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

Cybercriminalité:

Modèles de lignes directrices politiques et de textes législatifs

HIPCAR

Harmonisation des politiques, législations et procédures réglementaires en matière de TIC dans les Caraïbes

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

Cybercriminalité:

Modèles de lignes directrices politiques et de textes législatifs

HIPCAR

Harmonisation des politiques, législations et procédures réglementaires en matière de TIC dans les Caraïbes

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. Le présent Rapport n'a pas fait l'objet d'une révision rédactionnelle.

Merci de penser à l'environnement avant d'imprimer ce rapport.

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 la région des Caraïbes et donc d'en renforcer la prospérité et la capacité de transformation sociale, le Marché et l'économie uniques de la Communauté des Caraïbes (CARICOM) ont mis au point une stratégie en matière de TIC axée sur le renforcement de la connectivité et du développement.

La libéralisation du secteur des télécommunications est l'un des éléments clés de cette stratégie. 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 d'un marché régional.

Le projet "Renforcement de la compétitivité dans la région Caraïbes grâce à l'harmonisation des politiques, de la législation et des procédures réglementaires dans le secteur des TIC" (HIPCAR) cherche à remédier à ce problème potentiel en regroupant et accompagnant les 15 pays des Caraïbes 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), ce projet est entrepris en étroite collaboration avec l'Union des télécommunications des Caraïbes (CTU), qui en préside le comité directeur. Un comité de pilotage global, constitué de représentants du Secrétariat de l'ACP et de la Direction générale du développement et de la coopération – EuropeAid (DEVCO, Commission européenne), supervise la mise en œuvre du projet dans son ensemble.

Inscrit dans le cadre du programme ACP sur les technologies de l'information et de la communication (@CP-ICT), ce 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 HIPCAR 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 à la région 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 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 à d'autres régions qui, elles aussi, 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.

Je saisis cette occasion pour remercier la Commission européenne et le Secrétariat ACP pour leur soutien financier. Je remercie également le Secrétariat de la Communauté des Caraïbes (CARICOM) ainsi que celui de l'Union des télécommunications des Caraïbes (CTU) 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 représente l'achèvement des activités régionales réalisées dans le cadre du projet HIPCAR «Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures» (Amélioration de la compétitivité dans les Caraïbes au travers de l'harmonisation des politiques, législations et procédures réglementaires en matière de TIC), officiellement lancé en décembre 2008 à Grenade.

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: les Caraïbes (HIPCAR), l'Afrique subsaharienne (HIPSSA) et les Etats insulaires du Pacifique (ICB4PAC).

Le comité de pilotage du projet HIPCAR, présidé par l'Union des télécommunications des Caraïbes (CTU), a fourni conseils et assistance à une équipe de consultants incluant Dr. Marco Gercke et Mme. Pricilla Banner. Le document a ensuite été révisé, finalisé et adopté par un large consensus des participants lors des deux ateliers de consultation du Groupe de travail du projet HIPCAR qui se sont déroulés à Sainte-Lucie du 8 au 12 mars 2010 et à Saint-Kitts-et-Nevis du 19 au 22 juillet 2010 (voir Annexes). Les notes explicatives du modèle de texte législatif incluses dans ce document ont été préparées par Dr. Marco Gercke et traitent, entre autres, des points soulevés lors du second atelier.

L'UIT souhaite remercier tout particulièrement les délégués des ateliers des ministères caribéens chargés des TIC et des télécommunications, des ministères de la Justice et des affaires juridiques et autres organismes du secteur public, les régulateurs, le milieu universitaire, la société civile, les opérateurs et les organisations régionales, pour l'excellent travail et l'engagement dont ils ont fait preuve afin de produire le contenu du présent rapport. Cette large base de participation du secteur public représentant différents secteurs a permis au projet de bénéficier d'un échantillon représentatif d'opinions et d'intérêts. Nous remercions également tout aussi sincèrement le Secrétariat de la Communauté des Caraïbes (CARICOM) et de l'Union des télécommunications des Caraïbes (CTU) par leurs contributions.

Sans la participation active de l'ensemble de ces parties prenantes, la réalisation de ce document aurait été impossible sous cette forme, qui reflète les exigences et conditions générales de la région des Caraïbes tout en représentant les meilleures pratiques internationales.

Les activités ont été mises en œuvre par Mme Kerstin Ludwig, chargée de la coordination des activités dans les Caraïbes (Coordonnatrice du projet HIPCAR) 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 Nicole Morain, Assistante du projet HIPCAR, 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. Les auteurs du document ont bénéficié des commentaires de la Division applications TIC et cybersécurité (CYB) du Bureau de développement des télécommunications (BDT) de l'UIT. Ils ont aussi bénéficié de l'appui de M. Philip Cross, Représentant de zone de l'UIT pour les Caraïbes. L'équipe du Service de composition des publications de l'UIT a été chargée de la publication.

Table des Matières

Introduction

1.1. Le projet HIPCAR – objectifs et bénéficiaires

Le projet HIPCAR[1] a été officiellement lancé dans les Caraïbes par la Commission européenne (CE) et l'Union internationale des télécommunications (UIT) en décembre 2008, en étroite collaboration avec le Secrétariat de la Communauté des Caraïbes (CARICOM) et l'Union des télécommunications des Caraïbes (CTU). Il fait partie intégrante d'un projet-cadre, le projet UIT-CE-ACP, qui englobe également les pays de l'Afrique subsaharienne et du Pacifique.

L'objectif du projet HIPCAR consiste à aider les pays du CARIFORUM[2] à harmoniser leurs politiques, leur législation et leurs procédures réglementaires en matière de technologies de l'information et de la communication (TIC), de façon à créer un environnement favorable au développement et à la connectivité des TIC, faciliter l'intégration des marchés, favoriser l'investissement dans l'amélioration des capacités et des services liés aux TIC et améliorer la protection des intérêts des consommateurs de TIC dans l'ensemble de la région. L'objectif final du projet est d'accroître la compétitivité et le développement socio-économique et culturel dans la région des Caraïbes au travers des TIC.

Conformément à l'article 67 du Traité révisé de Chaguaramas, le projet HIPCAR peut être considéré comme une partie intégrante des efforts de cette région pour développer le marché et l'économie uniques de la CARICOM (CSME) au travers de la libéralisation progressive de son secteur des services liés aux TIC. Le projet apporte également son concours au Programme de connectivité de la CARICOM et aux engagements de la région pris dans le cadre du Sommet mondial sur la société de l'information (SMSI), de l'Accord général sur le commerce des services de l'Organisation mondiale du commerce (AGCS-OMC) et des Objectifs du Millénaire pour le développement (OMD). Il est également directement lié à la promotion de la compétitivité et à un meilleur accès aux services dans le contexte d'engagements découlant de traités tels que l'Accord de partenariat économique (APE) des États du CARIFORUM avec l'Union européenne.

Les pays bénéficiaires du projet HIPCAR incluent Antigua-et-Barbuda, les Bahamas, la Barbade, le Belize, le Commonwealth de la Dominique, la République dominicaine, la Grenade, le Guyana, Haïti, la Jamaïque, Saint-Kitts-et-Nevis, Sainte-Lucie, Saint-Vincent-et-les-Grenadines, le Suriname et Trinité-et-Tobago.

1.2. Comité de pilotage du projet et groupes de travail

Le projet HIPCAR a créé un Comité de pilotage du projet destiné à lui fournir les conseils et le contrôle nécessaires. Le Comité de pilotage comprend notamment des représentants du Secrétariat de la Communauté des Caraïbes (CARICOM), de l'Union des télécommunications des Caraïbes (CTU), de l'Autorité des télécommunications de la Caraïbe orientale (ECTEL), de l'Association des entreprises nationales de télécommunication des Caraïbes (CANTO), de la Communauté virtuelle des acteurs des TIC de la Caraïbe (CIVIC) et de l'Union internationale des télécommunications (UIT). Organisations (CANTO), Caribbean ICT Virtual Community (CIVIC), and International Telecommunication Union (ITU).

---

1 Le titre complet du projet HIPCAR est «Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures» (Amélioration de la compétitivité dans les Caraïbes au travers de l'harmonisation des politiques, législations et procédures réglementaires en matière de TIC). Ce projet fait partie d'un projet-cadre, le projet UIT-CE-ACP, réalisé à l'aide d'un financement de l'Union européenne fixé à 8 millions d'euros et d'un complément de 500 000 dollars de l'UIT. Il est mis en œuvre par l'Union internationale des télécommunications (UIT) en collaboration avec l'Union des télécommunications des Caraïbes (CTU) et avec la participation d'autres organisations de la région. (voir www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html).

2 Le CARIFORUM est une organisation régionale composée de quinze pays indépendants de la région des Caraïbes (Antigua-et-Barbuda, Bahamas, Barbade, Belize, Dominique, République dominicaine, Grenade, Guyana, Haïti, Jamaïque, Saint-Kitts-et-Nevis, Sainte-Lucie, Saint-Vincent-et-les-Grenadines, Suriname et Trinité-et-Tobago). Ces États sont tous signataires des conventions ACP–CE.

Afin de garantir la contribution des parties prenantes et la pertinence du projet pour chaque pays, des Groupes de travail pour le projet HIPCAR ont également été mis en place. Les membres de ces Groupes de travail sont désignés par les gouvernements nationaux et incluent des spécialistes d'organisations dédiées aux TIC, de la justice et des affaires juridiques et d'autres organismes du secteur public, de régulateurs nationaux, de points focaux nationaux TIC et des personnes chargées d'élaborer la législation nationale. Cette large base de participation du secteur public représentant différents secteurs a permis au projet de bénéficier d'un échantillon représentatif d'opinions et d'intérêts. Les Groupes de travail comprennent également des représentants d'organismes régionaux compétents (Secrétariat de la CARICOM, CTU, ECTEL et CANTO) et des observateurs d'autres entités intéressées de la région (par ex., la société civile, le secteur privé, les opérateurs, les universitaires, etc.).

Les Groupes de travail ont été chargés de couvrir les deux domaines de travail suivants:

1. *Politiques en matière de TIC et cadre législatif sur les questions de la société de l'information*, qui comporte six sous-domaines: commerce électronique (transactions et preuves), respect de la vie privée et protection des données, interception de communications, cybercriminalité et accès à l'information publique (liberté d'information).
2. *Politiques en matière de TIC et cadre législatif sur les télécommunications*, qui comporte trois sous-domaines: l'accès/le service universels, l'interconnexion et l'octroi de licences dans un contexte de convergence.

Les rapports des Groupes de travail publiés dans cette série de documents s'articulent autour de ces deux principaux domaines de travail.

1.3. Mise en œuvre et contenu du projet

Les activités du projet ont débuté par une table ronde de lancement, organisée à Grenade les 15 et 16 décembre 2008. À ce jour, tous les pays bénéficiaires du projet HIPCAR, à l'exception de Haïti, ainsi que les organisations régionales partenaires du projet, les organismes de réglementation, les opérateurs, les universitaires et la société civile, ont activement participé aux événements du projet notamment, outre le lancement du projet à Grenade, à des ateliers régionaux à Trinité-et-Tobago, à Sainte-Lucie, à Saint-Kitts-et-Nevis, au Suriname et à la Barbade.

Les activités de fond du projet sont menées par des équipes d'experts régionaux et internationaux en collaboration avec les membres du Groupe de travail et sont axées sur les deux domaines de travail mentionnés ci-dessus.

Pendant le stade I du projet, qui vient de se terminer, le projet HIPCAR a:

1. Entrepris des évaluations de la législation existante des pays bénéficiaires par rapport aux bonnes pratiques internationales et dans le cadre de l'harmonisation à l'échelle de la région; et
2. Rédigé des modèles de lignes directrices politiques et de textes législatifs dans les domaines de travail cités ci-dessus et à partir desquels les politiques, la législation/les réglementations nationales en matière de TIC peuvent être développées.

Ces propositions devront être validées ou approuvées par la CARICOM/CTU et par les autorités nationales de la région pour constituer la base de la prochaine phase du projet.

Le stade II du projet HIPCAR a pour but de fournir aux pays bénéficiaires intéressés, une assistance pour la transposition des modèles cités ci-dessus dans des politiques et dans la législation nationales en matière de TIC adaptées à leurs exigences, aux circonstances et à leurs priorités spécifiques. Le projet HIPCAR a réservé des fonds pour se permettre de répondre aux demandes d'assistance technique de ces pays, y compris pour le renforcement des capacités, nécessaire à cette fin.

1.4. Vue d'ensemble des six modèles de lignes directrices politiques et de textes législatifs du projet HIPCAR traitant de questions relatives à la société de l'information

Partout dans le monde et dans les Caraïbes, les pays cherchent les moyens d'élaborer des cadres juridiques qui tiennent compte des besoins des sociétés de l'information en vue de mettre à profit l'ubiquité croissante de la Toile mondiale pour s'en servir de canal de fourniture de services, en garantissant un environnement sûr et la puissance de traitement des systèmes d'information pour augmenter l'efficacité et l'efficience des entreprises.

La société de l'information repose sur le principe d'un accès à l'information et aux services et sur l'utilisation de systèmes de traitement automatisés pour améliorer la fourniture de services aux marchés et aux personnes *partout dans le monde*. Pour les utilisateurs autant que pour les entreprises, la société de l'information en général et la disponibilité des technologies de l'information et de la communication (TIC) offrent des occasions uniques. Les impératifs fondamentaux du commerce restant inchangés, la transmission immédiate de cette information commerciale favorise l'amélioration des relations commerciales. Cette facilité d'échange de l'information commerciale introduit de nouveaux paradigmes: en premier lieu, lorsque l'information est utilisée pour soutenir des transactions liées à des biens physiques et à des services traditionnels et en second lieu, lorsque l'information elle-même est la principale marchandise échangée.

La société dans son ensemble et les pays en développement, en particulier, tirent des TIC et des nouveaux services en réseau un certain nombre d'avantages. Les applications TIC (cybergouvernance, commerce électronique, cyberenseignement, cybersanté, cyberenvironnement, etc.), vecteurs efficaces de la fourniture d'une large gamme de services de base dans les régions éloignées et les zones rurales, sont considérées comme des facteurs de développement. Elles peuvent faciliter la réalisation des objectifs du Millénaire pour le développement, en luttant contre la pauvreté et en améliorant les conditions sanitaires et environnementales des pays en développement. Un accès sans entrave à l'information peut renforcer la démocratie, le flux de l'information échappant au contrôle des autorités nationales (comme cela fût le cas, par exemple, en Europe de l'Est). Sous réserve d'adopter une bonne démarche, de se situer dans un contexte approprié et d'utiliser des processus de mise en œuvre adéquats, les investissements en faveur des applications et des outils TIC permettent d'améliorer la productivité et la qualité.

Cependant, le processus de transformation s'accompagne de défis, le cadre juridique existant ne couvrant pas nécessairement les demandes spécifiques d'un environnement technique en mutation rapide. Dans les cas où l'information soutient les échanges de biens et de services traditionnels, il est nécessaire de clarifier la façon dont les postulats commerciaux traditionnels se réalisent. Dans le cas où l'information est le bien échangé, il convient de protéger le créateur/propriétaire du bien. Dans les deux cas, il convient de rationaliser la façon dont les méfaits sont détectés, poursuivis et réglés dans une réalité de transactions transfrontalières fondées sur un produit immatériel.

Six modèles de cadres étroitement liés

Le projet HIPCAR a élaboré six (6) modèles de cadres étroitement liés, qui offrent un cadre juridique complet permettant d'aborder l'environnement en évolution susmentionné des sociétés de l'information en fournissant l'orientation et le soutien nécessaires à l'établissement d'une législation harmonisée dans les pays bénéficiaires du projet HIPCAR.

En premier lieu, un cadre juridique a été élaboré pour protéger le droit des utilisateurs dans un environnement en évolution. À partir de ce cadre, d'autres aspects garantissant la confiance des consommateurs et des investisseurs dans la sécurité réglementaire et le respect de la vie privée ont été abordés avec l'élaboration des modèles de textes législatifs pour le projet HIPCAR destinés à traiter les questions touchant: **l'accès à l'information publique (liberté d'information)**, conçu pour encourager la culture de la transparence adéquate dans les affaires réglementaires au profit de toutes les parties

prenantes et **le respect de la vie privée et la protection des données**, qui vise à garantir le respect de la vie privée et des informations à caractère personnel de façon satisfaisante pour la personne concernée. Ce dernier cadre se concentre plus particulièrement sur les pratiques de confidentialité appropriées, tant dans le secteur public que dans le secteur privé.

