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

Interception de communications:

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

Interception de communications:

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 d'une nature similaire qui ne sont pas mentionnés. 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 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), 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 M. Gilberto Martíns de Almeida, le Dr. Marco Gercke et Mme. Karen Stephen-Dalton. Le projet de document a ensuite été révisé, discuté et adopté par un large consensus des participants lors des 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 la Barbade du 23 au 26 août 2010 (voir Annexes). Les Notes explicatives du modèle de texte législatif incluses dans ce document ont été préparées par le Dr. 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, les représentants 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 pour 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 l'Union des télécommunications des Caraïbes (CTU) pour 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 bonnes 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. M. Pau Puig Gabarró a réalisé le pré-formatage et l'équipe du Service de composition des publications de l'UIT a été chargée de la publication.

Table des matières

Page

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).

---

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 relie 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 traite de l'interception de communications, l'un des domaines de travail du Groupe de travail sur le cadre politique et législatif des TIC sur 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, y compris de Notes explicatives, que les pays des Caraïbes pourraient souhaiter utiliser lors de l'élaboration ou de la modernisation de leurs politiques et de la législation 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 bénéficiaires du projet HIPCAR de la région concernant les questions relatives à la société de l'information en s'arrêtant à six domaines: les transactions électroniques, les preuves électroniques dans le cadre du commerce électronique, le respect de la vie privée et la protection des données, l'interception de communications, la cybercriminalité et l'accès à l'information publique (liberté d'information). Cette évaluation a tenu compte des bonnes pratiques acceptées sur le plan international et régional.

Cette évaluation régionale, publiée séparément en complément du présent rapport[3], a impliqué une analyse comparative de la législation en vigueur en matière d'interception de communications dans les pays bénéficiaires du projet HIPCAR et une étude des lacunes potentielles à cet égard. Ces deux documents ont servi de base à l'élaboration des modèles de cadre politique et de texte législatif présentés ci-après. À la fois reflets des bonnes 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 modèle de texte législatif sur l'interception de communications a été élaboré en trois phases: (1) la rédaction d'un rapport d'évaluation; (2) l'élaboration du modèle de lignes directrices politiques; et (3) la rédaction du modèle de texte législatif. Le rapport d'évaluation a été préparé en deux phases par les consultants pour le projet HIPCAR. La première phase a été réalisée par Mme Karen Stephen-Dalton, la seconde par M. Gilberto Martíns de Almeida. Ensuite, le projet de modèle de lignes directrices politiques a été préparé par M. Martíns de Almeida, avant ses révision, discussions et finalisation par le Groupe de travail du projet HIPCAR sur les questions relatives à la société de l'information pendant le premier atelier de consultation du Groupe de travail du projet mentionné ci-dessus, qui s'est déroulé à Sainte-Lucie du 8 au 12 mars 2010. En se fondant sur le modèle de lignes directrices politiques, le consultant pour le projet HIPCAR, le Dr. Marco Gercke, a préparé le projet de modèle de texte législatif, qui a également été soumis à révision, discussions et finalisation par le Groupe de travail mentionné ci-dessus au cours du second atelier de consultation du projet qui s'est tenu à la Barbade du 23 au 26 août 2010 (voir Annexes). Les Notes explicatives pour le modèle de texte législatif ont été préparées par le Dr. Gercke en abordant, entre autres, les points soulevés lors du second atelier. Les documents ont été approuvés par un large consensus lors de ces ateliers. Le Comité de pilotage du projet HIPCAR et l'équipe de gestion du projet ont supervisé le processus d'élaboration de ces documents.

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.

[3] Voir «ICT Policy and Legislative Framework on Information Society Issues – Interception of Communications: Assessment Report on the Current Situation in the Caribbean » disponible à l'adresse www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

1.6. Importance de l'efficacité des politiques et des lois sur l'interception de communications

Dans le contexte de la société de l'information, où les communications[4] jouent un rôle très important, l'interception de communications, dans certaines circonstances, constitue un mécanisme essentiel de la protection des États et des personnes.

Cette pratique étant susceptible d'entrer en conflit avec le respect de la vie privée et d'autres droits importants, la définition des critères qui détermineront ou limiteront son utilisation nécessite une élaboration de politiques et une rédaction législative appropriées.

Conformément au *Toolkit for Cybercrime Legislation* de l'UIT[5], l'«interception» désigne «l'acquisition, la visualisation, la capture ou la copie du contenu ou d'une partie du contenu d'une communication, notamment les données relatives au contenu, les données informatiques, les données relatives au trafic, et/ou les émissions électroniques de ces données, par des moyens avec fils, sans fils, électroniques, optiques, magnétiques, oraux, ou d'autres moyens, *pendant la transmission* grâce à l'utilisation d'un dispositif électronique, mécanique, optique, à ondes, électromécanique, ou un autre type de dispositif.»[6]

Une telle définition explique la vaste portée de l'«interception» et de la «communication» qui lui est subordonnée et qui inclut le «contenu» (l'information communiquée) et le «trafic» (les données en rapport avec la communication)[7]. Elle décrit également différents moyens de communication susceptibles d'être interceptés. Bien entendu, les communications par Internet, en particulier la cybercriminalité, constituent une part importante des activités d'interception, tant du point de vue quantitatif que de la complexité.

Les Directives européennes 02/58/CE et 06/24/CE fournissent également des contributions pertinentes pour comprendre à quel point une interception de communications peut être complète. Les concepts de «données»[8] et de «données de localisation»[9] sont particulièrement intéressants à cet égard.

L'interception de communications peut être légalement admissible et applicable. De manière générale, l'interception légale comprend l'obtention de données de communication sur mandat légitime à des fins d'analyse ou de preuves. Le mandat légitime dans ce domaine est souvent lié à la cybersécurité et à la

---

4 Cette expression est définie par la Directive européenne 02/58/CE, dans son Article 2, «d », par «toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire de réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit. »

5 Disponible à l'adresse www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf , et élaboré conjointement à l'American Bar Association's Privacy & Computer Crime Committee, Section of Science & Technology Law.

6 Partie 1 – Définitions, article «k ».

7 La Convention de Budapest, administrée par le Conseil de l'Europe, a défini les «données relatives au trafic », dans son Article 1, «d », comme «toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent »; à son tour, l'expression «données informatiques » est définie dans ce document, à la lettre «b » de l'Article 1, comme «toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ». L'expression données relatives au trafic est également définie à l'Article 2, «b » de la Directive européenne 02/58/CE comme «toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation. »

8 Définies à l'Article 2, «a », de la Directive européenne 06/24/CE comme «les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur. »

9 Définies à l'Article 2, «c », de la Directive européenne 06/24/CE comme «toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ».

protection des infrastructures de communications. L'interception légale joue un rôle essentiel pour aider les organismes chargés de l'application de la loi, les organismes réglementaires ou administratifs et les services de renseignement dans la lutte contre le crime, étant donné la sophistication croissante des criminels d'aujourd'hui. L'interception légale représente un *moyen indispensable de collecter des informations contre des criminels impitoyables.*[10]

Les changements intervenus sur les marchés de la poste et des télécommunications et la large expansion de la nature et de la gamme de services disponibles dans la plupart des États sont remarquables. Les téléphones mobiles se sont répandus jusqu'à devenir les objets de propriété de masse qu'ils sont aujourd'hui. Les communications par Internet ont connu une très forte croissance ces dernières années et cette croissance se poursuit toujours. Quant au secteur postal, il se développe rapidement avec l'augmentation du nombre de sociétés offrant des services de livraison de paquets et de documents. Les criminels (notamment les terroristes) ont été prompts à exploiter ces changements extraordinaires intervenus dans le secteur des communications pour leurs activités criminelles alors que la législation de nombreux États n'a pas réussi à s'adapter à ces changements. Ceci risque de dégrader la capacité des organismes chargés de l'application de la loi, des organismes chargés de la sécurité et des agences de renseignement.

Les graves menaces criminelles et à la sécurité auxquelles la communauté mondiale est confrontée ont poussé de nombreux pays, notamment l'Australie, les États-Unis, le Royaume-Uni, Sainte-Lucie et la Jamaïque, à adopter des lois qui exigent des prestataires de services de communications électroniques qu'ils soient capables de réaliser des interceptions légales et de réglementer les activités d'interception de communications.

Pour que l'interception de communications soit légale, elle doit être conduite conformément à la loi nationale, qui peut réglementer l'interception de communications privée ou officielle. La légalité de l'interception de communications privée est restreinte à un nombre limité de situations qui peuvent inclure la surveillance électronique des employés sur le lieu de travail. La loi nationale peut régir l'interception de communications privée dans le contexte des relations du travail, du droit à la vie privée, ou dans d'autres cas.

Légiférer sur l'interception de communications est une tâche qui présente plusieurs défis complexes. Certains d'entre eux étant la conséquence d'une sophistication technologique accrue, tandis que d'autres sont davantage liés à la difficulté que représente l'harmonisation de systèmes juridiques et de lois nationales différents au sein d'une seule région.

L'informatique en nuage, les techniques de repostage, la cryptographie et la stéganographie sont des exemples de moyens technologiques susceptibles d'être utilisés par les criminels qui rendent difficiles ou impossibles l'interception de communications ou leur analyse. Par conséquent, l'utilisation de ces technologies à des fins illicites est source de préoccupation.

D'autre part, la nécessité d'un équilibre entre les demandes d'interception et le droit à la vie privée constitue une autre difficulté pour la mise en œuvre de l'interception de communications, celle-ci pouvant requérir une évaluation au cas par cas malgré l'augmentation rapide du volume d'ordres, provenant du monde entier.

Les difficultés de mise en œuvre de l'interception sont également associées à un contrôle de gestion complexe. Les quantités colossales de données cumulées et les multiples paramètres permettant de décider de les conserver ou de les supprimer montrent que l'interception de communications n'est pas seulement une question juridique complexe, mais également une tâche administrative compliquée.

[10] Notes sur le projet de loi sur l'interception de communications de l'OECO, page 6 consultable à l'adresse www.//unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024635.pdf

La diversité des systèmes juridiques et les différents stades de développement et de mise en œuvre des politiques relatives aux TIC représentent des complications supplémentaires sur la voie de l'harmonisation des lois nationales. En outre, les pays disposent également de cadres juridiques et réglementaires très divers pour leur environnement intérieur.

