un [juge ou magistrat] est convaincu, sur la base d'une demande effectuée par un agent [des forces de l'ordre] [de police] appuyée par [des informations obtenues sous serment] [une déclaration sous serment], qu'il existe de bonnes raisons de [suspecter] [croire] qu'il peut exister dans un lieu un objet ou des données informatiques:

(a) pouvant être jugés importants pour servir de preuve à une infraction; ou

(b) ayant été obtenus par une personne suite à une infraction,

le [juge] [magistrat] [peut] [doit] émettre un mandat autorisant un agent [des forces de l'ordre] [de police], avec toute l'assistance pouvant être nécessaire, à entrer dans le lieu pour perquisitionner et saisir l'objet ou les données informatiques en question, notamment perquisitionner ou accéder de manière similaire à:

(i) un système informatique ou partie d'un tel système et les données informatiques qui y sont stockées; et

(ii) un moyen de stockage des données dans lequel les données informatiques peuvent être stockées

(2) Si un agent [des forces de l'ordre] [de police] qui entreprend une perquisition sur la base de l'Article 25 (1) a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, l'agent sera en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système.

(3) Un agent [des forces de l'ordre] [de police] qui entreprend une perquisition a le pouvoir de saisir ou d'obtenir de façon similaire les données informatiques auxquelles il a accédé en vertu des paragraphes 1 ou 2.

Assistance

26. (1) Toute personne n'étant pas suspectée d'un crime ou autrement exemptée d'une obligation de se soumettre à un tel ordre, mais qui a connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qui s'y trouvent et qui font l'objet d'une perquisition aux termes de l'Article 26, doit autoriser et assister la personne habilitée à effectuer la perquisition, si cela est requis et exigé de manière raisonnable, à:

(a) fournir des informations permettant de prendre les mesures mentionnées à l'Article 26;

(b) accéder et utiliser un système informatique ou un moyen de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système;

(c) obtenir et copier ces données informatiques;

(d) utiliser l'équipement pour faire des copies; et

(e) obtenir un résultat intelligible d'un système informatique dans un format simple, admissible à des fins de procédures légales.

Titre V

Injonction de produire

27. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], que des données informatiques spécifiées, qu'une version imprimée ou que d'autres informations font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle ou d'une procédure pénale, il peut ordonner:

(a) à une personne sur le territoire de [Etat prenant les dispositions] qui contrôle un système informatique, de produire, à partir du système, des données informatiques spécifiées ou une version imprimée ou une autre forme de sortie intelligible de ces données; ou

(b) à un fournisseur de services Internet en [Etat prenant les dispositions] de produire des informations sur les personnes qui sont abonnées au service ou qui utilisent autrement ce service.

Conservation rapide

28. Si un agent [des forces de l'ordre] [de police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne de veiller à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur demande, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.

Divulgation partielle des données de trafic

29. Si un agent [des forces de l'ordre] [de police] est convaincu que les données stockées dans un système informatique font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il peut, en envoyant une notification écrite à une personne qui contrôle le système informatique, exiger de cette personne qu'elle divulgue [suffisamment] de données de trafic [pertinentes] associées à une communication spécifique, afin d'identifier:

(a) les fournisseurs de services Internet; et/ou

(b) l'itinéraire de la communication.

Titre V

Collection of traffic data

30. (1) Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe des motifs raisonnables de [suspecter] [croire] que les données de trafic associées à une communication spécifiée sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] ordonner à une personne qui contrôle lesdites données de:

(a) collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifique; ou

(b) permettre à un agent [des forces de l'ordre] [de police] spécifié de collecter ou enregistrer ces données et l'assister dans cette tâche.

(2) Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que les données de trafic sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifiée à l'aide de moyens techniques.

Interception des données relatives au contenu

31. (1) Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que le contenu d'une communication électronique est raisonnablement nécessaire aux besoins d'une enquête criminelle, il [peut] [doit]:

(a) ordonner à un fournisseur de services Internet dont les services sont disponibles en [Etat prenant les dispositions], à l'aide de moyens techniques, de collecter ou d'enregistrer des données de contenu associées à des communications spécifiées transmises par l'intermédiaire d'un système informatique, ou de permettre ou d'assister les autorités compétentes dans la collecte ou l'enregistrement de ces données; ou

(b) autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer lesdites données, à l'aide de moyens techniques.

Outil de criminalistique

32. (1) Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent [des forces de l'ordre] [de police] à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes:

(a) le suspect de l'infraction, si possible avec ses nom et adresse; et
(b) une description du système informatique ciblé; et
(c) une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; et
(d) les raisons justifiant la nécessité de l'utilisation.

(2) Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, ait lieu à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner:

(a) le moyen technique utilisé ainsi que la date et l'heure de l'application;
(b) l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et
(c) toute information obtenue.

Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès non autorisé.

(3) La durée de l'autorisation mentionnée à l'Article 32 (1) est limitée à [3 mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser.

(4) L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect.

(5) Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'Article 25.

(6) Si nécessaire, un agent de police peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation.