En second lieu, il a été élaboré un modèle de texte législatif HIPCAR relatif au **commerce électronique (transactions)**, incluant les signatures électroniques afin de faciliter l'harmonisation des lois sur les anticipations de défaillances et la validité juridique des pratiques liées à la formation des contrats. Ce cadre est conçu pour prévoir une équivalence entre les documents et contrats papier et électroniques, ainsi qu'assurer le fondement des relations commerciales dans le cyberespace. Un texte législatif consacré au **commerce électronique (preuves),** qui accompagne le cadre relatif au commerce électronique (transactions), a été ajouté afin de réglementer les preuves légales dans les procédures civiles et pénales.

Pour s'assurer que des enquêtes peuvent être menées sur les violations graves de la confidentialité et l'intégrité et la disponibilité des TIC et des données par l'application de la loi, des modèles de textes législatifs ont été élaborés afin d'harmoniser la législation dans le domaine du droit pénal et de la procédure pénale. Le texte législatif sur la **cybercriminalité** définit les infractions, les mécanismes d'enquête et la responsabilité pénale des principaux acteurs. Un texte législatif traitant de **l'interception de communications électroniques** établit un cadre approprié, qui interdit l'interception illégale des communications et définit un créneau étroit permettant l'application de la loi aux interceptions légales de communications si certaines conditions clairement définies sont remplies.

Élaboration des modèles de textes législatifs

Les modèles de textes législatifs ont été élaborés en tenant compte des principaux éléments des tendances internationales, ainsi que des traditions juridiques et des bonnes pratiques de la région. Ce processus a été engagé afin de s'assurer que les cadres s'adaptent au mieux aux réalités et aux exigences de la région des pays bénéficiaires du projet HIPCAR pour lesquels et par lesquels ils ont été élaborés. De la même façon, le processus a impliqué une importante interaction avec les parties prenantes à chaque étape de développement.

La première étape de ce processus complexe a consisté en une évaluation des cadres juridiques en vigueur dans la région passant par l'examen des lois, qui portaient sur tous les domaines concernés. Outre la législation promulguée, l'examen a concerné, le cas échéant, les projets de loi qui avaient été préparés, mais pour lesquels le processus de promulgation n'était pas achevé. Lors d'une seconde étape, les bonnes pratiques internationales (par exemple des Nations Unies, de l'OCDE, de l'UE, du Commonwealth, de la CNUDCI et de la CARICOM) et les législations nationales avancées (par exemple du Royaume-Uni, de l'Australie, de Malte et du Brésil, entre autres) ont été identifiées. Ces bonnes pratiques ont été utilisées comme références.

Pour chacun des six domaines, la rédaction d'analyses juridiques complexes a permis de comparer la législation en vigueur dans la région avec ces références. Cette analyse de droit comparé a fourni un instantané du degré d'avancement de la région dans les principaux domaines politiques. Ces observations ont été instructives, faisant apparaître un développement plus avancé des cadres liés à la législation sur les transactions électroniques, la cybercriminalité (ou «l'utilisation abusive de l'informatique») et l'accès à l'information publique (liberté d'information) que des autres cadres.

D'après les résultats des analyses de droit comparé, les parties prenantes régionales ont élaboré des principes politiques de départ qui, une fois approuvés par les parties prenantes, ont formé les bases d'une délibération politique approfondie et de l'élaboration des textes législatifs. Ces principes politiques ont confirmé certains sujets et tendances communs retrouvés dans la jurisprudence internationale, mais ont également identifié des considérations particulières qui devront être incluses dans le contexte d'une région constituée de petits États souverains insulaires en développement. La question de la capacité institutionnelle pour faciliter l'administration appropriée de ces nouveaux systèmes constitue un exemple de considération circonstancielle majeure ayant eu un effet sur les délibérations à ce stade du processus et à d'autres.

Les principes politiques ont ensuite été utilisés pour élaborer des modèles de textes législatifs personnalisés satisfaisant aux normes internationales et à la demande des pays bénéficiaires du projet HIPCAR. Chaque modèle de texte a une nouvelle fois été évalué par les parties prenantes du point de vue de la viabilité et de la possibilité à être traduit dans les contextes régionaux. À ce titre, le groupe des parties prenantes, composé d'un mélange de rédacteurs juridiques et d'experts politiques de la région, a élaboré des textes qui reflètent le mieux la convergence de normes internationales avec des considérations locales. Une large participation des représentants de la quasi-totalité des 15 pays bénéficiaires du projet HIPCAR, des régulateurs, des opérateurs, des organisations régionales, de la société civile et des universitaires a permis la compatibilité des textes législatifs avec les différentes normes juridiques de la région. Cependant, il a également été admis que chaque État bénéficiaire pouvait avoir des préférences particulières quant à la mise en œuvre de certaines dispositions. Par conséquent, les modèles de textes fournissent également des stratégies optionnelles au sein d'un cadre général harmonisé. Cette approche vise à faciliter l'acceptation généralisée des documents et à augmenter les chances d'une mise en œuvre dans les temps dans l'ensemble des pays bénéficiaires.

Interaction et chevauchement de la couverture des modèles de textes

En raison de la nature des questions abordées, plusieurs éléments communs apparaissent dans chacun de ces six cadres.

Dans le premier cas, il convient d'examiner les cadres qui prévoient l'utilisation de moyens électroniques dans la communication et l'exécution du commerce: **commerce électronique (transactions), commerce électronique (preuves), cybercriminalité** et **interception de communications**. Ces quatre cadres traitent de questions relatives au traitement des messages transmis par des réseaux de communication, l'établissement de tests appropriés pour déterminer la validité des dossiers ou des documents et l'intégration de systèmes conçus pour assurer le traitement équitable des matériaux papier et électronique dans la protection contre les mauvais traitements, la consommation et les procédures de résolution des litiges.

À ce titre, plusieurs définitions communes parmi ces cadres doivent tenir compte, lorsque nécessaire, de considérations relatives au champ d'application variable. Les concepts communs incluent: le «réseau de communication électronique», qui doit être aligné sur la définition existante du pays dans les lois relatives aux télécommunications en vigueur; le «document électronique» ou le «dossier électronique», qui doit refléter des interprétations élargies afin d'inclure par exemple le matériel audio et vidéo; et les «signatures électroniques», les «signatures électroniques avancées», les «certificats», les «certificats accrédités», les «prestataires de service de certification» et les «autorités de certification», qui traitent tous de l'application des techniques de cryptage pour fournir une validation électronique de l'authenticité et la reconnaissance du secteur technologique et économique qui s'est développé autour de la fourniture de ces services.

Dans ce contexte, le texte **commerce électronique (transactions)** établit, entre autres choses, les principes fondamentaux de reconnaissance et d'attribution nécessaires à l'efficacité des autres cadres. Il s'attache à définir les principes fondamentaux qui doivent être utilisés lors de la détermination de cas de nature civile ou commerciale. Ce cadre est également essentiel pour définir une structure de marché appropriée et une stratégie réaliste pour le contrôle du secteur dans l'intérêt du public et de la confiance du consommateur. Les décisions prises sur les questions liées à ce système administratif ont un effet sur la façon dont les signatures électroniques doivent être utilisées en termes de procédure à des fins de preuve, et sur la façon dont les devoirs et responsabilités définis dans la loi peuvent être attribués de manière appropriée.

Avec cette présomption d'équivalence, les autres cadres peuvent aborder de façon adéquate les points de départ liés au traitement approprié des transferts d'information électronique. Le cadre **Cybercriminalité**, par exemple, définit les infractions en rapport avec l'interception de communications, la modification des communications et la fraude informatique. Le cadre **Commerce électronique (preuves)** fournit le fondement qui introduit les éléments de preuve électroniques comme une nouvelle catégorie de preuves.

L'un des fils conducteurs importants qui relient les **transactions électroniques** et la **cybercriminalité** est la détermination des responsabilités appropriées des prestataires de services dont les services sont utilisés pour des méfaits faisant appel à des moyens électroniques. Une attention particulière a été accordée à la cohérence lors de la détermination des parties ciblées par les articles concernés, en veillant à l'application appropriée des obligations et à leur exécution.

Dans le cas des cadres conçus pour renforcer le contrôle réglementaire et la confiance de l'utilisateur, les modèles de textes élaborés par le projet HIPCAR concernent les deux extrêmes d'une même question: tandis que le modèle **Accès à l'information publique** encourage la révélation des informations publiques, sauf exceptions particulières, le modèle **Respect de la vie privée et protection des données** encourage la protection d'un sous-ensemble de ces informations qui seraient considérées comme exemptées dans le premier modèle. Il est important de noter que ces deux cadres sont conçus pour encourager une amélioration de la gestion des documents et des pratiques de tenue des dossiers dans le secteur public et, dans le cas du dernier cadre, également certains aspects du secteur privé. Il convient toutefois de souligner que, contrairement aux quatre autres modèles de textes, ces cadres ne s'appliquent pas exclusivement au support électronique et qu'ils ne visent pas à élaborer un cadre favorable au sein duquel les considérations concernant de nouveaux supports seraient transposées dans les procédures existantes. Pour assurer la cohérence, les cadres sont plutôt conçus pour réglementer la gestion appropriée des ressources d'information tant sous forme électronique que non électronique.

Un certain nombre de sources de chevauchements structurels et logistiques existent entre ces deux cadres législatifs. Certains se trouvent dans la définition des concepts clés d'«autorité publique» (les personnes sur qui les cadres seraient applicables), d'«information», de «données» et de «document», et les relations existant entre ceux-ci. Une autre forme importante de chevauchement concerne le contrôle approprié de ces cadres. Ces deux cadres requièrent l'établissement d'organes de contrôle suffisamment indépendants de toute influence extérieure pour garantir au public la valeur de leurs décisions. Ces organes indépendants doivent également avoir la capacité d'infliger des amendes et/ou des pénalités contre les parties qui entreprennent des actions à l'encontre des objectifs de l'un de ces cadres.

En conclusion

Les six modèles de textes législatifs pour le projet HIPCAR offrent aux pays bénéficiaires du projet un cadre complet permettant de traiter les domaines de réglementation les plus pertinents concernant les questions relatives à la société de l'information. Leur rédaction reflète à la fois les normes internationales les plus actuelles et les demandes des petits pays insulaires en développement en général et, plus particulièrement, des pays bénéficiaires du projet HIPCAR. La large participation des parties prenantes de ces pays bénéficiaires à toutes les phases d'élaboration des modèles de textes législatifs garantit qu'ils pourront être adoptés sans heurts et en temps voulu. Bien que l'attention ait porté sur les besoins des pays de la région des Caraïbes, certains pays d'autres régions du monde ont déjà retenu les modèles de textes législatifs susmentionnés comme de possibles lignes directrices pour eux-mêmes.

Étant donné les natures spécifiques et étroitement liées des modèles de textes du projet HIPCAR, les pays bénéficiaires du projet auraient tout intérêt à élaborer et mettre en place une législation fondée sur ces modèles de façon coordonnée. Les modèles consacrés au commerce électronique (transactions et preuves) fonctionnent plus efficacement avec l'élaboration et l'adoption simultanées des cadres relatifs à la cybercriminalité et à l'interception de communications, si étroitement liés et dépendants les uns des autres, pour résoudre les questions d'un développement réglementaire solide. De la même façon, les cadres relatifs à l'accès à l'information publique et au respect de la vie privée et à la protection des données présentent de telles synergies en termes de cadres administratifs et d'exigences de compétences fondamentales que leur adoption simultanée ne peut que renforcer leur mise en œuvre.

Une excellente occasion sera ainsi créée d'utiliser les cadres holistiques établis dans la région.

1.5. Ce rapport

Le présent rapport a trait à la cybercriminalité, l'un des domaines d'activité du Groupe de travail sur le Cadre législatif et politique des TIC concernant les questions relatives à la société de l'information. Il se compose d'un modèle de lignes directrices politiques et d'un modèle de texte législatif accompagné de notes explicatives que les pays des Caraïbes pourraient souhaiter utiliser lors de l'élaboration ou de la modernisation de leurs politiques et législations nationales dans ce domaine.

Avant de rédiger ce document, l'équipe d'experts du projet HIPCAR a préparé et examiné, en étroite collaboration avec les membres du Groupe de travail susmentionné, une évaluation de la législation en vigueur dans les quinze pays de la région bénéficiaires du projet HIPCAR concernant les questions relatives à la société de l'information, en s'arrêtant à six domaines: les opérations électroniques, les éléments de preuve électroniques dans le commerce électronique, la protection de la vie privée et des données, l'interception des communications, la cybercriminalité et l'accès à l'information publique (liberté d'information). Cette évaluation tenait compte des meilleures pratiques acceptées au plan international et régional.

Cette évaluation régionale, publiée séparément en complément du présent rapport[3], comprenait une analyse comparative de la législation en vigueur en matière de cybercriminalité dans les pays bénéficiaires du projet HIPCAR et une étude des lacunes potentielles à cet égard, deux documents qui ont servi de base à l'élaboration des modèles de cadre politique et de texte législatif présentés ci-après. À la fois reflets des meilleures pratiques et normes nationales, régionales et internationales, et garants de la compatibilité avec les traditions juridiques des Caraïbes, les modèles présentés dans ce rapport ont pour but de répondre aux besoins spécifiques de la région.

Le comité directeur d'HIPCAR, présidé par l'Union des télécommunications des Caraïbes (CTU), a fourni recommandations et soutien à une équipe de consultants, dont faisaient partie Dr. Marco Gercke et Mme Pricilla Banner. Le modèle de texte législatif sur la cybercriminalité a d'abord été élaboré en trois temps par les consultants du projet HIPCAR: 1) rédaction d'un rapport d'évaluation, 2) élaboration de modèles de lignes directrices politiques et 3) rédaction d'un modèle de texte législatif. Les ébauches de ces documents ont ensuite été révisées, discutées et adoptées par un large consensus des participants lors de deux ateliers de consultation du Groupe de travail du projet HIPCAR sur les questions relatives à la société de l'information, qui se sont déroulés à Sainte-Lucie du 8 au 12 mars 2010 et à Saint-Christophe-et-Niévès du 19 au 22 juillet 2010 (voir Annexes). Les notes explicatives du modèle de texte législatif proposé dans le présent document ont été rédigées par Dr. Marco Gercke à la suite, notamment, des questions soulevées lors du deuxième atelier. Ce document contient donc les données et informations valables en juillet 2010.

À la suite de ce processus, les documents ont été finalisés et diffusés à l'ensemble des parties prenantes pour être portés à l'attention des gouvernements des pays bénéficiaires du projet HIPCAR.

1.6. Importance de la lutte contre la cybercriminalité

Ces dernières décennies, la criminalité informatique et la cybercriminalité sont devenues une préoccupation majeure en matière d'application de la loi dans le monde. Depuis que le débat sur les abus criminels des technologies informatiques et de réseau a débuté dans les années 1960, l'importance du sujet n'a cessé de se faire jour[4]. Pendant un demi-siècle de vifs débats, diverses solutions ont été discutées pour répondre à cette question. Toutefois, malgré les évolutions techniques continues et les changements de méthodes en matière de traitement des infractions, la question reste à l'ordre du jour pour les gouvernements et les organisations internationales/régionales.

---

[3] Voir «Cybercrime: Assessment Report», disponible à l'adresse www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

[4] Concernant les premiers débats sur la criminalité informatique, voir *Bequai*, Computer Crime, 1978; *Blanton*, Computer Crime, 1978; *Coughran*, Computer abuse and criminal law, 1976; *MacIntyre*, Computer and Crime, 1977; *McKnight*, Computer Crime, 1973; *Parker*, Crime by Computer, 1976; *Rose*, An analysis of computer related crime: A research study, 1977; *Sokolik*, Computer Crime: Its setting and the need for deterrent legislation, 1979; *Wilson/Leibholz*, User's Guide to Computer Crime: Its Commission, Detection and Prevention, 1969.

Introduction

Entre les années 1960 et les années 1980, la manipulation informatique et l'espionnage des données – souvent non couverts par la législation criminelle en vigueur – et, en particulier, l'élaboration d'une réponse juridique, ont été au cœur des débats[5]. Cette situation a changé dans les années 1990 lorsqu'une interface graphique («WWW») a été introduite et que le nombre de sites Web et d'utilisateurs Internet a commencé à augmenter considérablement. Il est alors devenu possible de rendre l'information légalement disponible dans un pays et de permettre aux internautes du monde entier de la télécharger, même dans les pays où la publication de telles informations était criminalisée[6].

Ces dernières années, le débat a été dominé par de nouvelles méthodes très sophistiquées pour commettre des crimes, par exemple le «hameçonnage[7]» (ou «phishing»), les «attaques de botnets[8]» (réseaux zombis) et l'utilisation accrue de technologies plus difficiles à étudier pour les services de répression, telles que «les communications vocales sur IP (VoIP)[9]» et l'«informatique en nuage[10]».