Bien que les pays des Caraïbes puissent être parties à des conventions régionales et internationales, et dans la plupart des cas être membres de la Communauté des Caraïbes, la région ne dispose pas d'une puissance souveraine dotée de l'autorité de légiférer en leur nom en tant que groupe et de veiller au respect des lois, comme c'est le cas de la Communauté européenne.

Pour prendre l'exemple des États membres de l'Organisation des États de la Caraïbe orientale (OECO), le modèle de loi relative à l'interception de communications préparé en 2003 par le service de rédaction des lois de l'OECO a été approuvé la même année par la commission juridique composée de procureurs généraux (directement responsables de la mise en œuvre de la politique relative à l'interception), en vue de sa promulgation dans tous les États membres de l'OECO. Cependant, à ce jour, Sainte-Lucie est le seul membre de l'OECO à avoir promulgué une loi sur l'interception de communications (qui devrait être suivie par une loi similaire en Jamaïque).

Pour plus d'informations sur les défis auxquels est confrontée l'élaboration de politiques et de législations relatives à l'interception de communications, il est recommandé de lire les parties 3.2 et 3.3 du document de l'IUT *«Comprendre la cybercriminalité: guide pour les pays en développement»*[11].

[11] Disponible à l'adresse www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

Partie I:
Modèle de lignes directrices politiques – Interception de communications

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

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

- Une définition adéquate existe pour «interception», «communications», «données», «contenu», «trafic», «données relatives au contenu», «données relatives au trafic», «données de localisation».
- La formulation de la définition de ces termes est suffisamment large et associée à une liste d'exemples.
- Il existe une définition claire du type d'information (texte, visuelle, sonore) et de l'étendue des supports soumis à l'interception de communications, de façon à ce qu'elle englobe les documents électroniques ou non électroniques, les bandes magnétiques, les films, les enregistrements sonores, les images, etc., que ceux-ci soient produits par une partie publique ou privée, à tout moment.
- Dans les limites autorisées par les questions de sécurité nationale, une campagne publique est conduite afin de sensibiliser le public au type de communication soumise à interception et d'expliquer les politiques publiques qui la justifient et l'abordent.

2. LES PAYS DE LA CARICOM/DU CARIFORUM VISERONT À ÉTABLIR LE CADRE NÉCESSAIRE POUR DÉFINIR L'ORIGINE PUBLIQUE OU PRIVÉE ET LE RÔLE DES PARTIES CHARGÉES DE LA GESTION DE L'INTERCEPTION DE COMMUNICATIONS[12]

- Une disposition de la loi précise explicitement le rôle des «pouvoirs publics» (comme les organismes chargés de l'application de la loi) et des «organismes privés» (comme les FSI et les sociétés de télécommunication) dans le contexte de l'interception de communications.
- Une disposition établit une obligation, pour les parties privées, de coopérer avec les pouvoirs publics pour l'interception de communications, comme déterminé par la législation applicable (droits pénaux procéduraux, lois sur la sécurité nationale), dans la mesure juridiquement autorisée.
- Un règlement prévoit la reconnaissance et l'intégration des normes techniques généralement acceptées qui traitent de la surveillance électronique et/ou téléphonique, et qui pourraient servir pour l'interception de communications.
- Il existe une politique publique harmonisant l'interception de communications et le droit à la vie privée, la liberté d'information, la propriété intellectuelle et d'autres politiques publiques qui traitent de la promotion de la production, de la conservation et de la communication de l'information.

[12] Il existe une politique publique encourageant la coopération institutionnelle (par exemple, avec l'industrie et le commerce) pour le développement ou l'utilisation, selon le cas (et, dans la mesure nécessaire, le partage) de bases de données et autres mécanismes de conservation ou de publication de données pertinentes pour la réalisation des objectifs de l'interception de communications.
Les nouveaux défis auxquels l'interception de communications doit faire face (tels que la stéganographie, l'informatique en nuage et d'autres) font l'objet d'une surveillance constante.

- Des critères formels établissent la façon d'adresser les demandes et les ordres d'interception de communications provenant de l'étranger.
- Il existe des critères formels et une formation pour réaliser une interception de communications qui soit acceptée comme preuve électronique.

3. LES PAYS DE LA CARICOM/DU CARIFORUM DÉFINIRONT LES MANDATS STATUTAIRES ET LES NORMES AUXQUELS L'INTERCEPTION DE COMMUNICATIONS EST LIÉE

- La loi/le mandat statutaire est de nature habilitante et évite les dispositions trop contraignantes.
- La loi/le mandat statutaire affirme qu'aucune communication n'est interceptée sauf si l'intérêt public l'exige, et que l'interception est réalisée conformément aux procédures, normes et pratiques juridiques.
- La loi/le mandat statutaire précise les motifs constitutionnels de l'interception de communications, afin d'établir son importance par rapport à d'autres droits ou principes constitutionnels.
- La loi/le mandat statutaire prévoit les critères qui doivent guider la sélection des recherches électroniques des communications à intercepter.
- La loi/le mandat statutaire détermine les scénarios acceptables pour la mise en œuvre de l'interception de communications, en tenant compte de la durée et de l'étendue de la recherche, des mécanismes de filtrage, du délai maximum de conservation d'une communication interceptée, de la sécurité pour la conservation des communications interceptées, de la suppression appropriée et d'autres procédures.
- La loi/le mandat statutaire peut établir un traitement différent pour les données relatives au contenu, les données relatives au trafic et les données de localisation.
- La loi/le mandat statutaire stipule que la gestion de l'interception de communications est guidée par les objectifs de conformité aux principes de droit, d'efficience, d'efficacité et de suivi des enregistrements.
- La loi/le mandat statutaire définit les communications (telles que celles relatives au terrorisme, au contre-espionnage) devant faire l'objet de procédures d'interception et de structures administratives spéciales.

4. LES PAYS DE LA CARICOM/DU CARIFORUM DÉFINIRONT LES EXEMPTIONS À LA CONFORMITÉ DE L'INTERCEPTION DE COMMUNICATIONS

- La loi/le mandat statutaire prévoit des exemptions claires et précises, afin d'éviter les trop nombreuses exemptions qui pourraient aller à l'encontre des objectifs de l'interception de communications.
- La loi/le mandat statutaire définit les communications (bancaires, médicales et autres) non soumises à l'interception, sauf si un ordre juridique accorde une autorisation d'interception.
- La loi/le mandat statutaire sensibilise aux critères d'harmonisation de l'interception de communications et aux divers types de secrets (bancaire, fiscal, postal, professionnel, judiciaire et autres).
- La loi/le mandat statutaire affirme que lorsque l'intérêt public du maintien du secret d'une communication est supérieur à l'intérêt public de son interception, l'interception est considérée comme non autorisée.

- La loi/le mandat statutaire établit que l'interception de communications est cohérente avec la politique publique sur la liberté de crypter les communications (et d'utiliser d'autres moyens de dissimulation des communications, tels que le repostage).

5. LES PAYS DE LA CARICOM/DU CARIFORUM ÉTABLIRONT DES PROCÉDURES DE CONTRÔLE, D'APPLICATION, D'EXAMEN ET D'APPEL EN RAPPORT AVEC L'INTERCEPTION DE COMMUNICATIONS

- La loi/le mandat statutaire établit des procédures de contrôle, d'application, d'examen et d'appel en rapport avec l'interception de communications.
- La loi/le mandat statutaire établit que le demandeur et l'autorité publique ont le droit de faire appel devant les tribunaux des décisions de l'organe administratif.
- La loi/le mandat statutaire établit des échéanciers afin que les réponses aux demandes et la fourniture d'informations ne soient pas retardées au-delà d'un délai raisonnable.
- La loi/le mandat statutaire établit des sanctions pour les manquements aux devoirs et obligations liés à l'interception de communications.

6. LES PAYS DE LA CARICOM/DU CARIFORUM ÉTABLIRONT LE CADRE DE L'INTERCEPTION DE COMMUNICATIONS EN PARALLÈLE AVEC LES POLITIQUES PUBLIQUES PORTANT SUR DES SUJETS CONNEXES

- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique sur la sécurité nationale.
- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique sur la cybercriminalité.
- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique sur la liberté d'information.
- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique sur le respect de la vie privée et la protection des données.
- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique pertinente sur la censure.
- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique sur la sécurité de l'information.
- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique sur la propriété intellectuelle.
- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique sur la liberté de radiodiffusion.
- La loi/le mandat statutaire réglemente l'interception de communications d'une manière cohérente avec la politique publique sur l'*habeas data,* le cas échéant.

Partie II:
Modèle de texte législatif – Interception de communications

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

Organisation des articles

Partie II

Partie II

TITRE I – PRÉAMBULE

Titre abrégé 1. La présente loi peut être désignée comme la Loi sur l'Interception de communications et entrera en vigueur [le xxx/ après publication au Journal *officiel*].

Objectif 2. [La présente loi a pour objectif d'élaborer un cadre juridique pour l'interception légale des communications et de protéger et préserver le droit à l'anonymat, au cryptage et à la confidentialité des communications].

Définitions 3. (1) «Organisme» désigne un [organisme chargé de l'interception] ou [un autre organisme chargé de l'application de la loi].

(2) «Fonctionnaire habilité» désigne

a. le [Chef de police];

b. le [Directeur de la cellule de renseignement financier];

c. une personne qui, pour le moment, exerce légalement les fonctions d'une personne mentionnée à l'alinéa (a) ou (b);

d. une personne autorisée par écrit à agir au nom d'une personne mentionnée aux alinéas (a), (b) ou (c).

(3) «Communication» désigne

a. toute chose comportant de la parole, de la musique, des sons, des images visuelles ou des données de quelque dénomination que ce soit, notamment des données relatives au contenu, des données informatiques, des données relatives au trafic, et/ou les émissions électroniques de ces données; ou

b. les signaux servant à la transmission de quelque chose entre des personnes, entre une personne et une chose ou entre des choses, ou au déclenchement ou à la commande d'un appareil,

acheminés par l'intermédiaire d'un réseau de communication électronique ou d'une partie de ce réseau au moyen d'un dispositif électronique, mécanique, optique, à ondes, électromécanique, ou d'un autre type de dispositif.