(7) [Liste des infractions]

(8) Un pays peut décider de ne pas mettre en oeuvre l'Article 33.

TITRE VI: RESPONSABILITÉ

Non-obligation de surveillance

33. Lors de la fourniture des services évoqués dans ce chapitre, un prestataire de services Internet n'a pas d'obligation générale de surveiller les données qu'il transmet ou qu'il stocke, ni de rechercher des faits ou circonstances indiquant une activité illégale.

Le [ministre] peut, sous réserve des dispositions de toute autre loi, prescrire des procédures pour les prestataires de service afin de:

(a) signaler aux autorités publiques compétentes des activités prétendument illégales ou des informations fournies par les destinataires de leurs services; et

(b) communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services.

Fournisseur d'accès

34. (1) Un fournisseur d'accès n'est pénalement pas responsable lorsqu'il fournit l'accès et transmet des informations, à la condition qu'il:

(a) ne déclenche pas la transmission;

(b) ne sélectionne pas le destinataire de la transmission; ou

(c) ne sélectionne pas ou ne modifie pas les informations contenues dans la transmission.

(2) Les actes de transmission et de fourniture d'accès mentionnés au paragraphe 1 incluent le stockage automatique, intermédiaire et transitoire des informations transmises dans la mesure où il a lieu à la seule fin d'effectuer la transmission dans le réseau de communication, à condition que lesdites informations ne soient pas stockées au-delà du temps raisonnablement nécessaire à la transmission.

Hébergeur

35. (1) Un hébergeur n'est pas responsable pénalement des informations stockées à la demande d'un utilisateur du service, à condition que:

(a) l'hébergeur retire ou désactive rapidement l'accès aux informations après avoir reçu de la part d'une autorité publique ou d'un tribunal quelconque une injonction de retirer des informations illégales spécifiques qu'il stocke; ou

(b) l'hébergeur, lorsqu'il a pris connaissance ou conscience d'informations illégales spécifiques stockées autrement que par une injonction émanant des pouvoirs publics, informe rapidement les pouvoirs publics pour leur permettre d'évaluer la nature des informations et, si nécessaire, d'émettre une injonction pour en retirer le contenu.

(2) Le paragraphe 1 ne s'applique pas lorsque l'utilisateur du service agit sous l'autorité ou le contrôle de l'hébergeur.

(3) Si l'hébergeur retire le contenu après avoir reçu une injonction conforme au paragraphe 1, il est exempté de l'obligation contractuelle auprès de son client d'assurer la disponibilité du service.

Fournisseur de cache

36. Un fournisseur de cache n'est pas responsable pénalement du stockage automatique, intermédiaire et temporaire des informations, exécuté à la seule fin de rendre plus efficace la transmission des informations aux autres utilisateurs du service, à leur demande, à condition que:

(a) le fournisseur de cache ne modifie pas les informations;

(b) le fournisseur de cache se conforme aux conditions d'accès aux informations;

(c) le fournisseur de cache se conforme aux règles relatives à la mise à jour des informations, spécifiées d'une manière largement reconnue et utilisée par le secteur;

(d) le fournisseur de cache ne porte pas atteinte à l'utilisation légale des technologies, largement reconnues et utilisées par le secteur, pour obtenir des données sur l'utilisation des informations;

(e) le fournisseur de cache agit rapidement pour retirer ou désactiver l'accès aux informations qu'il a stockées, après avoir effectivement eu connaissance du fait que les informations à la source initiale de la transmission ont été supprimées du réseau, ou que l'accès à celui-ci a été désactivé, ou qu'un tribunal ou une autorité administrative a ordonné un tel retrait ou une telle désactivation.

Fournisseur de liens hypertextes

37. Un fournisseur de services Internet qui autorise l'accès aux informations fournies par un tiers en donnant un lien hypertexte électronique n'est pas responsable desdites informations si:

(a) le fournisseur de services Internet supprime ou empêche rapidement l'accès aux informations après avoir reçu une injonction de retirer le lien d'une autorité publique ou d'un tribunal quelconque; et

(b) le fournisseur de services Internet, lorsqu'il a pris connaissance ou conscience autrement que par une injonction émanant d'une autorité publique, d'informations illégales spécifiques stockées, informe rapidement les pouvoirs publics pour leur permettre d'évaluer la nature des informations et, si nécessaire, d'ordonner le retrait du contenu.

Fournisseur de moteurs de recherche

38. Un fournisseur gérant un moteur de recherche qui, de manière automatique ou sur la base des entrées effectuées par autrui, crée un index des contenus en ligne ou met à disposition des outils électroniques pour rechercher les informations fournies par des tiers, n'est pas responsable des résultats de recherche, à condition qu'il:

1. ne déclenche pas la transmission; et
2. ne sélectionne pas le destinataire de la transmission; et
3. ne sélectionne pas ou ne modifie pas les informations contenues dans la transmission.

Union internationale des télécommunications
Bureau de développement des télécommunications (BDT)
Place des Nations
CH-1211 Genève

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Genève, 2013