La capacité à lutter contre la cybercriminalité est essentielle pour les pays développés comme pour les pays en développement. Du fait de la dépendance accrue à la disponibilité des réseaux et des systèmes informatiques[11], ainsi que du nombre toujours plus important d'internautes, les crimes commis en utilisant les technologies de l'information vont très probablement devenir plus fréquents et potentiellement plus graves. Afin de protéger les utilisateurs ayant commencé à intégrer les services de réseau tels que les courriers électroniques, la communication via les réseaux sociaux ou les services bancaires en ligne, les pays doivent être capables d'agir lorsque ces services sont attaqués ou abusés de toute autre manière. Cependant, il est important d'être en mesure d'enquêter pour identifier les auteurs d'infractions et de recueillir des preuves numériques. Cela dépasse la protection des consommateurs. Internet est un marché mondial où les entreprises peuvent offrir leurs services dans le monde entier. Si les pays veulent créer un environnement permettant au commerce électronique de croître, ils doivent, à long terme, veiller à ce que les crimes à l'encontre de ces entreprises ne restent pas impunis.

En conséquence, la lutte contre la cybercriminalité est devenue une priorité dans la plupart des pays. Il est important de souligner que cette question, contrairement à d'autres, devrait très probablement rester une priorité pendant des années, dans la mesure où il n'est pas possible d'y répondre en une seule fois et de manière définitive. La cybercriminalité se développe constamment et les solutions juridiques nécessiteront parfois des ajustements continus.

Cantonner la réponse aux solutions techniques ne résoudra certainement pas les problèmes. Certaines solutions techniques mises en œuvre dans le cadre de stratégies de lutte contre la cybercriminalité incluent souvent des pare-feux (qui empêchent l'accès illégal aux systèmes informatiques) ou le cryptage (pour empêcher l'interception illégale des communications). Toutefois, l'expérience a montré que, outre les solutions techniques, des mesures législatives sont également nécessaires: une législation pénale sanctionnant certaines formes de crimes informatiques et la cybercriminalité, de même que l'existence d'instruments de procédure connexes permettant aux services de répression d'effectuer des enquêtes, sont des exigences vitales pour associer ces services à la lutte contre les crimes informatiques et la

5 Voir par exemple *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976; *Sieber*, Computerkriminalitaet und Strafrecht, 1977.

6 Concernant la dimension transnationale de la cybercriminlaité, voir *Sofaer/Goodman*, «Cyber Crime and Security – The Transnational Dimension» in *Sofaer/Goodman*, «The Transnational Dimension of Cyber Crime and Terrorism», 2001, page 7.

7 Le terme «hameçonnage» est utilisé pour décrire les actes visant à contraindre la victime à révéler des informations personnelles ou confidentielles. Il décrivait à l'origine l'utilisation de courriers électroniques pour hameçonner (to phish) des mots de passe et des données financières de milliers d'internautes. Dérivé du mot «fishing» (pêche), le remplacement du «f» par «ph» est lié à des conventions langagières prisées des pirates. Pour plus d'informations, voir Comprendre la cybercriminalité: guide pour les pays en développement, ITU 2009, chapitre 2.8.4.

8 Un botnet est un groupe d'ordinateurs infectés sur lesquels s'exécutent des programmes commandés à distance. Pour plus de détails, voir *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

9 *Simon/Slay*, «Voice over IP: Forensic Computing Implications», 2006.

10 *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, in Taeger/Wiebe, Inside the Cloud, 2009, page 499 et suivantes.

11 À cet égard, voir Comprendre la cybercriminalité: guide pour les pays en développement, ITU 2009, page 76

cybercriminalité. L'absence de législation adéquate dans certains pays risque avant tout de se traduire par l'incapacité des services de répression à aider les citoyens victimes de crimes informatiques. Plus grave encore est le fait que la non-criminalisation de certaines formes de cybercriminalité pourrait protéger les contrevenants ou même les motiver à pratiquer, depuis l'étranger, des activités illégales dans des pays dépourvus de législation. Empêcher les «refuges» permettant aux criminels d'opérer en toute impunité est, par conséquent, devenu un défi majeur de la lutte contre la cybercriminalité[12]. Où que se trouvent ces «refuges», il existe un risque que les délinquants les utilisent pour échapper aux enquêtes. Un exemple représentatif de ce problème est le ver informatique «Love Bug», développé par un pirate aux Philippines en 2000[13], qui avait infecté des millions d'ordinateurs dans le monde[14]. Les enquêtes locales avaient été entravées par le fait que, à l'époque, le développement et la diffusion de logiciels malveillants n'étaient pas suffisamment sanctionnés aux Philippines[15].

Bien que le développement de nouvelles technologies soit principalement centré sur la satisfaction des besoins des consommateurs dans les pays occidentaux, les pays en développement ont effectué des progrès importants pour réduire l'écart, en particulier en matière d'accès à l'information[16], même si des améliorations restent nécessaires. En 2005, le nombre d'internautes dans les pays en développement a dépassé le celui des nations industrialisées[17]. Avec la croissance de la connectivité et la conversion des entreprises traditionnelles au commerce électronique, la cybercriminalité n'est plus un problème limité aux seuls pays développés. Elle concerne également les pays en développement[18]. Toutefois, ces derniers, en particulier les petits pays insulaires, connaissent un nombre de difficultés spécifiques dans la mise en œuvre de leurs lois. Alors que les crimes auxquels ils sont confrontés sont, dans une certaine mesure, les mêmes que ceux des pays développés, les pays en développement ont des exigences spéciales lorsqu'il s'agit d'apporter des réponses. Par exemple, si les pays développés peuvent se doter d'un réseau dit 24/7 pour les demandes d'aide juridique internationale mutuelle, les pays en développement n'ont souvent pas la capacité d'entretenir une telle infrastructure. Il est par conséquent essentiel que les pays en développement tiennent compte des normes internationales, ainsi que de leur situation spécifique lors de l'élaboration d'une stratégie de lutte contre la cybercriminalité en général et de lois relatives à la cybercriminalité en particulier.

---

12 Ce problème a été traité par plusieurs organisations internationales. Par exemple, la résolution 55/63 de l'Assemblée générale de l'ONU énonce: «Les États devraient faire en sorte que leurs lois et leur pratique ne permettent pas que ceux qui exploitent les technologies de l'information à des fins criminelles puissent compter sur l'impunité.» Le texte complet de cette résolution est disponible sur www.unodc.org/pdf/crime/a_res_55/res5563f.pdf. Le plan d'action en dix points du G8 souligne que: «Il ne doit pas exister de refuges pour ceux qui exploitent les technologies de l'information à des fins criminelles.» Voir Comprendre la cybercriminalité: guide pour les pays en développement, ITU 2009, chapitre 5.2.

13 Pour plus d'informations, voir www.en.wikipedia.org/wiki/ILOVEYOU; concernant les conséquences de ce ver sur la protection des infrastructures essentielles de l'information, voir *Brock*, «ILOVEYOU» Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000.

14 BBC News, «Police close in on Love Bug culprit», 6 mai 2000.

15 Voir par exemple CNN, «Love Bug virus raises spectre of cyberterrorism», 8 mai 2000; *Chawki*, «A Critical Look at the Regulation of Cybercrime», www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, «Cyber Crime and Security – The Transnational Dimension» in *Sofaer/Goodman*, «The Transnational Dimension of Cyber Crime and Terrorism», 2001, page 10; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; Conférence des Nations Unies sur le commerce et le développement, Rapport 2005 sur l'économie de l'information, UNCTAD/SDTE/ECB/2005/1, 2005, chapitre 6, page 233.

16 Concernant les possibilités et la technologie disponible pour accéder à Internet dans les pays en développement, voir *Esteve/Machin*, Devices to access Internet in Developing countries, www2007.org/workshops/paper_106.pdf.

17 Voir «Development Gateway's Special Report, Information Society – Next Steps?», 2005, www.topics.developmentgateway.org/special/informationsociety.

18 Les demandes spécifiques des pays en développement sont traitées dans la publication de l'ITU intitulée «Comprendre la cybercriminalité: guide pour les pays en développement» publiée en 2009 et disponible gratuitement dans les six langues de l'ONU.

Partie I:
Modèles de lignes directrices politiques – cybercriminalité

Voici des modèles de lignes directrices politiques qu'un pays pourrait prendre en considération en matière de cybercriminalité.

1. LES PAYS DE LA CARICOM/DU CARIFORUM VISERONT À ÉTABLIR LES INTERPRÉTATIONS COMMUNES NÉCESSAIRES POUR LES PRINCIPAUX TERMES ASSOCIÉS À LA CYBERCRIMINALITÉ.

- Des définitions adéquates seront fournies pour les termes «ordinateur», «système informatique», «dispositif», «données informatiques», «données relatives au contenu», «données relatives au trafic», «données de localisation», «document», «enregistrement électronique», «document électronique», «signature électronique», «signature numérique» et «horodatage».
- La formulation de la définition de ces termes sera suffisamment large et assortie d'une liste d'exemples d'illustration.
- La terminologie laissée à l'interprétation judiciaire des juridictions sera définie, de même que les modalités de suivi des activités judiciaires en ce sens, afin de préserver l'harmonie des définitions législatives et judiciaires. À l'échelle nationale, chaque État membre décidera quelle est la meilleure option pour lui.
- L'harmonisation sera facilitée via la communication des précédents judiciaires: définir autant que possible les termes techniques spécifiques.
- Des supports de formation seront élaborés afin de fournir aux enquêteurs, aux procureurs et aux juges l'interprétation nécessaire de ces termes, si nécessaire, notamment aux parties prenantes concernées.

2. LES PAYS DE LA CARICOM/DU CARIFORUM ÉLABORERONT UN DROIT PÉNAL MATÉRIEL EN MATIÈRE DE CYBERCRIMINALITÉ

- Des dispositions couvriront les formes de cybercriminalité les plus courantes et les plus largement acceptées à l'échelle internationale, ainsi que les infractions d'intérêt spécifique pour la région (par exemple, le spam).
- Afin de garantir la capacité à coopérer avec les services de répression dans les pays de la région et en dehors de la région, la législation sera compatible avec les normes et les meilleures pratiques internationales, ainsi qu'avec les normes et meilleures pratiques régionales existantes (dans la mesure du possible).
- Une disposition criminalisera l'accès intentionnel et illégal à un système informatique, ainsi que la présence illégale dans un système informatique. Un alourdissement des peines pourra être envisagé dans les cas où les mesures de protection sont contournées pour intercepter la transmission pourrait être envisagé.
- Une disposition criminalisera l'interception intentionnelle et illégale de transmission de données non publiques (interception illégale). Cette disposition ne devra pas gêner l'interception légale par les autorités compétentes. Un alourdissement des peines pourra être envisagé dans les cas où les mesures de protection sont contournées pour intercepter la transmission.

> Modèles de lignes directrices politiques et de textes législatifs

- Une disposition criminalisera l'atteinte intentionnelle et illégale à l'intégrité des données informatiques. Il conviendra de veiller à ce que l'application d'un instrument de procédure nécessaire aux enquêtes ne soit pas entravée dans les cas où le contrevenant commet plusieurs infractions et que chacune d'elle n'entraîne que des dégâts limités.
- Une disposition criminalisera l'atteinte intentionnelle et illégale à l'intégrité des systèmes informatiques (par exemple, les attaques par déni de service). Un alourdissement des peines pourra être envisagé dans les cas où l'infrastructure critique est touchée.
- Une disposition criminalisera la production, la vente et autres actes similaires intentionnels et illégaux d'outils principalement conçus pour commettre des crimes informatiques. Il conviendra de veiller à ce qu'une telle législation ne criminalise pas l'utilisation légitime de ces outils logiciels.
- Une disposition criminalisera la falsification informatique intentionnelle et illégale. Il conviendra de veiller à ce que cette législation couvre en particulier l'envoi de courriers électroniques à des fins de hameçonnage. Un alourdissement des peines pourra être envisagé dans les cas où de nombreux courriers sont envoyés.
- Une disposition criminalisera la fraude informatique intentionnelle et illégale.
- Il conviendra de veiller à ce que la législation existante qui criminalise la fraude soit également applicable si les délinquants utilisent des moyens de communication électronique pour entrer en contact avec la victime.
- Une disposition criminalisera la production, la vente et autres actes similaires liés à la pornographie infantile. À cet égard en particulier, il conviendra de prendre en compte les normes internationales. La législation devra par ailleurs prévoir la criminalisation de la possession de matériels pédopornographiques et de l'accès aux sites Internet de pornographie infantile. Il conviendra d'accorder une exception accordée aux services de répression afin qu'ils puissent mener leurs enquêtes.
- Une disposition criminalisera les actes liés à l'envoi de spams si ceux-ci affectent la capacité des utilisateurs à utiliser Internet[19].
- La législation devra refléter les difficultés liées à l'attribution.
- Une disposition criminalisera les actes intentionnels et illégaux liés à l'identité. Il conviendra de prendre en compte les différentes phases du vol d'identité (obtention, transfert et utilisation d'informations liées à l'identité).

3. LES PAYS DE LA CARICOM/DU CARIFORUM ÉLABORERONT DES INSTRUMENTS DE PROCÉDURE EFFICACES, MAIS ÉQUILIBRÉS PERMETTANT AUX AUTORITÉS COMPÉTENTES D'ENQUÊTER SUR LA CYBERCRIMINALITÉ TOUT EN PROTÉGEANT LES DROITS DU SUSPECT.

- Les instruments de procédure ne devront pas porter atteinte aux droits du suspect acceptés à l'échelle internationale et régionale.
- Une disposition permettra aux autorités compétentes d'ordonner la conservation rapide des données informatiques envoyées.
- Une disposition permettra aux autorités compétentes d'ordonner la divulgation partielle des données informatiques conservées.
- Une disposition permettra aux autorités compétentes d'ordonner la production de données informatiques.

[19] (Une inquiétude demeure concernant la proportionnalité du recours)

- Une disposition permettra aux autorités compétentes d'utiliser des instruments de perquisition et de saisie spécifiques en matière de preuves numériques et de technologies informatiques. La loi réglementera les procédures de perquisition et de saisie de manière à éviter la collecte des preuves remises en question parce que non certifiées et produites comme preuves matérielles des données collectées et du contexte numérique existant.
- Une disposition permettra aux autorités compétentes d'ordonner la collecte légale de données de trafic et l'interception légale de données relatives au contenu.
- Une disposition limitée aux crimes graves permettra aux autorités compétentes d'utiliser des instruments d'enquête élaborés, par exemple des enregistreurs de frappes et des logiciels de criminalistique à distance pour collecter les mots de passe utilisés par une personne soupçonnée de tels crimes ou pour identifier la connexion utilisée par un suspect.

4. LES PAYS DE LA CARICOM/DU CARIFORUM ÉLABORERONT DES INSTRUMENTS DE COOPÉRATION TRANSNATIONALE DANS LES ENQUÊTES SUR LA CYBERCRIMINALITÉ

- Le cadre de coopération internationale devra refléter les normes internationales de coopération, ainsi que les besoins spécifiques concernant les enquêtes sur la cybercriminalité.
- Le cadre devra inclure la création d'un point de contact disponible 24/24 heures et 7/7 jours pour toute demande d'informations.
- Le cadre devra permettre l'utilisation de moyens rapides de communication (par exemple courriers électroniques et télécopie).

5. LES PAYS DE LA CARICOM/DU CARIFORUM ÉLABORERONT UN CADRE RÉGLEMENTANT LA RESPONSABILITÉ DES FOURNISSEURS DE SERVICES INTERNET

- S'il existe une responsabilité, le cadre devra limiter la responsabilité pénale du fournisseur d'accès concernant les infractions commises par les utilisateurs de son service, s'il n'a pas déclenché la transmission, n'a pas sélectionné le destinataire et n'a pas modifié les informations contenues dans la transmission.
- S'il existe une responsabilité, le cadre devra limiter la responsabilité pénale du fournisseur de cache pour le stockage automatique, intermédiaire et temporaire de l'information.
- S'il existe une responsabilité, le cadre devra limiter la responsabilité pénale de l'hébergeur, si celui-ci n'a pas connaissance de l'existence de données illégales ou s'il les retire immédiatement lorsqu'il en est informé.

Partie II:
Modèle de texte législatif – cybercriminalité

Voici un modèle de texte législatif qu'un pays peut prendre en considération lors de l'élaboration d'une législation nationale en matière de cybercriminalité. Ce modèle se fonde sur les lignes directrices politiques types présentées plus haut.

Organisation des articles

Partie II

TITRE I: PRÉAMBULE

Titre abrégé 1. La présente loi peut être désignée sous le titre de «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 d'empêcher les crimes liés à l'informatique et aux réseaux et d'enquêter sur ceux-ci.