(4) «Prestataire de communication» désigne une personne qui exploite un réseau de communication ou qui fournit un service de communication à plus de [nombre de] clients.

(5) «Réseau de communication» désigne toute installation ou infrastructure utilisée par une personne pour fournir des services de communication, notamment un réseau par lequel une personne peut envoyer ou recevoir des services de communication vers ou depuis –

a. tout lieu dans l'État;

b. tout lieu hors de l'État.

(6) «Service de communication» désigne tout service fourni au moyen d'un réseau de communication, que le réseau soit exploité ou non par la personne qui fournit le service.

(7) «Personne désignée» désigne le [Ministre] ou toute personne prévue pour l'application de la présente loi par le [Ministre] par ordonnance publiée au [nom de la publication] sous réserve de ratification.

(8) «Ordonnance de divulgation» désigne une ordonnance rendue aux termes de l'article 30, requérant l'accès aux données de communication stockées.

(9) «Intercepter» désigne l'acquisition, la visualisation, la capture, la surveillance ou la copie du contenu ou d'une partie du contenu d'une communication pendant sa transmission grâce à l'utilisation d'un dispositif ou d'une méthode d'interception.

(10) «Communication interceptée» désigne toute communication interceptée au cours de sa transmission.

(11) «Dispositif d'interception» désigne tout instrument, équipement ou appareil électronique, mécanique, optique, à ondes ou électromécanique utilisé ou susceptible d'être utilisé, en tant que tel ou combiné avec un autre instrument, équipement, programme ou appareil en vue d'intercepter une communication, mais ne désigne pas un instrument, équipement ou appareil, ou un composant dudit instrument, équipement ou appareil:

a. fourni à un client par un prestataire de communication dans le cadre normal de ses activités et utilisé par un client dans le cadre normal de ses activités;

b. fourni par un client pour se raccorder aux installations d'un tel service de communication et utilisé par le client dans le cadre normal de ses activités; ou

c. utilisé par un prestataire de communication dans le cadre normal de ses activités.

(12) «Mandat d'interception» désigne une autorisation délivrée en vertu de l'article 8.

(13) «Équipement recensé» désigne tout équipement déclaré être un équipement recensé en vertu de l'article 25 et incluant tout composant de cet équipement.

(14) «Ministre» désigne le [Ministre] [nom du ministère].

[(15) «Personne» inclut une personne morale ou une entité non constituée en personne morale.]

(16) «Données de communication stockées» désigne les communications qui n'ont pas commencé à être transmises sur un système de communication ou qui ont fini de l'être.

Application 4. (1) Rien dans la présente loi ne doit être interprété comme nécessitant ou interdisant l'anonymat ou le cryptage des communications.

(2) La présente loi ne s'applique pas si l'interception de communications est prévue dans le cadre d'une autre loi de [État].

Partie II

TITRE II – INTERCEPTION DE COMMUNICATIONS

Interdiction d'interception de communications

5. (1) Une personne qui intercepte intentionnellement une communication pendant sa transmission commet une infraction passible, sur déclaration de sa culpabilité, d'une amende maximale de [montant] et d'une peine d'emprisonnement maximal de [période].

(2) Une personne ne commet pas une infraction aux termes du paragraphe (1), si:

a. la communication est interceptée conformément à un mandat d'interception délivré par un [juge] en vertu de l'article 8;

b. sous réserve du paragraphe (3), cette personne a de bonnes raisons de croire que la personne à laquelle ou par laquelle la communication est transmise consent à l'interception;

c. la communication consiste en des données de communication stockées acquises conformément aux dispositions d'une autre loi;

d. la communication est interceptée comme un incident ordinaire à la fourniture de services de communication ou à l'application d'une loi en vigueur en rapport avec l'utilisation de ces services;

e. l'interception concerne une communication passée par l'intermédiaire d'un réseau de communication configuré de façon à rendre la communication immédiatement accessible au grand public; ou

f. l'interception concerne une communication transmise et reçue sur un réseau interne utilisé pour répondre aux besoins de la société ou du foyer, effectuée par une personne qui détient:

   i. le droit de contrôler l'exploitation ou l'utilisation du réseau; ou

   ii. le consentement exprès ou implicite d'une personne visée au point (i).

(3) Une personne ne commet pas une infraction aux termes du paragraphe (1) lorsque:

a. la communication est envoyée par ou destinée à une personne qui a consenti à l'interception; et

b. un fonctionnaire habilité estime qu'une interception de communication est nécessaire en cas d'urgence, dans le but de prévenir un décès, une blessure ou un dommage à la santé physique ou mentale d'une personne, ou d'atténuer une blessure ou un dommage à la santé physique ou mentale d'une personne, ou dans l'intérêt de la sécurité nationale.

Remarque: un pays peut limiter la criminalisation en établissant des exigences complémentaires.

Demande du mandat d'interception

6. (1) Un [fonctionnaire habilité] [procureur général au nom d'un fonctionnaire habilité] peut demander ex parte à un [juge] un mandat lui permettant d'intercepter des communications dans tous les cas où il y a de bonnes raisons de penser que les conditions mentionnées au paragraphe (1) de l'Article 8 sont satisfaites.

(2) Sous réserve de l'Article 14, une demande de mandat d'interception doit se présenter sous forme écrite et être accompagnée d'un affidavit contenant les éléments suivants:

a. le nom du fonctionnaire habilité [au nom duquel la demande est faite];

b. les faits et autres motifs sur lesquels se fonde la demande;

c. la durée de validité du mandat demandée et justifiée;

d. les informations suffisantes pour permettre au [juge] de délivrer un mandat d'interception selon les termes prévus au paragraphe (1) de l'Article 8;

e. le motif mentionné au paragraphe (1) de l'Article 8 pour lequel la demande est faite;

f. les détails complets des faits et circonstances allégués par le fonctionnaire habilité au nom duquel la demande est faite, notamment;

   i. si possible, une description de la nature et de l'emplacement des installations à partir desquelles, ou les locaux dans lesquels la communication doit être interceptée; et

   ii. le fondement qui permet de croire que les preuves liées au motif sur lequel la demande est faite seront obtenues grâce à l'interception;

g. s'il y a lieu, si d'autres méthodes d'enquête ont été appliquées sans pouvoir produire les preuves requises, ou la raison pour laquelle les autres méthodes d'enquête semblent raisonnablement être vouées à l'échec si elles étaient appliquées ou sont probablement trop dangereuses à appliquer pour obtenir les preuves nécessaires;

h. si une demande précédente a été faite pour la délivrance d'un mandat d'interception concernant la même personne, la même installation ou les mêmes locaux que ceux indiqués dans la demande et, si cette demande précédente existe, indiquer la situation actuelle de cette demande;

i. toute autre directive délivrée par le [juge].

(3) Lorsqu'un mandat d'interception est demandé pour des raisons de sécurité nationale, la demande est accompagnée d'une autorisation écrite signée par le [Ministre].

(4) Sous réserve du paragraphe (5), les dossiers liés à chaque demande de mandat d'interception ou de renouvellement ou de modification de ce mandat sont;

a. placés dans un paquet et scellés par le [juge] auquel la demande est faite immédiatement après la décision concernant la demande; et

b. conservés par la cour dans un lieu interdit au public ou pour lequel le [juge] donne son autorisation.

(5) Les dossiers mentionnés au paragraphe (5) pourront être ouverts si un [juge] l'ordonne et uniquement

a. dans le but de traiter une demande pour une autorisation complémentaire; ou

b. pour le renouvellement d'une autorisation, sauf décision contraire du tribunal.

(6) Une personne qui, dans une demande ou un affidavit en vertu de la présente loi, fait une déclaration qu'elle sait être fausse quant à certains détails significatifs commet une infraction et est passible, sur déclaration de sa culpabilité par procédure sommaire, d'une amende maximale de [montant] et d'un emprisonnement maximal de [période].

Divulgation de la demande

7. (1) Toute personne qui divulgue l'existence d'une demande de mandat d'interception à une autre personne que le fonctionnaire habilité commet une infraction passible, sur déclaration de sa culpabilité, d'une amende maximale de [montant] et d'un emprisonnement maximal de [période].

(2) Dans toute procédure, la personne poursuivie pourra montrer pour sa défense

a. que la divulgation a été faite à un conseiller juridique afin de demander un avis juridique;

b. que la personne à laquelle, ou selon le cas, par laquelle une divulgation mentionnée au paragraphe (1) a été faite, était le client ou un représentant du client.

(3) Dans une procédure, une personne poursuivie pour une infraction aux termes du paragraphe (1) pourra montrer pour sa défense que la divulgation a été faite par un conseiller juridique;

a. en vue d'une poursuite judiciaire, ou relativement à une poursuite judiciaire; et

b. aux fins de la procédure.

(4) Le paragraphe (2) ou (3) ne s'applique pas dans le cas d'une divulgation faite en procédure pénale.

(5) Dans une poursuite à l'encontre d'une personne pour infraction aux termes du présent paragraphe (1), la personne poursuivie pourra montrer pour sa défense que la divulgation se limitait à une divulgation autorisée par le fonctionnaire habilité.

Délivrance du mandat d'interception

8. (1) Un [juge] autorise l'interception et délivre un mandat d'interception s'il est convaincu que:

a. le mandat d'interception est nécessaire

i. dans l'intérêt de la sécurité nationale; ou

ii. pour la prévention ou la détection d'une infraction précisée à l'Annexe, lorsqu'il existe de bonnes raisons de croire que cette infraction a été, est, ou pourrait être commise; ou

iii. pour donner effet, dans des circonstances qui semblent, pour le [juge], être équivalentes à celles dans lesquelles il délivrerait un mandat d'interception en vertu du point (ii), aux dispositions d'un accord d'entraide judiciaire ou d'une loi;

b. les informations obtenues grâce à l'interception sont susceptibles d'aider l'enquête portant sur un sujet mentionné à l'alinéa (a), et que

c. d'autres procédures:

i. n'ont pas réussi ou n'ont que peu de chances de réussir à obtenir les informations que l'on souhaite acquérir au moyen du mandat d'interception;

ii. sont trop dangereuses pour être adoptées dans ces circonstances, ou

iii. sont irréalisables, eu égard à l'urgence du cas;

et que

d. il serait dans l'intérêt de l'administration de la justice de délivrer un mandat d'interception.