Définitions 3. (1) «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.

(2) «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.

(3) «Enfant» désigne toute personne de moins de dix-huit (18) ans.

(4) «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;

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

Cela inclut, sans s'y limiter, tout support pornographique audio, visuel ou écrit.

Un pays peut restreindre la criminalisation en ne mettant pas en œuvre (b) et (c).

5) «Système d'information» (ou «système informatique») désigne un dispositif ou un groupe de dispositifs interconnectés ou reliés, y compris Internet, qui, conformément à 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 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) «Infrastructures critiques» désigne les systèmes informatiques, les dispositifs, les réseaux, les programmes informatiques, les données informatiques qui sont tellement vitaux pour le pays que toute incapacité, destruction ou atteinte à l'intégrité de ces systèmes et actifs aurait un effet handicapant sur la sécurité, la sécurité nationale ou économique, la santé et la sûreté publiques nationales, ou toute combinaison de ces éléments.

(9) «Dispositifs» désigne, sans s'y limiter:

a. les composants des systèmes informatiques, tels que les cartes graphiques, la mémoire et les puces;

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.

(10) «Entraver», en relation avec un système informatique signifie, sans s'y limiter:

a. couper l'alimentation électrique d'un système informatique;

b. provoquer des interférences électromagnétiques sur un système informatique;

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

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

(11) «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.

(12) «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 pointe vers et affiche un autre document lorsqu'elle est exécutée.

(13) «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.

(14) «Courriers électroniques multiples» désigne tout message électronique, notamment courriel et messagerie instantanée, envoyé à plus de mille destinataires.

(15) «Logiciel de criminalistique à distance» désigne un logiciel d'enquête installé sur un système informatique et utilisé pour effectuer des tâches incluant, sans s'y limiter, l'enregistrement de frappes ou la transmission d'une adresse IP.

(16) «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 accédé;

e. sortir sur imprimante les données informatiques;

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.

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

(18) «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.

(19) «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 recherchées sont stockées sur l'autre système informatique;

c. un moyen de stockage de données informatiques.

(20) «Utiliser» désigne, sans s'y limiter:

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 – INFRACTIONS

Accès illégal

4. (1) 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.

(2) Un pays peut décider de ne pas criminaliser le simple accès non autorisé si d'autres recours efficaces existent. En outre, un pays peut 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.

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.

Partie II

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 imposer que l'infraction soit commise avec 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;

b. suppression de données informatiques;

b. altération de données informatiques;

d. rend les données informatiques dénuées de sens, inutiles ou inopérantes;

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

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 opère 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 et que cela affecte cette utilisation ou affecte 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,

avec 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 ne 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 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 la perte d'un bien d'un tiers par l'une des manières suivantes:

a. introduction, altération, effacement ou suppression des données informatiques;

b. atteinte au fonctionnement d'un système informatique;

avec l'intention frauduleuse ou malhonnête d'obtenir, sans 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 pornographique 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 pour un tiers, via un système informatique;

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

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 établit 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).

(3) Un pays peut ne pas criminaliser le comportement décrit à l'Article 13(1)(d)-(f).

Infractions liées à l'identité

14. 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.

Spam

15. (1) 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:

a. déclenche la transmission de courriers électroniques multiples à partir ou par l'intermédaire d'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 définir des critères plus restrictifs en ce qui concerne la criminalisation de la transmission de courriers électroniques multiples dans le cadre de relations clients ou commerciales. Un pays peut décider de ne pas criminaliser le comportement décrit à l'Article 15(1)(a) si d'autres recours efficaces existent.

Divulgation des détails d'une enquête

16. 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;

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

17. (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 20 à 22, 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

18. Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, 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 une amende maximale de [montant], ou les deux.

TITRE III – JURIDICTION

Juridiction 19. La présente loi s'applique à tout acte ou omission commis:

a. sur le territoire de [État prenant les dispositions];

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

c. par un citoyen de [État prenant les dispositions] en dehors de la juridiction de tout pays; ou

par un citoyen de [État prenant les dispositions] en dehors du territoire de [État 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 – DROIT PROCÉDURAL

Perquisition et saisie 20. (1) Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment], qu'il existe de bonnes raisons [de soupçonner] [de croire] qu'il peut exister dans un lieu un objet ou des données informatiques:

a. pouvant être considérés comme importants pour servir de preuve à une infraction; ou

b. ayant été obtenus par une personne suite à une infraction,

le magistrat [peut] [doit] émettre un mandat autorisant un agent [de répression] [de police], avec toute l'assistance pouvant être nécessaire, d'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 une partie d'un tel système et aux données informatiques qui y sont stockées; et

ii. un moyen de stockage des données informatiques dans lequel les données informatiques peuvent être stockées sur le territoire du pays.

(2) Si un agent de [répression] [police] qui entreprend une perquisition sur la base de l'Article 20(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 de [répression] [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 21. Toute personne n'étant pas suspectée d'un crime, 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 20 doit permettre et assister la personne autorisée 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 20;

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.

Injonction de produire

22. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent de [répression] [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 [État 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 [État prenant les dispositions], de produire des informations sur les personnes qui sont abonnées au service ou qui utilisent autrement ce service.

Conservation rapide

23. Si un agent de [répression] [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 qu'elle veille 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 une demande *ex parte*, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.

Divulgation partielle des données de trafic

24. Si un agent de [répression] [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 des données informatiques, exiger de cette personne qu'elle divulgue suffisamment de données de trafic associées à une communication spécifique, afin d'identifier:

a. les fournisseurs de services Internet; et/ou

b. l'itinéraire de la communication.

Collecte des données de trafic

25. (1) Si un [juge] [magistrat] est convaincu, sur la base d'[informations données 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 pour les besoins d'une enquête criminelle, il [peut] [doit] ordonner à une personne qui contrôle desdites 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 de [répression] [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'[informations données 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 pour les besoins d'une enquête criminelle, il [peut] [doit] autoriser un agent de [répression] [police] à collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifiée grâce à l'application de moyens techniques.

(3) Un pays peut décider de ne pas mettre en œuvre l'Article 25.

Interception des données relatives au contenu

26. (1) Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe des motifs raisonnables de [suspecter] [croire] que le contenu de communications électroniques est raisonnablement nécessaire pour les besoins d'une enquête criminelle, il [peut] [doit]:

a. ordonner à un fournisseur de services Internet dont les services sont disponibles en [État prenant les dispositions], en utilisant des moyens techniques, de collecter ou d'enregistrer ou de permettre aux autorités compétentes ou de les assister à collecter ou enregistrer les données de contenu associées à des communications spécifiées transmises par l'intermédiaire d'un système informatique; ou

b. autoriser un agent de [répression] [police] à collecter ou enregistrer lesdites données, en utilisant des moyens techniques.

(2) Un pays peut décider de ne pas mettre en œuvre l'Article 26.

Logiciel de criminalistique

27. (1) Si un [juge] [magistrat] est convaincu, sur la base d'[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 de [répression] [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 27(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 20.

(6) Si nécessaire, un agent de [répression] [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 œuvre l'Article 27.

TITRE V – RESPONSABILITÉ

Pas d'obligation de surveillance

28. Les fournisseurs de services Internet n'ont pas l'obligation générale de surveiller les informations qu'ils transmettent ou stockent au nom d'un tiers, ni l'obligation générale de rechercher activement les faits ou les circonstances indiquant une activité illégale pour échapper à la responsabilité pénale. Cette disposition n'affecte pas la possibilité, pour un tribunal ou une autorité administrative, d'exiger d'un fournisseur d'accès de mettre fin à, ou d'empêcher un acte sur la base d'une loi adoptée par le Parlement en [territoire].

Fournisseur d'accès

29. (1) Un fournisseur d'accès n'est pas responsable pénalement 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 la condition que lesdites informations ne soient pas stockées pour une période plus longue que ce qui est raisonnablement nécessaire pour la transmission.

Hébergeur

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

31. 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 la 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 l'industrie;

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

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

32. 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 par une autorité publique ou 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 lui permettre d'évaluer la nature des informations et, si nécessaire, d'ordonner le retrait du contenu.

Fournisseur de moteurs de recherche

33. 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 la condition qu'il:

a. ne déclenche pas la transmission;

b. ne sélectionne pas le destinataire de la transmission; et

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

Partie III:
Notes explicatives au modèle de texte législatif sur la cybercriminalité

INTRODUCTION

1. Le présent texte législatif fournit un cadre juridique à la criminalisation des infractions liées à l'informatique et aux réseaux. Les principaux objectifs de ce modèle de texte législatif sont de criminaliser certains contenus illégaux, conformément aux meilleures pratiques régionales et internationales, de fournir les instruments de procédure spécifiques nécessaires pour enquêter sur lesdites infractions et de définir la responsabilité du prestataire de services.

2. Les présentes notes explicatives ont été préparées pour expliquer le contenu du modèle de texte législatif et doivent être lues en parallèle avec celui-ci. Elles expliquent l'importance des dispositions et, le cas échéant, reflètent les discussions ayant eu lieu au sein du Groupe de travail[20] du projet HIPCAR[21]. Elles ne constituent pas une description détaillée du présent texte législatif et ne sont pas destinées à l'être. Par conséquent, lorsqu'un article ou une partie d'un article ne semble nécessiter aucun éclaircissement, commentaire ou référence, ou lorsqu'une disposition n'a donné lieu à aucune discussion, il n'est donné aucune explication détaillée.

3. Le modèle de texte législatif (loi) se compose de cinq parties:

   - Le **Titre I** fournit les définitions et fixe l'objectif de la loi;
   - Le **Titre II** fournit un ensemble de dispositions législatives importantes qui criminalisent certaines infractions;
   - Le **Titre III** présente des procédures pour déterminer la juridiction;
   - Le **Titre IV** fournit un ensemble d'instruments de procédure nécessaires pour enquêter sur la cybercriminalité;
   - Le **Titre V** définit les limitations de la responsabilité des fournisseurs de services Internet.

---

20 Les membres des groupes de travail du projet HIPCAR incluent des représentants du ministère et du régulateur nommés par leur gouvernement national, des organes régionaux et des observateurs concernés, par exemple des opérateurs et autres parties prenantes intéressées. Les Termes de référence des groupes de travail sont disponibles sur www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.

21 L'intitulé complet du projet HIPCAR est «*Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures*» (Renforcer la compétitivité dans les Caraïbes par l'harmonisation des politiques, de la législation et des procédures réglementaires dans le domaine des TIC). Ce projet de trois ans a été lancé en septembre 2008, dans le contexte d'un projet cadre englobant les pays ACP, financé par l'Union européenne et l'Union internationale des télécommunications (UIT). Ce projet est mis en œuvre par l'UIT en collaboration avec le Secrétariat de la Communauté caribéenne (CARICOM) et l'Union des télécommunications des Caraïbes (CTU).
Le deuxième atelier de consultation (étape B) du premier Groupe de travail du projet HIPCAR sur le cadre législatif des TIC concernant les questions de la société de l'information liées à la cybercriminalité a eu lieu à Saint-Kitts-et-Nevis les 19-22 juillet 2010. Les participants ont examiné, discuté et adopté le projet de modèle de texte législatif en la matière. L'utilisation des mots «groupe de travail» ou «rédacteurs» dans ce document se réfère à l'atelier susmentionné.

COMMENTAIRE ARTICLE PAR ARTICLE

TITRE I

Article 1. Définitions

(1) Fournisseur d'accès

Les rédacteurs du texte législatif ont décidé de limiter la responsabilité de certains fournisseurs de services Internet si leur capacité à empêcher les utilisateurs de commettre des crimes est limitée. Il était par conséquent nécessaire de faire la différence entre les différents types de fournisseurs. L'Article 3(1) précise que le terme «fournisseur d'accès» peut aussi bien désigner une personne morale qu'une personne physique. En conséquence, même l'opérateur d'un réseau privé peut être considéré comme un fournisseur d'accès.

(2) Fournisseur de cache

La mise en cache de contenu est une technique très utilisée pour améliorer la vitesse d'accès aux informations très recherchées. Elle couvre en particulier le stockage de sites Internet populaires par les prestataires de services sur des supports de stockage locaux, afin de réduire la bande passante et de rendre plus efficace l'accès aux données. Cela peut, par exemple, être réalisé en mettant en place des serveurs mandataires. Le processus de copie des données ne conduit à la qualification de fournisseur de cache que si le fournisseur configure son système de manière à ce que le processus de stockage se déroule de manière automatique, intermédiaire et temporaire à la seule fin d'améliorer l'efficacité de la transmission ultérieure. Par conséquent, le stockage manuel comme le stockage à long terme ne sont pas couverts.

(3) Enfant

Le terme «enfant» a été défini conformément à l'article 1 de la Convention de l'ONU relative aux droits de l'enfant. Les détails relatifs à la détermination de l'âge, par exemple la question de l'apparence peut être utilisée lorsque l'information sur l'âge réel de l'enfant ne peut pas être obtenue, seront établis à la discrétion des législateurs nationaux, conformément aux exigences des lois de chaque pays. À cet égard, la définition (7) contient certaines directives relatives à la pornographie infantile.

(4) Pédopornographie ou pornographie infantile

La définition de la pédopornographie a fait l'objet de discussions intenses parmi les rédacteurs du texte législatif. Alors qu'il a été largement convenu que l'expression doit couvrir la documentation d'un abus réel, les rédacteurs ont décidé de laisser aux législateurs nationaux le soin de déterminer s'ils veulent également qu'elle couvre les personnes ayant l'apparence d'un enfant ou les images représentant des mineurs. Dans ce contexte, les rédacteurs ont tenu compte du fait qu'à l'époque actuelle, des images réalistes peuvent être facilement créées à l'aide de technologies informatiques sophistiquées et que de telles images peuvent être utilisées pour encourager ou amener les enfants à participer à de tels actes.

Compte tenu du fait que la pornographie infantile n'est pas seulement diffusée sous forme d'images ou de vidéos, les rédacteurs ont décidé d'adopter une formulation couvrant les supports audio, visuels et écrits.

(5) Système informatique

Les termes «système informatique» et «système d'information» sont tous deux utilisés pour décrire les dispositifs de traitement des données qui combinent en général le matériel et les logiciels. Les systèmes informatiques incluent par conséquent les périphériques d'entrée et de sortie, ainsi que les dispositifs de stockage, dès lors qu'ils contiennent des éléments de traitement des données. Les rédacteurs du texte législatif ont décidé d'étendre la définition afin d'y inclure également Internet.

(6) Données informatiques

Les rédacteurs ont décidé de baser la définition de «données informatiques» sur les normes internationales. Afin de veiller à ce que chaque type de contenu soit couvert, les rédacteurs ont fourni des exemples entre parenthèses.

(7) Moyen de stockage de données informatiques

La capacité, comme la taille et la fonction des dispositifs de stockage informatique ont évolué ces dernières décennies. Les rédacteurs ont décidé d'élaborer une définition ouverte qui couvre les périphériques de stockage de masse ainsi que les systèmes de microstockage, qui sont par exemple utilisés dans les clés de voiture. Cette disposition s'applique par conséquent aux dispositifs de stockage permanent comme aux systèmes de stockage à court terme (par exemple, la RAM).

(8) Infrastructure critique

Aujourd'hui, les systèmes informatiques sont non seulement utilisés par les particuliers et les entreprises, mais également par les opérateurs d'infrastructures critiques, par exemple la fourniture d'énergie ou le contrôle du trafic. Dans la mesure où les infrastructures considérées critiques sont différentes d'un pays à l'autre, les rédacteurs ont décidé d'adopter une définition large de cette expression.

(9) Dispositifs

Les rédacteurs ont décidé de fournir une approche ouverte à l'application de dispositions se référant à un dispositif, en fournissant une série d'exemples. Par conséquent, cette liste d'exemples n'est pas définitive ou limitée, mais ouverte aux évolutions.

(10) Entraver

Certaines approches internationales de lutte contre la cybercriminalité criminalisent l'entrave illégale des systèmes informatiques sans fournir une définition précise de ce qui est couvert par la loi. Les rédacteurs ont décidé de veiller à ce que le terme «entraver» inclue les attaques de réseau (par exemple, la transmission de données informatiques), ainsi que les attaques physiques. Les coupures de courant accidentelles sont couvertes par la définition, mais sont exclues de la responsabilité pénale, la disposition concernée (Article 9) imposant la commission de l'acte et le caractère intentionnel.

(11) Hébergeur

Comme dans les définitions des autres catégories de fournisseurs de services Internet, le terme «hébergeur» peut se référer à une personne physique comme à une personne morale. Il n'est pas nécessaire que l'hébergeur possède des dispositifs de stockage. L'opérateur d'un site Internet qui autorise les utilisateurs à poster des messages joue également le rôle d'hébergeur.