(2) Au moment de l'examen de la demande de mandat d'interception, un [juge] peut demander à un fonctionnaire habilité de fournir d'autres informations liées à la demande, s'il l'estime nécessaire.

Portée et forme du mandat d'interception

9. (1) Un mandat d'interception est délivré par écrit et permet au fonctionnaire habilité:

a. d'intercepter une communication pendant sa transmission;

b. d'ordonner à un prestataire de communication d'intercepter la communication pendant sa transmission;

c. d'exécuter l'interception au moyen de réseaux de communication ou de prestataires de services de communication, comme décrit dans le mandat d'interception;

d. de divulguer les communications interceptées, obtenues ou requises par le mandat d'interception, aux personnes et de la manière indiquées dans le mandat d'interception.

(2) Un mandat d'interception autorise l'interception de:

a. communications transmises par des réseaux ou des prestataires de communication en provenance ou à destination:

i. d'une personne particulière désignée dans le mandat d'interception;

ii. d'une adresse particulière indiquée dans le mandat d'interception;

b. communications transmises par des réseaux ou des prestataires de communication à partir d'une connexion particulière précisée dans le mandat d'interception;

c. toute autre communication, le cas échéant, nécessaire pour intercepter la communication relevant de l'alinéa (a).

(3) Un mandat d'interception peut autoriser l'entrée dans les locaux précisés dans le mandat, comme mentionné à l'Article 18, en vue de l'installation, de l'entretien, de l'utilisation, ou de la récupération de tout équipement utilisé pour intercepter les communications indiquées dans le mandat.

Partie II

(4) Un mandat d'interception:

a. précise l'identité du fonctionnaire habilité au nom duquel la demande est faite;

b. identifie la personne qui exécutera le mandat d'interception;

c. identifie le prestataire de communication auquel le mandat d'interception doit être adressé et précise si le prestataire de communication est autorisé à intercepter les communications, le cas échéant; et

d. lorsque le mandat d'interception autorise l'entrée dans des locaux en vertu du paragraphe (3),

   i. il doit préciser si l'entrée est autorisée à tout moment du jour ou de la nuit ou uniquement pendant les heures indiquées;

   ii. il peut préciser les éventuelles mesures supplémentaires à prendre pour sécuriser et effectuer l'entrée dans les locaux.

(5) Un mandat d'interception peut contenir des dispositions accessoires nécessaires pour assurer sa mise en œuvre conformément à la présente Loi.

(6) Un mandat d'interception peut préciser des conditions ou des restrictions en rapport avec l'interception de communications autorisée dans ledit mandat.

Remarque: les pays peuvent, en fonction de leurs traditions juridiques, exiger des garanties procédurales supplémentaires.

(7) Pour les besoins du présent article, «adresse» désigne les locaux, l'adresse électronique, le numéro de téléphone, ou les éventuels numéros ou désignation utilisés pour identifier les réseaux, les prestataires ou les appareils de communication.

Durée et renouvellement du mandat d'interception

10. (1) Un mandat d'interception est valable pour la période, qui ne doit pas être supérieure à [*90*] jours, que le [juge] indique sur le mandat, mais peut être renouvelé à tout moment avant la fin de cette période, sur une demande faite en vertu des paragraphes (3) et (4).

(2) Un [juge] peut, sur une demande de renouvellement d'un mandat d'interception faite par un [fonctionnaire habilité] [*procureur général* au nom d'un fonctionnaire habilité], renouveler un mandat d'interception à tout moment avant l'expiration du mandat (ou de son éventuel renouvellement en cours).

(3) Une demande de renouvellement d'un mandat d'interception en vertu du paragraphe (2) doit être effectuée par écrit et être accompagnée d'un affidavit attestant des circonstances invoquées comme justifiant le renouvellement du mandat d'interception.

(4) Chaque demande de renouvellement d'un mandat d'interception est faite selon la manière prévue à l'Article 6 et donne:

a. la raison et la période pour lesquelles le renouvellement est requis; et

b. les détails complets, accompagnés des heures et des dates, de toutes les interceptions faites ou tentées en vertu du mandat, et une indication de la nature des informations obtenues par chacune de ces interceptions.

(5) Chaque demande de renouvellement d'un mandat d'interception est étayée par toute autre information que le [juge] peut exiger.

(6) Le renouvellement d'un mandat d'interception peut être accordé en vertu du présent article si le [juge] est convaincu que les circonstances mentionnées au paragraphe (1) de l'Article 8 ont toujours cours.

(7) Chaque renouvellement d'un mandat d'interception est valable pour la période, qui ne doit pas dépasser [*90*] jours, que le [juge] précise sur le renouvellement.

(8) Si, à tout moment avant la fin des périodes mentionnées aux paragraphes (1) et (7) de l'Article 10, le fonctionnaire habilité auquel le mandat est délivré ou la personne qui agit en son nom, s'aperçoit qu'un mandat d'interception n'est plus nécessaire, il doit faire une demande au [juge] pour la révocation du mandat d'interception.

Modification du mandat d'interception

11. (1) Un [juge] peut modifier une disposition d'un mandat d'interception à tout moment, après avoir entendu les observations du [*fonctionnaire habilité/du procureur général* agissant au nom d'un fonctionnaire habilité] et s'il est convaincu qu'un changement de circonstances s'est produit, et peut rendre les modifications demandées nécessaires ou indiquées.

(2) Une demande de modification du mandat d'interception est effectuée conformément à l'Article 6 et contient les informations mentionnées au paragraphe (2) de l'Article 6.

Révocation du mandat d'interception

12. (1) Un [juge] ayant délivré un mandat d'interception [ou, s'il n'est pas disponible, tout autre [juge] autorisé à délivrer un tel mandat] peut révoquer le mandat d'interception si

a. le fonctionnaire habilité ne soumet pas un rapport conformément à l'Article 15, le cas échéant;

b. le [juge] dès réception d'un rapport soumis en vertu de l'article 15 est convaincu que les objectifs du mandat d'interception ont été atteints;

c. les motifs sur lesquels le mandat d'interception a été délivré ont cessé d'exister; ou

d. les conditions de la demande mentionnées au paragraphe (1) de l'Article 8 ont changé au point que la demande ne serait plus possible.

(2) Lorsqu'un [juge] révoque un mandat d'interception en vertu du paragraphe (1), il informe immédiatement par écrit le fonctionnaire habilité concerné par la révocation.

(3) Si le mandat d'interception est révoqué, un fonctionnaire habilité enlève ou fait enlever des locaux auxquels le mandat d'interception se rapporte conformément au paragraphe (3) de l'Article 9, dès que possible après avoir été informé de la révocation, tout dispositif d'interception ayant été installé conformément au même paragraphe.

Conséquences de la révocation

13. Lorsqu'un mandat d'interception délivré conformément à la présente Loi est révoqué conformément à l'Article 12, le contenu de toutes les communications interceptées en vertu de ce mandat est irrecevable en tant que preuves dans une procédure pénale ou civile éventuelle, sauf si le tribunal est d'avis que l'admission de ces preuves ne rendrait pas le procès inéquitable ou ne porterait pas autrement préjudice à l'administration de la justice.

Demande urgente

14. (1) Lorsqu'un juge est convaincu que l'urgence des circonstances l'exige

a. il peut déroger aux exigences de demande écrite et d'affidavit et entendre une demande verbale de mandat d'interception; et

b. s'il est convaincu qu'un mandat d'interception est nécessaire, il délivre un mandat d'interception conformément à la présente Loi.

(2) Une demande conformément au paragraphe (1) (a) doit

a. contenir les informations mentionnées au paragraphe (2) de l'Article 6;

b. indiquer les détails de l'urgence du cas ou les autres circonstances exceptionnelles qui, de l'avis du fonctionnaire habilité, justifie de faire une demande verbale.

(3) Un [juge] peut, sur demande verbale qui lui est faite, délivrer un mandat d'interception, s'il est convaincu que

a. il existe de bonnes raisons de croire que le mandat d'interception doit être délivré; et

b. il n'est pas raisonnablement possible, compte tenu de l'urgence du cas ou de l'existence de circonstances exceptionnelles, que le [fonctionnaire habilité] [procureur général faisant la demande au nom du fonctionnaire habilité] fasse une demande écrite pour la délivrance du mandat d'interception demandé.

(4) Lorsque le [juge] accorde la demande de mandat d'interception d'urgence, le [juge] note immédiatement par écrit les détails de la demande. Le [juge] note également les termes du mandat.

(5) Un mandat d'interception délivré sur demande verbale doit avoir la même portée que celle mentionnée à l'Article 9.

(6) Chaque mandat d'interception d'urgence reste valable [*48*] heures à partir de l'heure à laquelle il a été donné, puis expire.

(7) Lorsqu'un mandat d'interception est délivré conformément au présent article, le [fonctionnaire habilité] [*procureur général* au nom du fonctionnaire habilité] doit, dans les [*48*] heures suivant l'heure de délivrance, soumettre au [juge] une demande écrite et un affidavit conformément aux dispositions de l'Article 6.

(8) À l'expiration de [*48*] heures à partir de l'heure de délivrance du mandat d'interception conformément au présent article, le [juge] réexamine sa décision de délivrer le mandat d'interception.

(9) Lors du réexamen de sa décision en vertu de paragraphe (8), le [juge] détermine si le mandat d'interception continue à être nécessaire en vertu de l'article 8.

(10) Si le [juge] est convaincu que le mandat d'interception continue à être nécessaire, il rend une ordonnance qui en confirme la délivrance.

(11) Si le [juge] n'est pas convaincu qu'un mandat d'interception continue à être nécessaire, il rend une ordonnance qui le révoque.

(12) Lorsqu'un mandat d'interception délivré ou renouvelé conformément au présent article est révoqué en vertu du paragraphe (11), le mandat cesse de produire ses effets dès cette révocation.

(13) Lorsque la délivrance d'un mandat d'interception est confirmée conformément au paragraphe (10) du présent article, les dispositions de l'article 10 s'appliquent quant à sa durée, comme si la date de l'ordonnance confirmant la délivrance du mandat d'interception était la date à laquelle le mandat a été délivré pour la première fois.