(12) Lien hypertexte

Les rédacteurs ont décidé de réglementer la responsabilité pénale des fournisseurs de liens hypertextes. Dans ce contexte, la loi fournit une définition large de «lien hypertexte», afin de couvrir les différentes solutions techniques.

(13) Interception

L'interception des processus de transfert de données est un instrument de procédure que l'on trouve dans différentes approches internationales de lutte contre la cybercriminalité. Toutefois, la plupart de ces instruments ne spécifient pas les actes ou ne fournissent pas les détails des procédures d'enquêtes légales. Les rédacteurs ont décidé d'inclure des exemples d'actes légitimes, ainsi que des types de communication pouvant être interceptées.

(14) Courriers électroniques multiples

Les rédacteurs ont reconnu l'impact négatif potentiel du spam pour les pays en développement. Un élément essentiel de la criminalisation du spam est la définition de courriers multiples. À cet égard, les rédacteurs ont décidé d'exiger au moins mille (1 000) messages.

(15) Logiciel de criminalistique à distance

Un des aspects ayant fait l'objet de discussions intenses durant les négociations relatives au texte législatif a été la réalisation de procédures d'enquêtes pointues. Les rédacteurs ont pris note des rapports sur l'utilisation de logiciels de criminalistique à distance dans les enquêtes nationales. Concernant la définition de «logiciel de criminalistique à distance», ils ont décidé de mettre l'accent sur les domaines possibles dans lesquels ces logiciels pourraient être utilisés (enregistrement de frappes et transmission d'adresses IP), mais de ne pas limiter à ces fonctions le champ d'application de ces logiciels.

(16) Saisir

La saisie de preuve est un processus d'enquête classique. En tenant compte du fait qu'en plus de la saisie de matériel, il existe diverses manières de collecter les preuves, les rédacteurs ont décidé de développer davantage cette définition en fournissant des exemples d'activités faisant partie de la saisie des preuves. L'un des exemples inclus dans les définitions est l'autorisation d'activer le système informatique du suspect. Les rédacteurs ont jugé utile d'indiquer qu'il s'agit d'une exigence essentielle pour les enquêtes pointues.

(17) Fournisseur de services Internet

Au lieu de fournir une seule définition de «fournisseur de services Internet», les rédacteurs ont décidé de différencier les types de prestataires.

(18) Données relatives au trafic

L'interception des données de trafic est un important processus d'enquête. Les rédacteurs ont décidé de fournir un ensemble de critères définissant clairement et limitant ainsi l'applicabilité de la disposition aux catégories de données concernées.

(19) Objet

Les objets sont les produits des saisies. L'interprétation du terme est laissée aux tribunaux nationaux, mais les rédacteurs ont décidé de fournir une série d'exemples.

(20) Utiliser

La définition du terme «utiliser» est pertinente pour l'emploi de logiciels de criminalistique à distance. Suite à des discussions intenses durant la séance du Groupe de travail, les rédacteurs ont décidé de préciser que non seulement l'utilisation de tels logiciels est couverte par la disposition, mais les activités préparatoires également.

TITRE II

Introduction aux Articles 4 à 15

L'objectif des Articles 4 à 15 du texte législatif est d'améliorer les moyens d'empêcher les crimes liés à l'informatique et aux réseaux et d'enquêter sur ceux-ci, en établissant une norme minimale commune des infractions concernées, sur la base des meilleures pratiques prévalant dans la région ainsi que des normes internationales. Dans ce contexte, la définition de normes dans les Articles 4 à 15 aidera les législateurs

nationaux à identifier les possibles lacunes du droit national et à former également la base d'une coopération internationale plus étroite exigeant en général un degré similaire de criminalisation en vertu du principe de double criminalité. Les Articles 4 à 15 fournissent une définition des normes minimales. Par conséquent, ils n'empêchent pas une criminalisation plus étendue à l'échelle nationale.

Durant les discussions, le groupe de travail a décidé d'ajouter certaines circonstances spéciales afin de restreindre la criminalisation qui résulte des différentes évaluations de la nature dangereuse du comportement impliqué ou de la nécessité d'utiliser le droit pénal comme contre-mesure dans la région. Cette approche offre de la souplesse aux différents États pour définir leur politique criminelle dans ce domaine.

Article 4: Accès illégal

Cette disposition criminalise le fait d'accéder à un système informatique. L'intérêt juridique protégé est l'intégrité du système informatique. La nécessité de criminaliser de tels actes reflète l'intérêt, pour les opérateurs ou les systèmes informatiques, de gérer leurs systèmes de manière paisible. La moindre intrusion non autorisée, pas seulement les crimes qui s'ensuivent, comme l'atteinte à l'intégrité des données, doit par conséquent être criminalisée, car elle peut créer des obstacles pour les utilisateurs légitimes des systèmes et générer des coûts de reconstruction élevés. Cette disposition complète les approches techniques visant à empêcher de tels comportements (par exemple, des mesures de protection des mots de passe) et permet aux services de répression de réaliser des enquêtes lorsque les contrevenants parviennent à commettre l'infraction.

Le terme «accès» ne se réfère pas à un certain moyen de communication, mais est ouvert et permet d'autres évolutions techniques. Il inclut tous les moyens d'entrer dans un autre système informatique, notamment les attaques Internet, ainsi que l'accès illégal aux réseaux sans fil. Même l'accès non autorisé à un ordinateur qui n'est pas connecté à un réseau (par exemple en contournant une protection par mot de passe) est couvert par la disposition. Comme toutes les autres infractions mentionnées dans le présent document, l'Article 4 impose que le contrevenant commette les infractions de manière intentionnelle. Par conséquent, les actes irresponsables ne sont pas couverts.

L'accès à un système informatique ne peut être poursuivi qu'aux termes de l'Article 4, s'il a lieu «sans motif ou justification légitime». Cela nécessite que le contrevenant agisse sans autorité (qu'elle soit législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) et que ce comportement ne soit pas autrement couvert par des moyens, motifs, justifications ou principes juridiques établis. L'accès à un système permettant l'accès libre et ouvert du public ou l'accès à un système avec l'autorisation du propriétaire ou d'autres ayants droit n'est par conséquent pas criminalisé. Les administrateurs de réseau et les entreprises de sécurité qui testent la protection des systèmes informatiques pour identifier les potentielles lacunes dans les mesures de sécurité ne commettent pas d'acte criminel.

Le fait que la victime du crime ait donné un mot de passe ou un code d'accès similaire au délinquant, par exemple parce que celui-ci l'a persuadé de le divulguer grâce à une approche réussie d'ingénierie sociale, ne signifie pas nécessairement que le contrevenant ait agi de manière légitime lorsqu'il a accédé au système informatique de la victime.

Article 5: Présence illégale

Cette disposition criminalise la présence illégale dans un système informatique. De manière similaire à l'Article 4, l'intérêt juridique protégé est l'intégrité du système informatique. La disposition, qui, de manière similaire, n'est contenue ni dans la Loi type du Commonwealth, ni dans la Convention du Conseil de l'Europe sur la cybercriminalité, reflète le fait que l'intégrité d'un système informatique peut être violée non seulement en entrant sans autorisation dans un système informatique, mais également en restant dans le système après expiration de l'autorisation. Un tel comportement ne peut pas être couvert par l'Article 4, car dans ce cas le contrevenant n'est pas entré illégalement dans le système.

La présence illégale suppose que le contrevenant ait toujours accès au système informatique. Cela peut être le cas s'il reste connecté ou continue d'effectuer des opérations. Le fait qu'il ait la possibilité théorique de se connecter au système informatique ne suffit pas.

L'Article 4 implique que le délinquant commette des infractions de manière intentionnelle. Les actes irresponsables ne sont pas couverts par cet article. L'Article 4 ne criminalise que les actes qui sont commis «sans motif ou justification légitime.»

Article 6: Interception illégale

Cette disposition vise à assimiler la protection des transferts électroniques à la protection des conversations vocales contre l'exploitation illégale et/ou l'enregistrement illégal existant déjà dans la plupart des systèmes juridiques. L'infraction en général s'applique à toutes les formes de transfert de données électroniques (par exemple, téléphone, télécopie, transfert de fichier ou courrier électronique).

L'applicabilité de l'Article 3 se limite à l'interception des transmissions réalisées par des moyens techniques. L'interception liée aux données électroniques peut être définie comme tout acte d'acquisition de données durant un processus de transfert. L'interception liée aux données électroniques peut être définie comme tout acte d'acquisition de données durant un processus de transfert. Elle peut avoir lieu en écoutant, suivant ou surveillant le contenu des communications. Cette disposition ne s'applique qu'à l'interception des transmissions; par conséquent, l'accès à des informations stockées n'est pas considéré comme l'interception d'une transmission.

Le terme «transmission» couvre tous les transferts de données, qu'ils aient lieu par téléphone, télécopie, courrier électronique ou transfert de fichier. L'infraction établie au titre de l'Article 6 ne s'applique qu'aux transmissions non publiques. Une transmission est «non publique» lorsque le processus de transmission est confidentiel. L'élément vital utilisé pour faire la différence entre les transmissions publiques et non publiques n'est pas la nature des données transmises, mais la nature du processus de transmission lui-même. Même l'interception d'informations publiquement disponibles peut être considérée comme délictueuse si les parties impliquées dans le transfert ont l'intention de garder secret le contenu de leurs communications. L'utilisation de réseaux publics n'exclut pas les communications «non publiques».

L'inclusion d'émissions électromagnétiques dans le texte législatif garantit qu'une approche complète a été adoptée, étant donné, en particulier, que les ordinateurs anciens génèrent des émissions électromagnétiques durant leur fonctionnement. Il était nécessaire que les émissions non couvertes par le terme «données» dans le texte législatif soient spécifiquement criminalisées.

L'Article 6 implique que le contrevenant effectue ou commette les infractions de manière intentionnelle et sans motif ou justification légitime. Ce n'est pas le cas si l'interception a lieu sur la base d'instructions ou avec l'autorisation des participants à la transmission, ou s'il s'agit d'une interception légitime basée sur des dispositions du droit pénal.

Article 7: Atteinte à l'intégrité des données

L'Article 7 vise à combler les lacunes existantes dans le droit pénal de certains pays et à fournir aux données informatiques et aux programmes informatiques des protections similaires à celles dont bénéficient les objets matériels contre les dommages causés intentionnellement.

Les termes «endommagement» et «détérioration» désignent tout acte lié à l'altération négative de l'intégrité de données et de logiciels. Dans une certaine mesure, ces deux termes se recoupent de manière importante. Le terme «effacement» désigne les actes par lesquels l'information est supprimée d'un support de stockage. Il est considéré comme comparable à la destruction d'un objet matériel. Jeter un fichier dans la corbeille électronique ne supprime pas le fichier du disque dur et n'est, par conséquent,

pas considéré comme un acte d'effacement, mais il peut être couvert par l'expression «refus d'accès». Le terme «altération de données» désigne la modification de données existantes, sans nécessairement diminuer leur disponibilité. Cet acte couvre notamment l'installation de logiciels malveillants comme des logiciels espions, des virus ou des publiciels sur l'ordinateur de la victime, même s'ils ne fonctionnent pas par la suite.

L'expression «rendre les données dénuées de sens» désigne tous les actes portant atteinte à l'intégrité des données et qui empêchent leur utilisation prévue. Cet acte implique que les données étaient auparavant utiles ou efficaces.

«Obstruction, interruption ou interférence avec l'utilisation légitime ou avec toute personne dans l'utilisation légitime de données» désigne toute action qui influence de manière négative un processus légal de traitement des données. L'application de cette disposition est particulièrement discutée en matière d'attaques par déni de service. Durant l'attaque, les données fournies sur le système informatique visé ne sont plus disponibles pour les potentiels utilisateurs légitimes, ni pour le propriétaire du système informatique. Toutefois, une disposition plus spécifique (Article 9) a été introduite afin de garantir la criminalisation de tels actes.

La suppression de données informatiques désigne une action qui affecte la disponibilité des données pour la personne ayant accès au support, où les informations sont stockées de manière négative.

L'Article 6 implique que le contrevenant effectue les infractions de manière intentionnelle et sans motif ou justification légitime. Le droit d'altérer les données a été examiné, en particulier dans le contexte des «remailers» qui sont utilisés pour modifier certaines données afin de permettre l'anonymat des communications. L'utilisation intentionnelle de tels services est considérée comme une autorisation à effectuer les altérations nécessaires.

Article 8: Espionnage des données

La Convention sur la cybercriminalité comme la Loi type du Commonwealth et le projet de Convention de Stanford présentent des solutions juridiques à l'interception illégale, mais pas à l'obtention illégale de données. On peut se demander si l'Article 3 de la Convention sur la cybercriminalité s'applique à d'autres cas qu'aux infractions commises en interceptant des processus de transfert de données.

L'Article 8 garantit le secret des données informatiques stockées et protégées. Contrairement à d'autres approches, cet article couvre non seulement les secrets économiques, mais aussi les données informatiques stockées en général. En termes d'objectifs de protection, cette approche est large, mais l'application de cette disposition est limitée puisque l'obtention de données n'est criminalisée que lorsque ces données sont spécialement protégées contre tout accès non autorisé. La protection spéciale exige que l'hébergeur des informations ait mis en place des mesures de protection rendant bien plus difficile l'obtention de données sans autorisation. Il peut s'agir, par exemple, de protection par mot de passe ou de cryptage. Il est nécessaire que les mesures de protection aillent au-delà des mesures de protection standard qui s'appliquent aux données, ainsi qu'à d'autres biens, comme les restrictions d'accès à certaines parties de bâtiments gouvernementaux. D'un autre côté, il n'est pas nécessaire que les mesures soient liées aux technologies informatiques. Même des mesures physiques telles que des verrous permettent l'application de la disposition.

L'acte d'obtention couvre toute activité entreprise par le contrevenant pour entrer en possession des données concernées. Cela peut, par exemple, être effectué en retirant un dispositif de stockage ou en copiant les fichiers de la source d'origine sur le support de stockage du délinquant.

Article 9: Atteinte à l'intégrité du système

Afin de protéger l'accès des opérateurs et des utilisateurs aux TIC, une disposition a été incluse et criminalise l'entrave intentionnelle à l'utilisation légitime d'un système informatique. Cette disposition vise par conséquent à protéger l'intégrité des systèmes informatiques. L'application de cette disposition implique que le contrevenant entrave ou porte atteinte au fonctionnement d'un système informatique.

Le terme «entrave» se rapporte à tout acte qui porte atteinte au bon fonctionnement d'un système informatique. Le terme est défini plus en détail à l'Article 3. Le Groupe de travail a examiné si le problème des spams électroniques pouvait être résolu aux termes de l'Article 5, puisque les spams peuvent surcharger les systèmes informatiques. Dans la mesure où l'application d'une disposition similaire dans la Convention sur la cybercriminalité concernant le spam a été difficile, les rédacteurs ont décidé d'inclure une disposition spécifique sur le spam à l'Article 15. L'Article 9 implique que le contrevenant commette l'infraction de manière intentionnelle et sans motif ou justification légitime. En conséquence, les tests autorisés de sécurité informatique ne seront pas criminalisés.

L'alinéa 2 prévoit une sanction plus lourde si les infractions affectent l'infrastructure critique. Le fonctionnement d'un système informatique est devenu essentiel pour le contrôle d'infrastructures critiques comme la santé, le transport et la fourniture d'énergie. L'alinéa 2 prend donc cette menace en compte, en offrant la possibilité d'envisager des peines plus importantes.

Deux cas différents sont mentionnés à l'alinéa 2, à savoir (1) affecter les systèmes informatiques exclusivement utilisés pour les opérations des infrastructures critiques et (2) affecter les systèmes informatiques qui n'exploitent pas exclusivement les infrastructures critiques, mais qui figurent parmi d'autres objectifs utilisés pour la protection des infrastructures critiques. Dans le second cas, il est nécessaire de prouver que le comportement a eu lieu à un moment où le système informatique effectuait des opérations d'infrastructures critiques.

Article 10: Dispositifs illégaux

Le paragraphe 1(a) définit les dispositifs destinés à commettre et promouvoir la cybercriminalité ainsi que les mots de passe qui permettent d'accéder à un système informatique. Le terme «dispositifs» couvre le matériel, ainsi que des solutions basées sur des logiciels pour commettre l'une des infractions mentionnées. Ces logiciels incluent par exemple des programmes virus ou des programmes conçus ou adaptés pour accéder à des systèmes informatiques. Contrairement aux dispositifs, les mots de passe, code d'accès ou données informatiques similaires n'effectuent pas des opérations, mais sont des codes d'accès. Il s'agit par exemple de mots de passe publiés qui permettent d'accéder à des bases de données ou des services payants. La publication des vulnérabilités d'un système, qui pourraient servir d'instructions pour contourner les mesures de protection, n'est pas couverte par la disposition dès lors qu'elles ne contiennent pas de codes d'accès. Contrairement aux systèmes de code d'accès classique, les vulnérabilités ne permettent pas nécessairement un accès immédiat à un système informatique, mais elles permettent à l'auteur de les utiliser pour réussir à attaquer un système informatique.