Rapport sur les progrès

15. Un [juge] ayant délivré un mandat d'interception peut, au moment de sa délivrance ou à tout moment avant la date de son expiration, demander par écrit au fonctionnaire habilité au nom duquel la demande de mandat d'interception concernée a été faite, de lui établir un rapport par écrit sur:

a. les progrès de réalisation des objectifs du mandat d'interception; et

b. tout autre sujet que le [juge] considère nécessaire.

Rapport final

16. (1) Dès que possible après l'expiration d'un mandat d'interception, le fonctionnaire habilité qui en a fait la demande rédige un rapport écrit au [juge] ayant accordé le mandat d'interception ou, si ce [juge] ne peut pas agir, à un autre [juge], sur la manière dont le pouvoir conféré par le mandat d'interception a été exécuté et sur les résultats obtenus par l'exécution de ce pouvoir.

(2) Chaque rapport établi aux fins du paragraphe (1) contient les informations suivantes:

a. l'endroit où le dispositif d'interception a été placé;

b. le nombre d'interceptions effectuées au moyen du dispositif d'interception;

c. si des preuves pertinentes ont été obtenues au moyen du dispositif d'interception;

d. si des preuves pertinentes ont été, ou doivent être, utilisées au cours d'une procédure pénale; et

e. si des enregistrements d'une communication interceptée en vertu du mandat d'interception ont été détruits conformément à l'Article 23 et, dans la négative, pourquoi ils n'ont pas été détruits.

Partie II

TITRE III – EXÉCUTION D'UNE INTERCEPTION

Exécution d'un mandat d'interception

17. (1) Un fonctionnaire habilité exécutant un mandat d'interception peut intercepter les communications indiquées dans le mandat conformément aux termes du mandat d'interception, pendant leur transmission au moyen d'un dispositif d'interception.

(2) Un fonctionnaire habilité peut demander à une personne d'intercepter des communications si le mandat le spécifie.

(3) Un fonctionnaire habilité ou une personne qui, en vertu d'un mandat d'interception, intercepte ou favorise l'interception de communications, doit prendre toutes les mesures raisonnables pour minimiser l'impact de l'interception sur les tiers.

(4) Un fonctionnaire habilité ou une personne agissant en vertu d'un mandat d'interception ou conformément audit mandat, ou une personne qui aide de bonne foi une personne dont elle a de bonnes raisons de croire qu'elle agit conformément à une telle autorisation, n'encourt aucune responsabilité pénale ou civile pour tout agissement raisonnablement effectué relevant du mandat d'interception.

Intrusion dans des locaux pour exécuter un mandat d'interception

18. Si un mandat d'interception contient la permission pour un fonctionnaire habilité de pénétrer dans des locaux en vertu de paragraphe (3) de l'Article 9, un fonctionnaire habilité peut, à l'heure précisée sur le mandat d'interception, pénétrer dans les locaux et accomplir les actes qu'il est autorisé à accomplir conformément au mandat d'interception.

Devoir d'assistance

19. (1) Une personne qui fournit des services de communication permet à un fonctionnaire habilité d'exercer un mandat d'interception et l'aide si cela se révèle nécessaire et raisonnable.

(2) Lorsque le fonctionnaire habilité prévoit d'ordonner à une personne d'intercepter des communications, le [juge] oblige cette personne à exécuter l'interception conformément au mandat d'interception délivré en conformité avec le paragraphe (1) de l'Article 8 ou de l'Article 14.

Défaut d'assistance

20. Une personne qui, intentionnellement et sans excuse ou justification légitime, n'autorise pas ou n'aide pas un fonctionnaire habilité dans l'exécution d'une interception selon les indications des paragraphes (1) et (2) de l'Article 19, commet une infraction passible, sur déclaration de sa culpabilité, d'une amende maximale de [montant] et d'un emprisonnement maximal de [période].

Confidentialité de la communication interceptée

21. (1) Un fonctionnaire habilité prend les dispositions suivantes, nécessaires pour garantir la confidentialité de l'interception:

a. limiter au minimum nécessaire et aux fins pour lesquelles le mandat d'interception a été délivré:

i. la mesure dans laquelle la communication interceptée est divulguée;

ii. le nombre de personnes auxquelles une partie de cette communication est divulguée;

iii. la mesure dans laquelle cette communication est copiée; et

iv. le nombre de copies faites de toute partie de la communication;

et

b. veiller à ce que chaque copie faite de toute partie de cette communication soit

i. stockée de façon sécurisée aussi longtemps que sa rétention est nécessaire, et

ii. détruite conformément aux dispositions de l'Article 23.

(2) Toute personne autorisée à intercepter des communications ou à fournir une aide à l'exécution de l'interception préserve la confidentialité des informations suivantes:

a. l'existence et le contenu du mandat d'interception;
b. les détails de la délivrance du mandat d'interception et des éventuels renouvellement ou modification de l'une ou de l'autre;
c. l'existence et le contenu de toute demande d'assistance;
d. les mesures prises pour exécuter le mandat d'interception;
e. tous les matériaux interceptés ainsi que les données de communication associées.

Infraction à la confidentialité des informations sur l'interception

22. Une personne qui, intentionnellement et sans excuse ou justification légitime, divulgue une information qu'elle est tenue de conserver confidentielle conformément aux dispositions de l'Article 21, commet une infraction passible, sur déclaration de sa culpabilité, d'une amende maximale de [montant] et d'un emprisonnement maximal de [période].

Destruction des enregistrements

23. (1) Un fonctionnaire habilité veille à ce que les enregistrements sans rapport avec l'objectif du mandat d'interception soient immédiatement détruits.

(2) Tout enregistrement des informations obtenues par le biais de l'interception de communications en application d'un mandat d'interception, qu'il s'agisse d'informations totalement ou partiellement, et directement ou indirectement en rapport avec l'objectif du mandat d'interception, doit être détruit dès qu'il apparaît qu'aucune poursuite, ou qu'aucune autre poursuite, ne sera engagée dans laquelle ces informations sont susceptibles de devoir être produites comme éléments de preuve.

(3) Rien dans le paragraphe (2) ne s'applique à un quelconque enregistrement d'une information citée dans une procédure devant un tribunal.

(4) Chaque rapport fait à un [juge] conformément à l'article 16 indique si le paragraphe (2) a déjà été respecté et, dans la négative, le [juge] donne des instructions relatives à l'éventuelle destruction de l'enregistrement selon ce qu'il estime nécessaire pour assurer le respect de ce paragraphe, y compris l'exigence selon laquelle le [juge] doit être informé lorsque l'enregistrement aura été détruit.

Non destruction des enregistrements

24. Une personne qui, intentionnellement et sans excuse ou justification légitime, ne respecte pas les exigences des paragraphes (1) et (2) de l'Article 23, commet une infraction passible, sur déclaration de sa culpabilité, d'un emprisonnement maximal de [période] et d'une amende maximale de [montant].

Partie II

TITRE IV – ÉQUIPEMENTS D'INTERCEPTION

Équipement recensé doté de capacités d'interception

25. [(1) Le [*ministre*], par avis publié au [*Journal officiel*], déclare tout instrument, dispositif ou équipement filaire, sans fil, électronique, optique, magnétique ou de tout autre type principalement conçu à des fins d'interception de communications, dans les conditions ou les circonstances précisées dans l'avis, comme étant un équipement recensé doté de capacités d'interception.

(2) Un avis peut être modifié ou retiré à tout moment.

(3) Le premier avis aux termes du paragraphe (1) est délivré par le [ministre] dans les [*trois mois*] qui suivent la date d'entrée en vigueur de la présente Loi.

(4) Avant que le [Ministre] n'exerce le pouvoir qui lui est accordé en vertu du paragraphe (1), le projet de l'avis proposé est publié au [*Journal officiel*], accompagné d'un avis invitant toutes les parties intéressées, dans un délai déterminé, à soumettre par écrit leurs commentaires et leurs observations en rapport avec l'avis proposé.

(5) Un délai de [*un mois*] doit s'écouler entre la publication du projet d'avis et l'avis visé au paragraphe (1).

(6) Le paragraphe (4) ne s'applique pas:

a. si le [Ministre], à la suite des commentaires et des observations reçus aux termes du paragraphe (4), décide de publier un avis mentionné au paragraphe (1) sous une forme modifiée;

b. à toute déclaration aux termes du paragraphe (1) au sujet de laquelle le [ministre] est d'avis que l'intérêt public nécessite qu'elle soit faite sans délai.

(7) Tout avis en vertu du paragraphe (1) doit, avant sa publication au [*Journal officiel*] faire l'objet d'une résolution de ratification.]

Interdiction de fabrication, de possession et d'utilisation d'équipement recensé doté de capacités d'interception

26. [(1) Sous réserve du paragraphe (2) du présent article et de l'Article 27, une personne ne doit pas assembler, posséder, vendre, acheter et utiliser un équipement recensé.

(2) Le paragraphe (1) ne s'applique pas dans le cas d'une autorisation accordée en vertu de l'Article 28.]

Utilisation d'un équipement sans autorisation

27. [(1) Une personne qui, intentionnellement et sans excuse ou justification légitime, contrevient aux exigences de l'Article 26 ou ne les observe pas, commet une infraction passible, sur déclaration de sa culpabilité, d'un emprisonnement maximal de [période] et d'une amende maximale de [montant].

(2) Lorsqu'une personne est reconnue coupable d'un crime allant à l'encontre du paragraphe (1), le tribunal peut, dans le cadre de la sentence, ordonner que l'équipement doté de capacités d'interception soit confisqué.

Remarque: un pays peut inclure des dispositions autorisant la résiliation de la licence au cas où le prestataire de communication contreviendrait, intentionnellement, et sans excuse ou justification légitime, aux exigences de l'Article 26 ou ne les observerait pas.].

Autorisation d'utiliser un équipement recensé doté de capacités d'interception

28. [(1) Le [Ministre] peut, sur demande, exempter une personne, un organisme privé ou un organisme chargé de l'application de la loi de l'un ou de tous les agissements interdits répertoriés en vertu du paragraphe (1) de l'Article 26 pendant la durée et aux conditions que le [Ministre] définit.

(2) Le [Ministre] ne peut accorder une dérogation en vertu du paragraphe (1) que s'il est convaincu que

a. cette dérogation est dans l'intérêt public;

b. la fin pour laquelle l'équipement recensé sera fabriqué, assemblé, possédé, vendu, acheté ou médiatisé est raisonnablement nécessaire; et que

c. des circonstances spéciales justifient une telle dérogation.

(3) Une dérogation en vertu du paragraphe (1) est accordée en délivrant à la personne concernée un certificat d'exemption dans lequel son nom et l'étendue, la période et les conditions de l'exemption sont précisées.

(4) Un certificat d'exemption accordé en vertu du paragraphe (3) est publié au [*Journal officiel*] et devient valable à la date de cette publication.

(5) Un certificat d'exemption peut, à tout moment et de manière similaire, être modifié ou retiré par le [ministre].

(6) Un certificat d'exemption expire

a. au terme de la période pour laquelle il a été accordé; et

b. lors du retrait aux termes du paragraphe (5)].

TITRE V – DIVULGATION DE DONNÉES DE COMMUNICATION STOCKÉES

Interdiction d'accès aux données informatiques stockées

29. (1) L'accès illégal aux communications stockées est interdit.

(2) Une personne qui, intentionnellement et sans excuse ou justification légitime, accède aux communications stockées, ou autorise une autre personne à accéder à une communication stockée, le permet ou le tolère commet une infraction passible, sur déclaration de sa culpabilité, d'un emprisonnement maximal de [période] et d'une amende maximale de [montant].

(3) Une excuse légitime est donnée si:

a. l'accès à la communication stockée répond à une ordonnance de divulgation;

b. l'accès à la communication stockée répond à un mandat d'interception; ou

c. l'accès à la communication stockée répond à d'autres mandats et ordonnances délivrés conformément à la législation relative à la procédure.

Partie II

Divulgation de données de communication stockées

30. (1) Lorsqu'il apparaît à la [personne désignée] [au juge] qu'une personne fournissant un service de communication est ou pourrait être en possession de données de communications, ou être capable d'en obtenir, la [personne désignée] [le juge] peut, par ordonnance de divulgation, exiger du prestataire de communication:

a. qu'il divulgue à un fonctionnaire habilité l'intégralité des données en sa possession ou obtenues par la suite, ou

b. si le prestataire n'est pas déjà en possession des données, qu'il obtienne les données et les divulgue à un fonctionnaire habilité.

(2) Un(e) [personne désignée] [un juge] ne délivre pas d'ordonnance de divulgation en rapport avec des données de communications sauf s'il est convaincu que celle-ci est nécessaire pour obtenir les données et les divulguer à un fonctionnaire habilité.

(3) Un(e) [personne désignée] [un juge] ne délivre pas d'ordonnance de divulgation en vertu du paragraphe (2) en rapport avec des données de communication sauf s'il est convaincu que celle-ci est nécessaire pour obtenir ces données;

a. dans l'intérêt de la sécurité nationale;

b. dans le but d'empêcher ou de détecter un crime, ou de prévenir des troubles publics;

c. dans l'intérêt de la sécurité publique;

d. dans le but de protéger la santé publique;

e. dans le but, en cas d'urgence, de prévenir un décès, une blessure ou un dommage à la santé physique ou mentale d'une personne, ou d'atténuer une blessure ou un dommage à la santé physique ou mentale d'une personne.

(4) Une ordonnance de divulgation en vertu du présent article indique:

a. les données de communication auxquelles elle s'applique;

b. le fonctionnaire habilité auquel la divulgation doit être faite;

c. la manière dont la divulgation doit être faite;

d. les sujets relevant du paragraphe (3) en référence desquels l'ordonnance est délivrée; et

e. la date à laquelle elle est délivrée.

(5) Une ordonnance de divulgation n'exige pas;

a. que des données de communications soient divulguées après la fin du délai d'un mois débutant à la date à laquelle l'ordonnance est délivrée; ou

b. la divulgation, après la fin de ce délai, de données de communications dont le fournisseur du service de communication n'est pas en possession, ou qu'il doit obtenir pendant ce délai.

(6) Sous réserve du paragraphe (7), le prestataire d'un service de communication auquel une ordonnance de divulgation est délivrée en vertu du présent article ne divulgue à personne l'existence ou l'application de l'ordonnance, ou toute information à partir de laquelle cette existence ou application peut être raisonnablement déduite.

(7) La divulgation mentionnée au paragraphe (6) peut être faite à:

a. un dirigeant ou un agent du prestataire de service afin de garantir le respect de l'ordonnance de divulgation;

b. un conseiller juridique afin d'obtenir des conseils ou une représentation juridiques en rapport avec l'ordonnance de divulgation,

et une personne mentionnée à l'alinéa (a) ou (b) ne divulgue pas l'existence ou l'application de l'ordonnance de divulgation, sauf au fonctionnaire habilité désigné dans l'avis afin de:

i. garantir le respect de l'avis, ou d'obtenir des conseils ou une représentation juridiques en rapport avec l'ordonnance de divulgation, dans le cas d'un dirigeant ou d'un agent du prestataire de service; ou de

ii. donner des conseils ou faire des représentations juridiques en rapport avec l'ordonnance de divulgation, dans le cas d'un conseiller juridique.

Non respect de la confidentialité de l'information figurant sur l'ordonnance de divulgation

31. Une personne qui, intentionnellement et sans excuse ou justification légitime, divulgue des éléments de ce dont elle doit protéger la confidentialité en vertu du paragraphe (6) de l'Article 30, commet une infraction passible, sur déclaration de sa culpabilité, d'un emprisonnement maximal de [période] et d'une amende maximale de [montant].].

TITRE VI – COÛT DE L'INTERCEPTION

Répartition des coûts

32. (1) Tous les coûts engagés par un prestataire de communication qui lui permettent d'intercepter des communications et/ou de stocker des communications, y compris les coûts d'investissement, les coûts techniques, les coûts d'entretien et les coûts d'exploitation, doivent être supportés par le prestataire de communication.

(2) Un pays peut établir le modèle de remboursement des coûts directs engagés par le prestataire de communication en matière de personnel et d'administration nécessaires à la fourniture d'une aide pour l'exécution du mandat d'interception.

TITRE VII – MESURES DE PROTECTION

Secret professionnel

33. [Si les preuves obtenues par l'interception de communications sont privilégiées en vertu de la [loi] protégeant:

a. [le secret médical];

b. [les communications à caractère professionnel entre un conseiller juridique et un client];

c. [le secret bancaire];

d. [le secret financier];

e. [tout autre secret qu'un pays souhaite protéger en vertu de la loi]

ces preuves doivent rester confidentielles et ne pas être citées devant un tribunal, sauf en cas d'accord de la personne autorisée à renoncer à ce privilège].

Suivi de l'interception de communications

34. [(1) Il est créé une autorité de contrôle indépendante dotée du pouvoir de donner des directives et d'effectuer des contrôles afin de s'assurer que l'interception de communications est réalisée conformément à autorisation légale.

(2) Au lieu de créer une autorité de contrôle indépendante distincte, un pays peut investir une autorité qui:

a. ne participe pas activement au processus d'enquête; et

b. a la capacité de réaliser les fonctions nécessaires pour superviser l'interception avec les fonctions de l'autorité de contrôle indépendante.

(3) [7] jours au plus après avoir soumis un rapport final (Article 16), un fonctionnaire habilité soumet les informations suivantes à l'autorité de contrôle indépendante afin de tenir le Registre des mandats d'interception:

a. date de délivrance du mandat;

b. [juge] ayant délivré le mandat;

c. organisme auquel le mandat a été délivré; et

d. période pendant laquelle le mandat a été en vigueur.

(4) L'autorité de contrôle indépendante:

a. tient le Registre des mandats d'interception, en notant les informations indiquées au paragraphe (3) de l'Article 34; et

b. soumet un rapport sur le suivi de l'interception de communications au commissaire indépendant à l'interception de communications tous les [*6*] mois

(5) L'autorité de contrôle indépendante peut, moyennant un avis écrit à [l'agent en chef de l'autorité idoine], demander à [l'autorité idoine] de soumettre les informations nécessaires pour s'assurer que l'interception de communications est réalisée conformément à la présente Loi.

(6) Lorsque, en conséquence du suivi, l'autorité de contrôle indépendante estime qu'un fonctionnaire habilité a violé une disposition de la présente Loi, l'autorité de contrôle indépendante peut inclure cette violation dans le rapport sur le suivi de l'interception de communications].

Commissaire indépendant à l'interception de communications

35. [(1) Le Commissaire indépendant à l'interception de communications est nommé par le Parlement.

(2) Le Commissaire indépendant exerce ses fonctions pendant la période, qui ne doit pas être supérieure à [*5*] ans, précisée dans l'acte de sa nomination. Son mandat est cependant renouvelable.

(3) Le Commissaire indépendant, aux fins d'une inspection:

a. peut, après avoir notifié l'agent en chef de l'[organisme], pénétrer, à toute heure raisonnable, dans les locaux occupés par l'[organisme]; et

b. est habilité à avoir un accès libre et sans réserves, à toute heure raisonnable, à tous les dossiers de l'[organisme] liés à l'interception; et

c. est habilité à faire des copies et à prendre des extraits des enregistrements de l'organisme ou du Registre des mandats d'interception; et

d. peut demander à un agent de l'[organisme] de lui donner les informations que le Registre des mandats d'interception considère nécessaires, qu'il s'agisse d'informations en possession de l'agent ou auxquelles l'agent a accès, et qui sont pertinentes pour l'inspection.

(4) L'[agent en chef] d'[un organisme] veille à ce que les agents de l'[organisme] fournissent au Commissaire indépendant l'aide nécessaire en rapport avec l'accomplissement ou l'exercice de ses fonctions ou des pouvoirs de ses fonctions en vertu du présent Article en fonction des demandes raisonnables du Commissaire indépendant.

(5) Toutes les demandes faites par le Commissaire indépendant dans l'exercice de ses fonctions en vertu des paragraphes (3) et (4) doivent recevoir une réponse dans les [*7*] jours.

(6) Lorsque, après une inspection, le Commissaire indépendant estime qu'un fonctionnaire habilité ou un [organisme] a violé une disposition de la présente Loi, il peut engager ses propres enquêtes sur le cas.