Le terme «production» désigne tout processus de création d'un dispositif ou d'un mot de passe. La production de parties non exécutables d'un logiciel n'est pas couverte. Le terme «vente» désigne les activités exécutées pour la vente de dispositifs et de mots de passe en contrepartie d'argent ou d'autres compensations. L'expression «obtention pour utilisation» couvre des actes liés à l'obtention active de mots de passe et de dispositifs. Le fait que l'acte d'obtention soit lié à l'utilisation de tels outils requiert, en général, une intention de l'auteur d'approvisionner les outils à utiliser qui va au-delà de l'intention «régulière», et qu'ils soient utilisés pour commettre l'une ou l'autre des infractions visées au Titre II.

Le terme «importation» couvre des activités d'obtention de dispositifs et de codes d'accès à partir de pays étrangers. Il en résulte que des contrevenants qui importent de tels outils pour les vendre peuvent être poursuivis avant même d'offrir ces outils à la vente. Concernant le fait que l'obtention de tels outils n'est criminalisée que si elle peut être liée à l'utilisation, on peut se demander si la seule importation sans intention de vendre ou d'utiliser les outils est couverte par l'Article 10.

Le terme «exportation» désigne l'expédition, la transmission ou le transfert effectif de dispositifs ou de codes d'accès en dehors d'un pays, ainsi que le transfert de dispositifs ou de codes d'accès au sein d'un pays, avec la connaissance ou l'intention que ces dispositifs ou codes d'accès seront expédiés, transférés ou transmis à l'extérieur du pays. Le terme «diffusion» couvre les actes de transmission de dispositifs ou de mots de passe à des tiers. L'expression «obtention pour utilisation» couvre des actes liés à l'obtention active de mots de passe et de dispositifs. L'expression «mise à disposition» désigne un acte permettant à d'autres utilisateurs d'avoir accès à des objets. Elle couvre également la création ou la compilation de liens hypertextes visant à faciliter l'accès à ce service.

Cette disposition en général s'applique non seulement aux dispositifs exclusivement conçus pour faciliter la commission d'infractions informatiques, mais également aux dispositifs généralement utilisés à des fins légitimes et pour lesquels l'intention spécifique des auteurs est de commettre des infractions. La limitation aux dispositifs conçus uniquement pour commettre des crimes est trop restrictive et peut entraîner des difficultés insurmontables en ce qui concerne l'établissement de la preuve dans les procédures pénales, ce qui rend cette disposition quasiment inapplicable ou applicable dans de rares cas seulement. Une précision a été ajoutée à l'alinéa 3 afin que les tests autorisés ne soient pas affectés.

L'Article 10 impose que le délinquant commette des infractions de manière intentionnelle. Outre l'intention régulière concernant les actes couverts, l'Article 10 impose également l'intention spéciale que le dispositif soit utilisé dans le but de commettre l'une des infractions établies au Titre II.

L'alinéa 2 contient une présomption légale selon laquelle il est considéré que tout suspect en possession de plus d'un élément mentionné aux alinéas 1 (i) et (ii) possède cet élément dans l'intention criminelle exigée, sauf preuve du contraire.

L'Article 10 implique que le contrevenant agisse sans motif ou justification légitime. Dans ce contexte, la précision dans les alinéas doit être prise en compte. En conséquence, l'utilisation légitime d'outils logiciels dans le cadre des mesures d'autoprotection n'est pas considérée comme étant effectuée sans motif légitime.

Article 11: Falsification informatique

La plupart des législations pénales criminalisent la falsification de documents matériels. La structure dogmatique des approches juridiques nationales varie d'une juridiction à l'autre. Alors qu'un concept est basé sur l'authenticité de l'auteur du document, un autre repose sur l'authenticité de la déclaration. L'Article 11 vise à protéger la sécurité et la fiabilité des données électroniques en créant une infraction parallèle à la falsification classique de documents matériels afin de combler les lacunes du droit pénal, dans la mesure où les dispositions juridiques classiques liées à la falsification peuvent ne pas s'appliquer aux données stockées de manière électronique.

La falsification informatique cible les données informatiques telles que définies par l'Article 3. Dans ce contexte, peu importe qu'elles soient directement lisibles et/ou intelligibles. Cette disposition ne se réfère pas seulement aux données informatiques en tant qu'objet de l'un des actes mentionnés; il est également nécessaire que ces actes aboutissent à des données non authentiques. L'Article 11 impose, du moins en ce qui concerne l'élément moral de l'infraction, que les données soient l'équivalent d'un document public ou privé.

L'entrée de données doit correspondre à la production d'un faux document matériel. Le terme «altération» se réfère à la modification de données existantes. La suppression de données informatiques se réfère à une action qui affecte la disponibilité des données. Il peut s'agir, par exemple, d'informations pertinentes provenant d'une base de données, qui sont bloquées durant la création automatique d'un document électronique. Le terme «effacement» est défini à l'Article 4 et couvre les actes par lesquels des informations sont retirées.

L'Article 11 impose que le délinquant effectue les infractions de manière intentionnelle et sans motif ou justification légitime.

Article 12: Fraude informatique

La fraude est un délit courant dans le cyberespace. L'application de dispositions existantes à des cas liés à Internet peut s'avérer difficile lorsque les dispositions législatives criminelles nationales classiques sont basées sur la fausseté de la personne. C'est la raison pour laquelle le Groupe de travail a décidé d'inclure une disposition criminalisant la fraude informatique.

L'Article 12 présente une liste des actes de fraude informatique les plus courants. Il est nécessaire que les manipulations du contrevenant entraînent une perte économique ou matérielle directe pour un tiers, notamment une perte d'argent et de biens matériels ou immatériels ayant une valeur économique.

L'introduction de données informatiques couvre tous les types de manipulations d'introduction, comme l'introduction de données incorrectes dans l'ordinateur, ainsi que les manipulations de logiciels et autres interférences avec le traitement de données. Le terme «altération» se réfère à la modification de données existantes. La suppression de données informatiques se réfère à une action qui affecte la disponibilité des données. Le terme «suppression» désigne le retrait de données informatiques.

L'expression «atteinte au fonctionnement d'un système informatique», telle que mentionnée en b), couvre les actes tels que les manipulations de matériels, les actes empêchant les sorties sur imprimante et les actes affectant les enregistrements ou les flux de données ou l'ordre dans lequel les programmes sont exécutés.

De manière similaire à l'application des autres dispositions du texte législatif, l'Article 11 impose que le contrevenant agisse de manière intentionnelle. Cette intention se réfère à la manipulation, ainsi qu'à l'incidence des pertes financières subséquentes. En outre, l'Article 12 impose que le contrevenant ait agi dans une intention frauduleuse ou malhonnête en vue d'obtenir un avantage économique ou autre pour lui-même ou pour un tiers. Les actes exclus de la responsabilité criminelle par suite d'un manque d'intention particulière sont, par exemple, les pratiques commerciales relatives à la concurrence qui peuvent causer un préjudice économique à une personne et apporter un bénéfice à une autre, mais qui ne sont pas pratiquées dans une intention frauduleuse ou malhonnête.

De plus, l'Article 12 implique que le contrevenant agisse sans motif ou justification légitime.

Article 13: Pédopornographie ou pornographie infantile

L'Article 13 contient une large criminalisation des actes liés à la pédopornographie. La criminalisation de la pédopornographie vise à protéger plusieurs intérêts juridiques. En criminalisant la production de ce type de pornographie, cette disposition vise à empêcher les enfants d'être victimes d'abus sexuels. Concernant l'interdiction des actes liés à l'échange de pornographie infantile (offre, diffusion), ainsi qu'à la possession de pornographie infantile, la criminalisation de tels actes vise à anéantir le marché des matériels pédopornographiques, puisque la demande constante en nouveaux matériels peut motiver les contrevenants à continuer d'abuser des enfants. En outre, l'interdiction d'échanger des contenus vise à empêcher les personnes d'avoir accès à ces matériels et ainsi éviter un effet domino concernant les abus d'enfants.

Le terme «produire» désigne tout processus de création de pornographie. Il est nécessaire que la production de pornographie infantile soit effectuée en vue de sa diffusion par le biais d'un système informatique. Si le contrevenant produit le matériel pour son propre usage ou qu'il a l'intention de le distribuer sous une forme non électronique, l'Article 9 de la Convention sur la cybercriminalité n'est pas applicable.

Le terme «offrir» couvre les actes sollicitant autrui à obtenir de la pornographie infantile. Il n'est pas nécessaire que ces matériels soient offerts de manière commerciale, mais que la personne qui les offre soit en mesure de les fournir. L'expression «mettre à disposition» désigne un acte permettant à d'autres utilisateurs d'avoir accès à des matériels pédopornographiques. Cet acte peut être commis en mettant des matériels pédopornographiques sur des sites Internet ou en se connectant à des systèmes de partage de fichiers et en permettant à des tiers d'accéder à ces matériels sur des supports ou des dossiers de stockage non verrouillés.

Le terme «diffuser» correspond à l'acte de transmettre des matériels pédopornographiques à des tiers. Le terme «transmettre» couvre toutes les communications au moyen de signaux transmis. L'expression «obtenir pour soi-même ou pour autrui» couvre tout acte d'obtention active de pornographie infantile. Le terme «posséder» désigne le contrôle exercé de manière intentionnelle par une personne sur la pornographie infantile. Cela implique que le contrevenant a le contrôle non seulement de dispositifs de stockage local, mais aussi de dispositifs à distance auxquels il peut accéder et qu'il peut contrôler. En outre, la possession en général exige un élément moral tel qu'énoncé dans la définition ci-dessus. L'expression «obtenir l'accès» couvre tout acte de déclenchement du processus d'affichage d'informations rendues disponibles au moyen de technologies d'information et de communication. C'est par exemple le cas si le contrevenant entre le nom de domaine d'un site Internet de pédopornographie connu et qu'il déclenche le processus de réception d'informations à partir de la page d'accueil, lequel s'accompagne d'un processus nécessaire de téléchargement automatique. Cela permet aux services de répression de poursuivre les contrevenants lorsqu'ils sont en mesure de prouver que le contrevenant a ouvert des sites Internet de pédopornographie, mais qu'ils ne sont pas capables de prouver que le contrevenant a téléchargé du matériel. Il est difficile de collecter des preuves, par exemple, si le délinquant recourt à une technologique de cryptage pour protéger les fichiers téléchargés sur son support de stockage. Cette disposition s'applique également dans les cas où la consommation de pornographie infantile peut avoir lieu sans téléchargement de matériel. Ce peut être le cas si le site Internet autorise les vidéos en flux continu et si, compte tenu de la configuration technique de ce processus, il ne met pas les informations reçues en mémoire tampon, mais les élimine juste après les avoir transmises.

Les rédacteurs ont décidé de permettre aux pays de ne pas criminaliser le comportement décrit à l'Article 13(1)(d)-(f).

Article 14: Infractions liées à l'identité

Cette disposition couvre les principales phases des infractions typiques liées à l'identité. Seule la phase d'obtention d'informations liées à l'identité n'est pas couverte par cette disposition, cet acte étant couvert par les autres dispositions du Titre II du texte législatif.

Le terme «transférer» désigne le processus de transmission de données d'un ordinateur à un autre système informatique. Il s'applique si les bases de données disposant d'informations liées à l'identité obtenues de manière illégale sont transférées à des groupes criminels qui organisent la vente de telles informations. Le terme «posséder» désigne le contrôle exercé de manière intentionnelle par une personne sur des informations liées à l'identité. Le terme «usage» couvre un large éventail de pratiques, telles que la soumission de ces informations pour effectuer des achats en ligne.

Il est nécessaire que le contrevenant effectue cette action de manière intentionnelle et qu'il ait en outre l'intention particulière de commettre, d'aider ou d'encourager une infraction.

Article 15: Spam

Cette provision traite de la question du spam en criminalisant trois (3) des principaux actes que la plupart des envois de spam ont en commun. Outre le fait de limiter la criminalisation à trois actes majeurs, le contrevenant ne peut être poursuivi que si son acte affecte le commerce. La variante a) couvre le déclenchement de la transmission de courriers électroniques multiples. Elle criminalise le transfert de courriers de masse sans la permission du destinataire. La limitation de la criminalisation d'actes perpétrés sans motif ou justification légitime joue un rôle important pour distinguer les courriers de masse légitimes (comme les lettres d'information) du spam illégal. La variante b) criminalise le contournement des technologies antispam en abusant des systèmes informatiques protégés pour relayer ou transmettre des messages électroniques. Il est nécessaire que le contrevenant agisse de manière intentionnelle dans le but de tromper ou d'induire en erreur le destinataire ou les prestataires concernés. La variante c) couvre le contournement des technologies antispam en falsifiant les informations se trouvant dans les en-têtes. Selon le type de manipulation, un tel acte peut également être couvert par l'Article 11 du texte législatif.

L'Article 15 impose que le contrevenant effectue les infractions de manière intentionnelle et sans motif ou justification légitime. Par conséquent, les tests informatiques autorisés ne doivent pas être criminalisés. En raison d'opinions divergentes quant à la nécessité de criminaliser la diffusion de spams, les rédacteurs ont décidé de laisser à la discrétion des pays le choix de ne pas criminaliser un tel comportement dans l'Article 15(2)(a), à la condition que d'autres recours efficaces existent.

Article 16: Divulgation des détails d'une enquête

La confidentialité des enquêtes peut être d'une grande importance pour les objectifs et les stratégies utilisés dans la réalisation de telles activités. C'est particulièrement le cas si les enquêtes ne sont pas encore achevées et que les preuves pertinentes en question pourraient être modifiées. À cet égard, cette mesure répond à la nécessité, pour les services de répression, de veiller à ce que le suspect faisant l'objet de l'enquête ne soit pas au courant de ladite enquête, ainsi qu'au droit des personnes à la vie privée. Ce dernier est inclus pour protéger la vie privée du sujet des données ou d'autres personnes pouvant être mentionnées ou identifiées dans ces données.

Article 17: Refus d'assistance

Souvent, les services de répression dépendent de l'assistance d'administrateurs système et d'autres personnes ayant des connaissances spécifiques pour identifier le lieu de stockage des preuves ou obtenir l'accès aux informations stockées. L'Article 20 établit une mesure coercitive pour faciliter la perquisition et la saisie de données informatiques. L'Article 17 établit les conséquences du non-respect de cette obligation. À cet égard, «refus» implique que le contrevenant pouvait faire preuve d'objectivité et était personnellement capable de suivre l'ordre.

Article 18: Harcèlement au moyen de communications électroniques

En raison de sa pertinence croissante pour les pays des Caraïbes, les rédacteurs ont décidé d'inclure une disposition criminalisant le harcèlement au moyen de communications électroniques. Cette criminalisation exige que le contrevenant ait déclenché une communication électronique. Une communication électronique est déclenchée si, par exemple, le délinquant envoie un courriel ou un message dans un «chat». La disposition impose, par ailleurs, qu'il utilise un système informatique pour encourager les comportements graves, répétés et hostiles. Enfin, elle impose que le contrevenant agisse avec une intention particulière (intention de contraindre, d'intimider, de harceler, ou de provoquer une importante détresse émotionnelle).

Partie III

TITRE III

Article 19: Juridiction

Cet Article présente un ensemble de critères pour établir les compétences relatives aux infractions criminelles énumérées aux Articles 4-17. L'Article 19 a) se base sur le principe de territorialité. La juridiction territoriale est déclenchée si la personne qui attaque un système informatique et le système victime se trouvent dans le même territoire ou pays. Ce principe s'applique également si le système informatique attaqué se trouve sur le territoire de la juridiction, même si ce n'est pas le cas du contrevenant.

L'Article 19 b) contient des variantes du principe de territorialité. Elles imposent que chaque partie établisse une juridiction pénale pour les infractions commises sur tout bateau battant son pavillon ou tout avion immatriculé conformément à son droit. Ces deux principes font déjà partie des principes de juridiction en dehors de la cybercriminalité, puisque les bateaux et les avions sont souvent considérés comme une extension du territoire d'un État. Si le crime est commis sur un bateau ou un avion au-delà du territoire de l'État du pavillon, il n'y a en général aucun exercice de la juridiction. La connexion étant de plus en plus souvent proposée à bord des avions et des bateaux, ce principe pourrait devenir plus pertinent.