(7) Lorsqu'une enquête réalisée en vertu du paragraphe (6) conduit le Commissaire indépendant à découvrir un manquement à la présente loi, celui-ci peut délivrer une décision exécutoire exigeant l'élimination de la violation ou l'arrêt de l'activité qui contrevient à la présente loi.

(8) La décision exécutoire délivrée en vertu du paragraphe (7) doit être délivrée sous forme écrite et présente un caractère obligatoire pour un fonctionnaire habilité, un organisme public ou un organisme privé.

(9) Si un fonctionnaire habilité, un organisme public ou un organisme privé ne respecte pas l'exigence de la décision délivrée en vertu du paragraphe (7) dans les [*14*] jours suivant la réception de la décision, le Commissaire indépendant peut déposer une requête auprès d'un tribunal pour faire exécuter la décision.

(10) Un individu ou l'autorité publique a le droit de faire appel des décisions du Commissaire indépendant devant les tribunaux.].

Partie II

TITRE VIII – ADMISSIBILITÉ DES PREUVES

Admissibilité des communications interceptées en tant qu'éléments de preuve

36. [(1) Seules les données de communications interceptées conformément à la présente loi sont admissibles en tant que preuves en conformité avec la loi relative à l'admissibilité des preuves.

(2) Les détails d'une communication interceptée en vertu d'un mandat d'interception ou d'un mandat d'interception d'urgence ne sont recevables comme preuves par un tribunal contre une personne que si la partie qui entend les présenter donne à cette personne un préavis raisonnable de son intention, accompagné

a. d'une transcription de la communication privée, lorsque cette personne entend la présenter sous forme d'enregistrement ou d'une attestation écrite énonçant les détails complets de la communication lorsque cette personne entend en présenter des preuves orales; et

b. d'une attestation de l'heure, du lieu (si celui-ci est connu) et de la date de la communication, ainsi que des noms et adresses des parties à la communication, s'ils sont connus.

(3) Même si la communication a été interceptée en vertu d'un mandat d'interception ou d'une autorisation d'urgence, les éléments de preuve d'une communication interceptée au moyen d'un dispositif d'interception, ou de sa substance, de son sens ou de son objet, ne peuvent être présentés devant un tribunal que si celles-ci ont un rapport avec le crime indiqué dans l'Annexe.

Irrecevabilité des communications interceptées en tant qu'éléments de preuve

37. Lorsqu'une communication interceptée au moyen d'un dispositif d'interception autrement qu'en application d'un mandat d'interception ou d'un mandat d'interception d'urgence délivré en vertu de l'Article 14 ou d'une autorité conférée par ou en vertu de tout autre texte applicable est parvenue à la connaissance d'une personne en conséquence directe ou indirecte de cette interception ou de sa divulgation, aucune preuve ainsi acquise de cette communication, ou de sa substance, de son sens, ou de son objet, et aucune autre preuve obtenue en conséquence directe ou indirecte de l'interception ou de la divulgation de cette communication, ne doit être donnée à l'encontre d'une personne, excepté dans des procédures relatives à l'interception illégale d'une communication au moyen d'un dispositif d'interception ou à la divulgation illégale d'une communication interceptée illégalement de cette manière.].

Partie II

TITRE IX – ANNEXE

Modification de l'Annexe 38. (1) Le Ministre peut, par ordonnance, faire des ajouts à la liste ou des retraits de la liste d'infractions contenues dans l'Annexe.

(2) Une ordonnance faite en vertu du paragraphe (1) doit faire l'objet d'une résolution de ratification.

Règlement 39. (1) Le Ministre peut promulguer un règlement pour appliquer l'objet de la présente loi.

(2) Un règlement promulgué en vertu du paragraphe (1) doit faire l'objet d'une résolution de ratification du parlement.

ANNEXE

(Article 8 (1) (a) (ii))

(1) [Meurtre, homicide involontaire ou trahison].

(2) [Enlèvement ou rapt].

(3) [Blanchiment d'argent] contraire à la [Loi sur le produit du crime et le blanchiment d'argent (prévention)].

(4) [Production, fabrication, fourniture ou autre trafic de drogue dangereuse] en violation de la [Loi relative aux drogues dangereuses].

(5) [Importation ou exportation d'une drogue dangereuse] en violation de la [Loi relative aux drogues dangereuses].

(6) [Importation, exportation ou transbordement de toute arme à feu ou munitions] en violation de la [Loi sur les armes à feu].

(7) [Fabrication ou trafic d'armes à feu ou de munitions] en violation de la [Loi sur les armes à feu].

(8) [Détention illégale d'une arme prohibée ou de toute autre arme à feu ou munition] contraire à un [article de la Loi sur les armes à feu].

(9) Infraction contraire à un [article de la Loi sur la prévention de la corruption].

(10) [Incendie criminel].

(11) [Convention internationale sur le détournement, infractions terroristes, etc.].

(12) [Loi sur la prévention du terrorisme].

(13) Tentative ou complot pour commettre une infraction relevant de l'un des alinéas qui précèdent, ou aide, concours, conseils, ou autre forme d'assistance pour commettre une telle infraction.

Partie III:
Notes explicatives relatives au modèle de texte législatif sur l'interception de communications

INTRODUCTION

1. Le présent texte législatif fournit un modèle de cadre juridique pour une interception légale des communications. Les principaux objectifs de ce texte sont d'interdire l'interception illégale de communications, de définir un nombre limité de circonstances conduisant à l'autorisation de l'interception, d'établir des normes pour donner cette autorisation et l'exécuter, d'équilibrer la puissance de l'État et la vie privée de l'individu et de protéger la confidentialité et la liberté des communications.

2. Le présent texte législatif a été préparé et adopté conformément au modèle de lignes directrices politiques du premier atelier de consultation du Groupe de travail 1 pour le projet HIPCAR sur les questions relatives à la société de l'information.

3. Ces notes sont préparées pour expliquer le contenu du modèle de texte législatif et doivent être lues simultanément au texte législatif. Elles expliquent l'importance des dispositions et, le cas échéant, reflètent les discussions au sein du Groupe de travail[13] pour le projet HIPCAR[14] et les lignes directrices politiques du premier atelier de consultation du Groupe de travail 1 pour le projet HIPCAR. Ces notes ne sont pas une description détaillée de la loi et ne sont pas destinées à en être une. Aussi, lorsqu'un article ou une partie d'un article ne semble pas nécessiter de clarification, de commentaires ou de références exhaustifs, ou lorsqu'une disposition particulière n'a donné lieu à aucune discussion au sein du Groupe de travail, aucune explication détaillée n'est fournie.

4. Le texte législatif est constitué de neuf titres:

   - **Le Titre I** fournit les définitions et fixe les objectifs du texte législatif;
   - **Le Titre II** interdit l'interception illégale et établit l'ensemble limité de conditions dans lesquelles l'interception est considérée comme légale. Il contient également des dispositions établissant la procédure permettant d'obtenir une autorisation pour intercepter des communications. Enfin, il fournit les raisons pour lesquelles un mandat d'interception est accordé aux autorités concernées, ainsi que les règles relatives à la durée, au renouvellement et à la révocation des mandats;
   - **Le Titre III** élabore un cadre pour l'exécution de l'interception de communications;

---

13 Les membres des Groupes de travail pour le projet HIPCAR incluent les représentants du ministère et du régulateur nommés par leurs gouvernements nationaux, les organismes régionaux et observateurs concernés, tels que les opérateurs et d'autres parties prenantes intéressées. Les mandats des Groupes de travail sont disponibles à l'adresse: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.
Le second atelier de consultation (stade B) du Groupe de travail 1 pour le projet HIPCAR sur le cadre législatif applicable aux TIC – questions relatives à la société de l'information s'est déroulé à la Barbade, du 23 au 26 août 2010. Les participants ont examiné le projet de modèle de texte législatif sur le domaine de travail respectif, en ont discuté et l'ont adopté par un large consensus. Lorsque l'expression «Groupe de travail » apparaît dans le présent document, elle fait référence à l'atelier susmentionné.

14 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 de 3 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. Le projet est mis en œuvre par l'Union internationale des télécommunications (UIT) en collaboration avec le Secrétariat de la Communauté des Caraïbes (CARICOM) et l'Union des télécommunications des Caraïbes (CTU).

- **Le Titre IV** aborde la question de l'interdiction des équipements dotés de capacités d'interception et suggère le régime de réglementation de l'utilisation de ce type d'équipement;
- **Le Titre V** fournit des recommandations pour la mise en œuvre des dispositions relatives à la divulgation des données de communications stockées;
- **Le Titre VI** couvre la question de la répartition des coûts engagés par l'interception;
- **Le Titre VII** fournit des recommandations pour les mesures de protection des communications privilégiées et donne la possibilité de mettre en place des mesures de suivi et de contrôle;
- **Le Titre VIII** contient des recommandations sur la question de la recevabilité des preuves;
- **Le Titre IX** fournit une annexe des crimes graves auxquels le Titre I du présent texte législatif fait référence.

COMMENTAIRE DES ARTICLES

TITRE I – PRÉAMBULE

5. Le Titre I fournit les dispositions préliminaires, telles que le titre, les définitions, l'objectif et la clause d'entrée en vigueur.

6. Les articles 2 et 3 ont donné lieu à une discussion au sein du Groupe de travail pour le projet HIPCAR en ce qui concerne le style de la rédaction législative dans différents pays. La question de savoir si l'article contenant les définitions devait être placé avant l'article indiquant les objectifs du modèle de texte législatif a fait l'objet de discussions. Il a été convenu de laisser chaque État trancher cette question.

Article 3. Définitions

7. Les termes entre crochets indiquent les choix dont disposent les États dans le cadre de la mise en œuvre de la législation. En raison des textes applicables existants ou du système juridique national, un pays peut décider de choisir un autre terme pour les mots figurant entre crochets.

8. La définition d'«Organisme» fournie par le paragraphe (1) permet aux États bénéficiaires de choisir l'organisme chargé des interceptions. Un débat a eu lieu au sein du Groupe de travail sur l'opportunité de faire des recommandations quant aux organismes auxquels ce pouvoir devait être accordé. Cependant, il a été convenu que chaque pays déciderait lui-même de l'organisme auquel la capacité d'intercepter les communications serait accordée.