L'Article 19 c) se base sur le principe de nationalité. Le principe de nationalité est le plus fréquemment appliqué par les pays de droit civil. Si un ressortissant commet une infraction à l'étranger, l'État est tenu d'avoir la possibilité d'engager des poursuites correspondantes si l'acte constitue également une infraction en vertu du droit de l'État dans lequel elle a été commise ou si l'acte ne relève de la compétence territoriale d'aucun État.

TITRE IV

Articles 20 à 27

En matière de cybercriminalité, une enquête réussie exige que les services de répression aient accès aux instruments appropriés nécessaires à la réalisation de celle-ci. L'identification des contrevenants ainsi que la protection de l'intégrité des données informatiques durant l'enquête entraînent plusieurs difficultés inhérentes uniques pour les services de répression. L'objectif du Titre IV est d'améliorer les instruments de procédure nationaux en définissant des normes minimales standard basées sur les meilleures pratiques dans la région, ainsi que sur les normes internationales. Dans ce contexte, la définition de normes aidera les législateurs nationaux à découvrir de possibles lacunes dans le droit procédural de leur pays. Les Articles 20 à 27 ne définissent que les normes minimales. Par conséquent, ils n'empêchent pas l'élargissement de la criminalisation à l'échelle nationale.

Le Titre IV introduit de nouveaux instruments d'enquête (tels que l'Article 27) et vise également à adapter les mesures procédurales (telles que l'Article 20). Tous les instruments mentionnés visent à permettre l'obtention et/ou la collecte de données afin de réaliser des enquêtes ou des procédures pénales particulières. Les instruments décrits au Titre IV ne seront pas seulement utilisés dans les enquêtes traditionnelles portant sur la cybercriminalité, mais également dans toute enquête impliquant des données informatiques et des systèmes informatiques.

Les rédacteurs ont longuement discuté de l'importance des sauvegardes. Ils ont obtenu un consensus sur le fait que l'application des instruments de procédure prévus aux Articles 20 à 27 doit être soumise à des conditions et à des sauvegardes. Les rédacteurs ont discuté de la question de savoir s'il faut inclure un ensemble complet de sauvegardes ou s'il faut utiliser les sauvegardes existant déjà dans le droit national. Dans la mesure où ce texte législatif n'est pas directement applicable et qu'il ne fournit que des

recommandations pour l'ajustement et l'harmonisation des législations nationales, et compte tenu des différences pouvant exister dans la législation nationale de chaque pays des Caraïbes, les rédacteurs ont décidé de ne pas définir de sauvegardes, mais de laisser ce point au processus national de mise en œuvre, afin de veiller à ce que toutes les conditions ou sauvegardes pouvant être fournies de manière constitutionnelle, législative, juridique ou autre soient applicables en ce qui concerne les instruments du Titre IV. Dans la mesure où de nouveaux instruments peuvent être établis durant le processus de mise en œuvre, il peut se révéler nécessaire d'étendre les sauvegardes existantes pour maintenir l'équilibre entre les exigences de l'application des lois et la protection des libertés et des droits humains.

Les différences au sein des systèmes juridiques dans les Caraïbes ont non seulement été prises en compte en matière de sauvegardes, mais également en matière de définition des conditions d'application des instruments. Les dispositions offrent des options d'ajustement quant à l'autorité en charge d'ordonner l'application d'un instrument (par exemple, un juge, un magistrat, un service de répression, un agent de police), le fondement d'une action (par exemple les informations obtenues sous serment ou une déclaration sous serment), le degré de certitude (par exemple «soupçonner» ou «croire»), ainsi que la nécessité de répondre (par exemple «peut» ou «doit»). Enfin, les rédacteurs ont décidé de permettre aux pays de différer la mise en œuvre de certaines procédures. Concernant les normes différentes relatives à la capacité à intercepter une communication, la capacité de restreindre les instruments de procédure a été spécifiquement prévue.

Tous les instruments énumérés aux Articles 20 à 27 ne s'appliquent qu'aux enquêtes menées sur le territoire de l'État responsable de l'enquête. Concernant la dimension transnationale de la cybercriminalité, les rédacteurs ont discuté de la nécessité d'ajouter un ensemble séparé de dispositions spécifiques à la coopération internationale dans les enquêtes transnationales sur la cybercriminalité. Toutefois, les rédacteurs ont convenu que compte tenu du mandat du Groupe de travail, la réglementation sur la coopération internationale ne devrait pas être incluse.

Article 20: Perquisition et saisie

Même dans la criminalité liée à la haute technologie, le processus de perquisition et de saisie reste un important processus d'enquête. En général, les procédures pénales nationales qui prévalent incluent des pouvoirs de perquisition et de saisie en matière d'objets matériels. Toutefois, dans la mesure où certaines juridictions ne traitent pas les données informatiques comme des objets et qu'elles ne permettent que la recherche d'objets matériels, cet article vise à moderniser les lois nationales relatives à la perquisition et à la saisie de données informatiques stockées en établissant un pouvoir équivalent en matière de données stockées.

L'objectif de l'Article 20(1) est de faciliter le processus de collecte des preuves numériques. La disposition précise qu'un mandat est nécessaire pour entreprendre toute opération de perquisition. Cela s'applique aux données informatiques stockées. Si un tel mandat est émis, il autorise les services de répression non seulement à activer un système informatique ou à y accéder sous une autre forme, mais aussi à entrer chez le suspect. L'application du processus ne se limite pas aux seuls cas où des preuves définitives d'une infraction peuvent être collectées, mais aussi aux cas où les données informatiques ont été acquises par une personne suite à une infraction.

Afin de veiller à ce que la formulation de la disposition n'entrave pas l'application de techniques d'enquête avancées, les rédacteurs ont décidé de ne pas spécifier les techniques pouvant être utilisées pour effectuer une perquisition ou accéder à un système informatique. Le terme «perquisition» inclut, sans s'y limiter, la recherche, la lecture, l'inspection ou l'examen des données.

L'Article 20(2) permet aux autorités chargées de l'enquête d'étendre leur perquisition ou d'obtenir un accès similaire à un autre système informatique en tout ou en partie, si certaines conditions sont remplies. Les rédacteurs ont décidé qu'une telle autorisation est nécessaire dans la mesure où les systèmes de stockage à distance sont de plus en plus utilisés. Concernant la limitation des instruments de

procédure aux enquêtes nationales, la disposition ne s'applique pas si les informations concernées sont stockées dans un système informatique à l'extérieur du territoire (même s'il est techniquement possible d'y accéder). La disposition ne prescrit pas comment une extension de la perquisition doit être entreprise, cet aspect étant laissé à la législation nationale.

L'Article 20(3) autorise les autorités compétentes à saisir ou à obtenir des preuves numériques. Le terme «saisir» est défini à l'Article 3. Outre les approches traditionnelles telles que la saisie de matériel informatique (notamment les dispositifs de stockage de données informatiques), la disposition permet aux autorités chargées d'enquêter de mener des enquêtes pointues et plus minimalistes, par exemple la production d'une copie des données en question. Étant donné que ces mesures pourraient conduire à la production de multiples copies, d'autres mesures sont nécessaires. En conséquence, les autorités compétentes peuvent inclure la capacité à retirer les données à leur source d'origine et à maintenir l'intégrité des données afin de veiller à ce qu'elles ne soient pas modifiées durant le processus d'enquête.

Article 21: Assistance

L'identification des preuves numériques pertinentes s'accompagne de difficultés particulières, notamment pour l'identification d'espaces de stockage physiques, compte tenu de la quantité de données pouvant être traitées et stockées, ainsi que des éventuelles mesures de sécurité mises en œuvre. L'assistance de personnes disposant de connaissances spécifiques (par exemple les administrateurs système) quant au fonctionnement d'un système informatique peut, par conséquent, être indispensable dans une enquête. Une telle coopération représente un avantage non seulement pour les autorités chargées d'enquêter, mais aussi pour les entreprises, dans la mesure où sans cette assistance, lesdites autorités peuvent être contraintes de rester sur les lieux perquisitionnés et d'empêcher l'accès au système informatique durant de longues périodes pendant qu'elles effectuent leurs enquêtes. Un tel allongement de l'enquête pourrait créer un désavantage économique pour les entreprises légitimes. Par conséquent, les rédacteurs ont décidé de créer une obligation pour les personnes concernées ayant des connaissances sur le fonctionnement d'un système informatique ou sur les mesures appliquées, de protéger les données informatiques qui s'y trouvent. Une telle assistance est cependant limitée à ce qui fait l'objet d'une demande raisonnable. L'Article 21 définit cinq (5) domaines d'assistance. Toutefois, les rédacteurs ont trouvé qu'il était important de souligner que la règle interdisant de témoigner contre soi-même entrave l'application de la disposition relative au suspect du crime.

Article 22: Injonction de produire

Les autorités compétentes disposent de divers processus et procédures puissants pour collecter les preuves électroniques pertinentes. L'un des processus les plus puissants est la perquisition et la saisie de données informatiques. Cela peut s'avérer particulièrement important lorsque, durant la réalisation d'une perquisition de données stockées sur les serveurs d'un hébergeur. De telles procédures peuvent porter atteinte au fonctionnement de l'entreprise (même si le prestataire aide les services de répression à identifier l'emplacement physique). Les rédacteurs ont donc décidé d'inclure un processus à l'Article 22(a) qui oblige une personne sur son territoire à fournir des données informatiques stockées spécifiées. Cette disposition ne doit pas être interprétée comme une obligation de conserver des données. L'application de cette disposition n'est pas limitée à certaines catégories de données et s'applique aux données relatives au contenu et au trafic. Concernant la réglementation spécifique des informations relatives aux abonnés, à l'Article 22(b), cette catégorie de données n'est pas incluse à l'Article 22(a). Afin d'empêcher un abus du processus, les rédacteurs ont limité les requêtes à celles où l'information fait l'objet d'une demande raisonnable. Outre ce critère, une injonction émanant d'une autorité compétente (magistrat/juge) est requise.

Dans les cas où les enquêteurs essaient d'identifier un suspect, ils peuvent ne pas se concentrer sur les données générées durant des communications électroniques, mais plutôt sur les informations relatives aux abonnés qui leur permettront de faire le lien entre un comportement criminel et une personne. Les rédacteurs ont décidé de traiter cette question dans un alinéa spécifique (Article 22(b)). L'Article 22(b) est

applicable à toute information personnelle relative à un abonné ou à une personne utilisant autrement un service Internet. Dans la mesure où les informations relatives aux abonnés ne sont disponibles que si un service est offert, l'obligation de produire ces données est limitée au fournisseur de services Internet. La disposition ne se limite pas aux informations relatives aux abonnés qui sont stockées de manière électronique, elle couvre également les enregistrements non électroniques.

Article 23: Conservation rapide

Les données informatiques nécessaires pour identifier un contrevenant ou prouver qu'un crime a été commis peuvent facilement être effacées ou modifiées avant que les enquêteurs ne puissent obtenir des preuves. La modification ou l'effacement ne se produit pas nécessairement dans l'intention de protéger le contrevenant (par exemple, les données de trafic utiles à l'identification sont souvent effacées de manière automatique très peu de temps après la fin d'une communication, car elles ne sont plus requises). Contrairement à d'autres approches internationales (par exemple la directive européenne sur la conservation des données), les rédacteurs ont décidé de ne pas prescrire la mise en œuvre d'obligations de conservation de données, mais d'établir un processus permettant aux services de répression d'ordonner la préservation de telles données lorsque c'est nécessaire.

Sur la base d'une injonction émise conformément à l'Article 23, toute personne recevant ainsi un ordre (hormis le suspect) est obligée de conserver les données qui ont été traitées durant l'exécution du service. L'Article 23 n'inclut pas l'obligation, pour la personne qui contrôle les données, de transmettre les données en question aux autorités compétentes. L'obligation de transmission est réglementée par les Articles 22 et 24. Après avoir reçu l'injonction, la personne contrôlant ces informations n'a pas le droit d'autoriser l'effacement manuel ou automatique des données spécifiées dans l'injonction, pendant une période de sept (7) jours. Les rédacteurs ont estimé que cette période était suffisante pour obtenir une injonction exigeant la transmission des données en question. Si l'injonction ordonnant la conservation rapide n'est pas suivie en temps voulu d'une injonction d'extension de la période ou d'une injonction de produire, la personne contrôlant les données est autorisée à effacer les informations stockées.

Afin de veiller à ce que les enquêteurs disposent d'un processus efficace pour empêcher l'effacement de preuves pertinentes, et en tenant compte du fait que l'Article 23 n'empêche que l'effacement d'informations sans donner aux services de répression l'accès à ces informations, les rédacteurs ont décidé de ne pas exiger d'injonction émanant d'un juge ou d'un magistrat. Cependant, l'Article permet à tout agent de police d'ordonner la conservation rapide. L'injonction de produire (Article 22) exigeant une injonction émanant de l'autorité compétente autorisée à le faire, les droits du suspect faisant l'objet de l'enquête sont correctement protégés.

La période de conservation peut être prolongée une (1) fois. Une telle extension doit se faire sur injonction d'un magistrat ou d'un juge.

Article 24: Divulgation partielle

Bien que les rédacteurs aient en principe convenu d'une distinction stricte entre l'autorisation d'ordonner la conservation des données (laquelle peut être émise par n'importe quel agent de police) et la transmission des données (laquelle exige une injonction par un magistrat ou un juge), ils ont souligné la nécessité de veiller à ce que les enquêteurs soient en mesure d'obtenir un accès immédiat à certaines données de trafic. Sans cette divulgation partielle, les enquêteurs ne seraient pas en mesure, dans certains cas, de suivre le délinquant et de conserver davantage de données utiles lorsque plusieurs fournisseurs sont impliqués. Contrairement à l'injonction de produire, cet instrument se limite aux données relatives au trafic.

Article 25: Collecte des données de trafic

Les rédacteurs ont reconnu que les données de trafic jouent un rôle important dans les enquêtes sur la cybercriminalité. Surveiller les données de trafic générées pendant l'utilisation de services Internet permet aux enquêteurs d'identifier l'adresse IP d'un contrevenant et de tenter ensuite d'identifier sa localisation physique. L'Article 25 présente deux (2) approches différentes: Selon l'Article 25(1), toute personne ayant le contrôle de données de trafic peut recevoir l'ordre de collecter ou d'enregistrer ces données ou d'autoriser et d'assister un agent de police à collecter ou enregistrer ces données. L'Article 25(2) contient un mandat qui autorise un agent de police à entreprendre la collecte des données relatives au trafic. La collecte des données de trafic ayant fait l'objet de discussions aussi controversées que celles relatives à l'interception des données de contenu, les rédacteurs ont décidé d'insister sur le fait que les pays peuvent, à leur discrétion, décider de ne pas mettre en œuvre l'Article 25.

Article 26: Interception des données relatives au contenu

Dans certains cas, la collecte des données de trafic ne suffit pas à assurer la condamnation du suspect. C'est particulièrement vrai lorsque les enquêteurs connaissent déjà le partenaire de communication et les services utilisés, mais qu'ils n'ont pas de détails sur les informations échangées. Les rédacteurs ont décidé d'inclure une disposition permettant l'interception des communications de données. Afin de garantir une approche harmonisée, la disposition a été rédigée conformément au modèle de texte législatif sur l'interception des communications.

L'Article 26 présente deux (2) approches différentes. Selon l'Article 26(a), un fournisseur de services Internet peut recevoir l'injonction d'enregistrer ou de collecter des données relatives au contenu. L'Article 26(b) autorise les services de répression à effectuer l'interception. Cette disposition ayant fait l'objet de polémiques durant les discussions du Groupe de travail, les rédacteurs ont convenu que les pays pourraient décider de ne pas mettre en œuvre l'Article 26.

Article 27: Logiciel de criminalistique

Durant les discussions au sein du Groupe de travail, les rédacteurs ont analysé des méthodes d'enquête sophistiquées. Après d'intenses débats, les rédacteurs ont décidé d'inclure une disposition autorisant les enquêteurs à utiliser des logiciels de criminalistique à distance pour collecter des preuves pertinentes. Ils ont reconnu qu'il s'agit d'un processus très intrusif qui pourrait porter atteinte aux droits fondamentaux du suspect. Ils ont donc décidé d'inclure un certain nombre de restrictions. Premièrement, l'utilisation de tels logiciels exige que les preuves ne puissent pas être collectées à l'aide d'autres processus. Deuxièmement, l'injonction d'un juge ou d'un magistrat est requise. Troisièmement, la demande doit contenir quatre informations majeures (Article 27(1)(a)-(d). En outre, les actes autorisés sont limités par les paragraphes 1 et 2. Les rédacteurs ont décidé de permettre aux pays de mettre en œuvre d'autres restrictions en limitant l'application de l'instrument aux crimes contenus dans une liste figurant à l'Article 27(7) ou en ne mettant pas œuvre cette disposition (Article 27(8)).

TITRE V

Article 28: Pas d'obligation de surveillance

Les fournisseurs de services Internet ont, dans une certaine mesure, la possibilité technique théorique de surveiller les activités liées à leurs services. Sans une réglementation claire, on ne sait pas avec certitude s'il existe une obligation de surveiller ces activités et si les fournisseurs peuvent être poursuivis en cas de non-respect de cette obligation. Outre les possibles conflits avec les réglementations relatives à la protection des données et le secret des télécommunications, une telle obligation causerait

particulièrement des difficultés aux hébergeurs qui hébergent des milliers de sites Internet. Pour éviter ces conflits, l'Article 28 exclut une obligation générale de surveiller les informations transmises ou stockées. La disposition limite uniquement la responsabilité des fournisseurs en matière de responsabilité pénale.

Article 29: Fournisseur d'accès

Selon l'Article 29, la responsabilité des fournisseurs d'accès (Article 29(1)) et des opérateurs de routeurs (Article 29(2)) est totalement exclue pour autant qu'ils se conforment aux trois conditions exposées à l'Article 29. En conséquence, le fournisseur d'accès n'est généralement pas responsable des infractions pénales commises par ses utilisateurs. Cette exclusion totale de responsabilité ne dégage pas les fournisseurs de l'obligation d'empêcher d'autres infractions si un tribunal ou une autorité administrative leur en donne l'ordre.

Article 30: Hébergeur

Les rédacteurs ont pris acte que l'identification de contenus illégaux constitue une difficulté majeure pour l'hébergeur. La recherche manuelle de contenus illégaux serait impossible à effectuer pour les grands fournisseurs en particulier, qui hébergent des milliers de sites Internet. En conséquence, les rédacteurs ont décidé de limiter la responsabilité des hébergeurs. Toutefois, contrairement au fournisseur d'accès, la responsabilité de l'hébergeur n'est généralement pas exclue, mais seulement si certaines conditions sont remplies.

L'Article 30(1)(a) limite la responsabilité si l'hébergeur retire rapidement un contenu après en avoir reçu l'injonction par une autorité publique ou un tribunal. Rapidement signifie en général moins de 24 heures.

L'Article 30(1)(b) énonce que si l'hébergeur n'a vraiment pas connaissance d'activités illégales ou de contenus illégaux stockés sur ses serveurs, il n'est pas responsable. Les rédacteurs ont jugé important de souligner que l'hypothèse selon laquelle des contenus illégaux peuvent être stockés sur ses serveurs n'est pas considérée comme étant équivalente à une connaissance réelle du problème. Si des informations sont portées à l'attention d'un fournisseur, elles doivent être suffisamment concrètes et spécifiques pour lui permettre d'identifier l'emplacement des contenus illégaux. Si le fournisseur obtient des connaissances concrètes sur des activités illégales ou des contenus illégaux, il ne peut éviter la responsabilité que s'il informe une autorité publique du contenu potentiellement illégal. Contrairement à la directive de l'Union européenne sur le commerce électronique, qui établit la responsabilité lorsque l'hébergeur ne retire pas les contenus illégaux après avoir eu connaissance de leur existence, les rédacteurs ont décidé de laisser aux autorités publiques le soin de décider si le contenu est illégal. Les pays peuvent spécifier à quelle autorité compétente de tels contenus doivent être signalés.

L'Article 30 ne s'applique pas qu'aux fournisseurs qui limitent leurs services à la location de capacités techniques de stockage de données. Les services Internet populaires tels que les plateformes d'enchères offrent également des services d'hébergement. Les pays peuvent décider de mettre en place un service d'assistance téléphonique afin de signaler les contenus illégaux.

Dans la mesure où le retrait d'un contenu illégal peut, malgré cette nature illégale, porter atteinte à l'obligation contractuelle du fournisseur à l'égard de son client, les rédacteurs ont décidé d'inclure une précision à l'Article 30(3) pour les cas où une injonction a été reçue conformément au paragraphe 1.

Article 31: Fournisseur de cache

L'Article 31 limite la responsabilité du fournisseur de cache. Le terme «cache» est utilisé dans ce contexte pour décrire le stockage de sites Internet populaires sur des supports de stockage locaux afin de réduire la bande passante et d'augmenter l'efficacité de l'accès aux données. Dans ce contexte, un serveur mandataire peut servir des demandes sans contacter le serveur spécifié en saisissant le contenu sauvegardé sur le support de stockage local à partir d'une requête précédente. Les rédacteurs ont reconnu l'importance économique du cache et décidé d'exclure la responsabilité en ce qui concerne le stockage provisoire automatique si le prestataire se conforme aux conditions définies à l'Article 31.

Article 32: Fournisseur de liens hypertextes

Les liens hypertextes jouent un rôle important dans la connexion et la mise à disposition des contenus Internet. Ils permettent aux fournisseurs de ces liens de guider les utilisateurs vers des informations spécifiques disponibles en ligne. Un lien hypertexte fournit la commande pour que le navigateur ouvre l'adresse Internet déposée. En raison des similitudes avec l'hébergement de contenu, les rédacteurs ont décidé de réglementer la responsabilité des fournisseurs de liens hypertextes de la même manière que celle de l'hébergeur (Article 30).

Article 33: Fournisseur de moteurs de recherche

Les fournisseurs de moteurs de recherche proposent des services de recherche utilisés pour identifier des documents d'intérêt en spécifiant certains critères. Ces moteurs recherchent des documents pertinents qui correspondent aux critères indiqués par l'utilisateur. Ils jouent un rôle important dans le bon développement d'Internet. Les contenus mis à disposition sur un site Internet, mais qui ne figurent pas à l'index du moteur de recherche ne peuvent être consultés que si la personne souhaitant y accéder connaît l'URL complète. En raison des similitudes avec les fournisseurs d'accès, les rédacteurs ont décidé de réglementer la responsabilité des fournisseurs de moteurs de recherche de la même manière que celle de l'hébergeur (Article 30).

ANNEXES

Annexe 1

Participants au premier Atelier de consultation le Groupe de travail du projet HIPCAR traitant du cadre législatif relatif aux TIC – questions relatives à la société de l'information. Gros Îlet, Sainte-Lucie, du 8 au 12 mars 2010

Participants et observateurs officiellement désignés

Pays	Organisation	Nom	Prénom
Antigua-et-Barbuda	Ministère de l'Information, de la Radiodiffusion, des Télécommunications, de la Science et de la Technologie	SAMUEL	Clement
Bahamas	Autorité pour la réglementation et la concurrence des services	DORSETT	Donavon
Barbade	Ministère des Finances, des Investissements, des Télécommunications et de l'Énergie	BOURNE	Reginald
Barbade	Ministère de l'Industrie et du Commerce	COPPIN	Chesterfield
Barbade	Cable & Wireless (Barbade) Ltd.	MEDFORD	Glenda E.
Barbade	Ministère de l'Industrie et du Commerce	NICHOLLS	Anthony
Belize	Commission des services publics	SMITH	Kingsley
Grenade	Commission nationale de réglementation des télécommunications	FERGUSON	Ruggles
Grenade	Commission nationale de réglementation des télécommunications	ROBERTS	Vincent
Guyana	Commission des services publics	PERSAUD	Vidiahar
Guyana	Bureau du Premier ministre	RAMOTAR	Alexei
Guyana	Unité nationale de gestion des fréquences	SINGH	Valmikki
Jamaïque	Université des Antilles	DUNN	Hopeton S.
Jamaïque	LIME	SUTHERLAND CAMPBELL	Melesia
Saint-Kitts-et-Nevis	Ministère de l'Information et de la Technologie	BOWRIN	Pierre G.
Saint-Kitts-et-Nevis	Ministère du Procureur général, de la Justice et des Affaires juridiques	POWELL WILLIAMS	Tashna
Saint-Kitts-et-Nevis	Ministère de l'Autonomisation de la jeunesse, des Sports, des Technologies de l'information, des Télécommunications et de la Poste	WHARTON	Wesley
Sainte-Lucie	Ministère des Communications, des Travaux publics, des Transports et des Services publics	FELICIEN	Barrymore
Sainte-Lucie	Ministère des Communications, des Travaux publics, des Transports et des Services publics	FLOOD	Michael R.
Sainte-Lucie	Ministère des Communications, des Travaux publics, des Transports et des Services publics	JEAN	Allison A.
Saint-Vincent-et-les-Grenadines	Ministère des Télécommunications, des Sciences, de la Technologie et de l'Industrie	ALEXANDER	K. Andre

Annexe 1

Pays	Organisation	Nom	Prénom
Saint-Vincent-et-les-Grenadines	Ministère des Télécommunications, des Sciences, de la Technologie et de l'Industrie	FRASER	Suenel
Suriname	Telecommunicatie Autoriteit Suriname / Autorité des télécommunications du Suriname	LETER	Meredith
Suriname	Ministère de la Justice et de la Police, Département de la Législation	SITALDIN	Randhir
Trinité-et-Tobago	Ministère de l'Administration publique, Division des services juridiques	MAHARAJ	Vashti
Trinité-et-Tobago	Autorité des télécommunications de Trinité-et-Tobago	PHILIP	Corinne
Trinité-et-Tobago	Ministère de l'Administration publique, Secrétariat pour les TIC	SWIFT	Kevon

Participants des organisations régionales/internationales

Organisation	Nom	Prénom
Secrétariat de la Communauté des Caraïbes (CARICOM)	JOSEPH	Simone
Communauté virtuelle des acteurs des TIC de la Caraïbe (CIVIC)	GEORGE	Gerry
Communauté virtuelle des acteurs des TIC de la Caraïbe (CIVIC)	WILLIAMS	Deirdre
Union des télécommunications des Caraïbes (CTU)	WILSON	Selby
Délégation de la Commission européenne pour la Barbade et la Caraïbe orientale (CE)	HJALMEFJORD	Bo
Autorité des télécommunications de la Caraïbe orientale (ECTEL)	CHARLES	Embert
Autorité des télécommunications de la Caraïbe orientale (ECTEL)	GILCHRIST	John
Autorité des télécommunications de la Caraïbe orientale (ECTEL)	HECTOR	Cheryl
Union internationale des télécommunications (UIT)	CROSS	Philip
Union internationale des télécommunications (UIT)	LUDWIG	Kerstin
Bureau des négociations commerciales (anciennement MCNR), Secrétariat de la Communauté des Caraïbes (CARICOM)	BROWNE	Derek E.
Secrétariat de l'Organisation des États de la Caraïbe orientale (OECO)	FRANCIS	Karlene

Consultants pour le projet HIPCAR participant à l'Atelier

Nom	Prénom
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[22]	J Paul
PRESCOD	Kwesi

[22] Président de l'Atelier

Annexe 2

Participants au second Atelier de consultation (stade B) pour le Groupe de travail du projet HIPCAR traitant du cadre législatif relatif aux TIC – questions relatives à la société de l'information Frigate Bay, Saint-Kitts-Et-Nevis, du 19 au 22 juillet 2010

Participants et observateurs officiellement désignés

Pays	Organisation	Nom	Prénom
Antigua-et-Barbuda	Ministère de l'Information, de la Radiodiffusion, des Télécommunications, de la Science et de la Technologie	SAMUEL	Clement
Bahamas	Autorité pour la réglementation et la concurrence des services	DORSETT	Donavon
Barbade	Ministère des Finances, des Investissements, des Télécommunications et de l'Énergie	BOURNE	Reginald
Barbade	Bureau des négociations commerciales	BROWNE	Derek
Barbade	Ministère de l'Industrie et du Commerce	NICHOLLS	Anthony
Belize	Ministère des Finances	LONGSWORTH	Michelle
Belize	Commission des services publics	PEYREFITTE	Michael
Dominique	Ministère de l'Information, des Télécommunications et du Renforcement des circonscriptions	CADETTE	Sylvester
Dominique	Ministère du Tourisme et des Affaires juridiques	RICHARDS-XAVIER	Pearl
Grenade	Commission nationale de réglementation des télécommunications	FERGUSON	Ruggles
Grenade	Commission nationale de réglementation des télécommunications	ROBERTS	Vincent
Guyana	Commission des services publics	PERSAUD	Vidiahar
Guyana	Bureau du Président	RAMOTAR	Alexei
Guyana	Unité nationale de gestion des fréquences	SINGH	Valmikki
Jamaïque	Group Digicel	GORTON	Andrew
Jamaïque	Bureau du Premier Ministre	MURRAY	Wahkeen
Jamaïque	Cabinet du Procureur général	SOLTAU-ROBINSON	Stacey-Ann
Jamaïque	LIME	SUTHERLAND CAMPBELL	Melesia
Saint-Kitts-et-Nevis	Ministère de la Sécurité nationale	ARCHIBALD	Keisha
Saint-Kitts-et-Nevis	Département de la Technologie	BOWRIN	Pierre
Saint-Kitts-et-Nevis	Projet ICT4EDC	BROWNE	Nima
Saint-Kitts-et-Nevis	Gouvernement de Saint-Kitts-et-Nevis	CHIVERTON	Eurta
Saint-Kitts-et-Nevis	Département de la Technologie	HERBERT	Christopher
Saint-Kitts-et-Nevis	Ministère de l'Autonomisation de la jeunesse, des Sports, des TI, des Télécommunications et de la Poste	LAZAAR	Lloyd
Saint-Kitts-et-Nevis	Ministère des Finances, département des Renseignements financiers	MASON	Tracey
Saint-Kitts-et-Nevis	Ministère du Développement durable	MUSSENDEN	Amicia
Saint-Kitts-et-Nevis	Ministère de l'Autonomisation de la jeunesse, des Sports, des TI, des Télécommunications et de la Poste	PHILLIP	Glen
Saint-Kitts-et-Nevis	Cabinet du Procureur général	POWELL WILLIAMS	Tashna
Saint-Kitts-et-Nevis	Ministère des Finances, département des Renseignements financiers	SOMERSALL-BERRY	Jacqueline

Annexe 2

Pays	Organisation	Nom	Prénom
Saint-Kitts-et-Nevis	Ministère de l'Autonomisation de la jeunesse, des Sports, des TI, des Télécommunications et de la Poste	WHARTON	Wesley
Sainte-Lucie	Ministère des Communications, des Travaux publics, des Transports et des Services publics	DANIEL	Ivor
Sainte-Lucie	Ministère des Communications, des Travaux publics, des Transports et des Services publics	FELICIEN	Barrymore
Sainte-Lucie	Cable & Wireless (Sainte Lucie) Ltd.	LEEVY	Tara
Sainte-Lucie	Cabinet du Procureur général	VIDAL-JULES	Gillian
Saint-Vincent-et-les-Grenadines	Ministère des Télécommunications, des Sciences, de la Technologie et de l'Industrie	ALEXANDER	K. Andre
Saint-Vincent-et-les-Grenadines	Ministère des Télécommunications, des Sciences, de la Technologie et de l'Industrie	FRASER	Suenel
Suriname	Telecommunicatiebedrijf Suriname (TELESUR)	JEFFREY	Joan
Suriname	Telecommunicatie Autoriteit Suriname	LETER	Meredith
Suriname	Ministère de la Justice et de la Police	SITLADIN	Vyaiendra
Suriname	Ministère des Transports, des Communications et du Tourisme	SMITH	Lygia
Trinité-et-Tobago	Bureau du Premier Ministre, département de l'Information	MAHARAJ	Rishi
Trinité-et-Tobago	Ministère de l'Administration publique, Division des services juridiques	MAHARAJ	Vashti
Trinité-et-Tobago	Autorité des télécommunications de Trinité-et-Tobago	PHILIP	Corinne
Trinité-et-Tobago	Ministère de l'Administration publique, Secrétariat pour les TIC	SWIFT	Kevon

Participants des organisations régionales/internationales

Organisation	Nom	Prénom
Secrétariat de la Communauté des Caraïbes (CARICOM)	JOSEPH	Simone
Communauté virtuelle des acteurs des TIC de la Caraïbe (CIVIC)	HOPE	Hallam
Communauté virtuelle des acteurs des TIC de la Caraïbe (CIVIC)	ONU	Telojo
Autorité des télécommunications de la Caraïbe orientale (ECTEL)	WRIGHT	Ro Ann
Union internationale des télécommunications (UIT)	CROSS	Philip
Union internationale des télécommunications (UIT)	LUDWIG	Kerstin
Secrétariat de l'Organisation des États de la Caraïbe orientale (OECO)	FRANCIS	Karlene

Consultants pour le projet HIPCAR participant à l'Atelier

Nom	Prénom
GERCKE	Marco
MORGAN[23]	J Paul
PRESCOD	Kwesi

[23] Président de l'Atelier.

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