9. Le même choix est offert par le paragraphe (2), qui donne la définition d'un fonctionnaire habilité. S'il est extrêmement important de déterminer et de définir qui pourra demander un mandat d'interception et effectuer les procédures d'interception, le choix est laissé aux États bénéficiaires. Ils détermineront leur propre liste de personnes auxquelles la permission de demander une autorisation d'intercepter les communications sera accordée.

10. Le paragraphe (3) définit le terme «communication» aux fins de la construction d'un cadre de réglementation de l'interception. Pour le texte législatif qui interdit l'interception de communications, il est très important, en premier lieu, de rédiger une définition neutre du point de vue technologique et, en second lieu, d'éviter les limitations susceptibles d'exclure des types pertinents de communications de l'interdiction d'interception. Voilà pourquoi la définition de «communication» est rédigée de façon à inclure à la fois les *données* et les *signaux* acheminés par l'intermédiaire d'un réseau de communication électronique ou d'une partie de ce réseau au moyen d'un dispositif électronique, mécanique, optique, à ondes, électromécanique, ou d'un autre type de dispositif.

11. La définition de **«prestataire de communication»** est construite dans le paragraphe (4) afin d'imposer l'obligation d'intercepter des communications. Dans la mesure où la Loi prévoit la possibilité d'obliger les opérateurs à intercepter des communications en conformité avec le mandat, pour protéger les petits prestataires de communication qui ne sont pas capables de procéder à une interception, chaque pays définit le nombre de clients desservis par un prestataire de communication afin de fournir au tribunal la possibilité d'obliger l'opérateur (le prestataire) de communication à effectuer des interceptions.

12. La définition de **«réseau de communication»** a fait l'objet d'une importante discussion. En premier lieu, la discussion a porté sur le fait de savoir si la définition devait inclure la transmission de l'information ou la fourniture de services de communication. En second lieu, il s'agissait de décider si le réseau de communication faisait principalement référence aux services ou aux installations et à l'infrastructure. Enfin, le Groupe de travail s'est interrogé sur la nécessité de fournir des définitions séparées pour les réseaux de communication public et privé aux fins de l'élaboration du cadre de réglementation de l'interception de communications.

13. Il a été convenu que la définition du réseau de communication devait être rédigée de manière à fournir une distinction claire entre les installations, l'infrastructure et les services. Par conséquent, le Groupe de travail a décidé de définir le réseau de communication comme toute installation ou infrastructure utilisée par une personne pour fournir des services de communication.

14. En outre, il a été décidé qu'il n'était pas nécessaire de faire une distinction entre les réseaux publics et privés aux fins de l'interception. Cette remarque est d'abord applicable à l'interdiction de l'interception: les communications doivent être protégées de la même façon, quel que soit le réseau sur lequel elles transitent. De plus, pour l'octroi du pouvoir d'intercepter, des mesures de protection et des procédures identiques sont applicables pour les deux types de réseaux, afin de protéger de la même manière les droits des personnes qui utilisent différents types de réseaux. Par conséquent, aucune distinction n'a été faite entre réseau de communication public et réseau de communication privé aux fins de la présente loi.

15. Le Groupe de travail a également discuté de la définition de «communication» en ce qui concerne la portée du texte législatif. La question de savoir si le texte législatif devait réglementer l'interception de tous les types de communications, y compris le service postal, ou uniquement les communications électroniques a été soulevée. Bien qu'un grand nombre de participants aient estimé que les services postaux et les communications électroniques n'avaient pas lieu d'être traités différemment pour ce qui est de l'interception (par ex., l'interception doit être interdite, des mesures de protection solides doivent être mises en place), le Groupe de travail a convenu que son mandat ne couvre pas l'interception des services postaux.

16. La définition de **«service de communication»** fournie par le paragraphe (6) est importante pour faire la distinction entre réseaux de communication et services de communication. Elle établit que, aux fins du présent texte législatif, le service de communication inclut un service fourni tant par la personne qui exploite le réseau que par la personne qui fournit uniquement le service sans faire fonctionner le réseau.

17. Les définitions de **«personne désignée»** et d'**«ordonnance de divulgation»** sont fournies par les paragraphes (7) et (8), respectivement, pour les besoins du Titre V – divulgation de données de communications stockées. Ces définitions ne doivent être incluses par un État membre que s'il adopte l'approche suggérée par le Titre V et met en œuvre les dispositions réglementant l'accès aux données de communications qui n'ont pas encore commencé d'être transmises ou qui ont déjà été transmises par un réseau de communication.

18. Le paragraphe (9) fournit l'une des principales définitions de ce texte législatif. Afin de déterminer ce qui est interdit et réglementé par le présent texte législatif, ce paragraphe établit qu'«**intercepter»** désigne l'acquisition, la visualisation, la capture, la surveillance ou la copie du contenu ou d'une partie du contenu d'une communication pendant la transmission grâce à l'utilisation d'un dispositif ou d'une méthode d'interception. Cette définition fournit deux éléments

essentiels pour définir ce que le verbe «intercepter» inclut. En premier lieu, elle comprend les différentes actions qui peuvent être menées pour intercepter une communication, comme visualiser, surveiller, copier et acquérir. En second lieu, la définition établit que, dans le cadre de l'interception, tout ceci est uniquement applicable à la communication pendant sa transmission. Le Groupe de travail a discuté du fait que, dans la mesure où la signification de dispositif d'interception est également fournie dans le texte législatif, il n'y avait pas besoin de fournir une explication détaillée pour dispositif ou méthode d'interception dans la définition d'intercepter.

19. Le paragraphe (10) définit le terme **«communication interceptée»** afin de la distinguer, par exemple, des données de communications stockées. Même si la communication est stockée une fois l'interception faite, la principale approche pour la qualifier d'interceptée est qu'elle a été acquise pendant sa transmission. La définition de communication interceptée est également pertinente pour appliquer les dispositions protégeant la confidentialité des données interceptées et les obligations de détruire tous les enregistrements.

20. La définition de l'interception incluant une référence au terme «dispositif d'interception», ce dernier est défini par le paragraphe (11). La définition de **«dispositif d'interception»** a été conçue pour inclure tout instrument, équipement ou appareil électronique, mécanique, optique, à ondes ou électromécanique utilisé ou susceptible d'être utilisé, en tant que tel ou combiné avec un autre instrument, équipement, programme ou appareil en vue d'intercepter une communication. Lors de la séance plénière de l'atelier de consultation, la discussion a porté sur le fait de savoir si la définition de dispositif d'interception devait inclure les logiciels. Certains participants ont fait remarquer que les logiciels peuvent être utilisés pour effectuer une interception. Cependant, il a été convenu que les logiciels ne peuvent pas, en soi, sans matériel, être utilisés pour intercepter les communications or la définition de dispositif d'interception couvre tout type de matériel. Par conséquent, il a été convenu qu'il n'était pas nécessaire d'inclure les logiciels dans cette définition.

21. Afin de protéger les activités normales des entreprises, le paragraphe (11) exclut tout instrument, équipement ou appareil, ou tout composant dudit instrument, équipement ou appareil fourni et utilisé dans le cadre normal de l'exploitation d'une entreprise, soit par les clients, soit par les prestataires de communication.

22. Le paragraphe (12) fournit la définition du **«mandat d'interception»** en faisant référence à l'Article 8. La principale discussion concernant le choix du terme «mandat» plutôt que du terme «ordre» est incluse dans ce rapport explicatif (Article 8).

23. Aux fins du cadre de l'interception de communications, le paragraphe (13) définit ce qu'est un **«équipement recensé»**. Il convient de noter que le terme «équipement recensé» est différent de celui de «dispositif d'interception». Alors que le dispositif d'interception est un dispositif (incluant des équipements à double usage) qui peut être utilisé pour réaliser une interception, l'équipement recensé fait référence au régime spécial développé pour restreindre l'utilisation de l'équipement principalement conçu en vue d'une interception. Il est conseillé aux pays de n'inclure la définition d'équipement recensé que s'ils adoptent l'approche suggérée par l'Article 25 du présent texte législatif.

24. La définition de **«Ministre»** est fournie pour donner aux États la possibilité de définir un ministère qui élaborera les règlements relatifs à l'interception de communications. Cela peut, par exemple, être le ministère de la Sécurité nationale ou tout autre ministère auquel le pouvoir de traiter des questions d'interception est octroyé.

25. La définition d'une «personne» fournie par le paragraphe (15) a été rédigée par le Groupe de travail afin d'inclure aussi bien une personne morale qu'une entité non constituée en personne morale.

26. Le terme **«données de communications stockées»** est inclus dans la liste de définitions, la distinction entre communication pendant sa transmission et communication qui n'a pas commencé à être transmise sur un système de communication ou qui a achevé de l'être étant pertinente pour établir une distinction nette entre l'interception et la divulgation de données de communications

stockées. Le présent modèle de texte législatif fournit différents cadres pour accorder le pouvoir d'intercepter une communication en train d'être transmise et fournir un accès aux communications stockées. Il est essentiel de bien faire la distinction entre ces deux procédures et deux types de communications différents en termes d'interception.

1.7. Article 4: Application

27. Le principal objectif de cet Article est de déterminer la portée du modèle de texte législatif, de façon à ce que rien dans cet acte législatif spécifique, qui doit exclusivement être applicable dans le contexte de l'interception de communications dans le cas de crimes graves, ne puisse être utilisé pour limiter les droits des individus. Le paragraphe (1) dispose ainsi que rien dans ce texte législatif ne doit être interprété comme nécessitant ou interdisant l'anonymat ou le cryptage des communications. Cette disposition est élaborée pour prévenir l'éventualité d'une utilisation du texte législatif comme un fondement pour interdire le cryptage des communications. Cela ne signifie pas que ce texte législatif interdit à un État bénéficiaire d'établir ce type d'interdiction. Cependant, celle-ci doit être distincte du présent acte législatif.

28. Le paragraphe (1) a donné lieu à d'importantes discussions dans le Groupe de travail et lors de la séance plénière de l'atelier de consultation sur le fait de savoir si le cryptage des communications était un droit des individus et si ce droit devait être limité dans la rubrique du cadre relatif à l'interception de communications. Alors que les orientations politiques soulignaient que le projet du modèle de texte législatif ne devait pas entraver le droit de l'individu à l'anonymat et au cryptage, certains des participants à l'atelier ont dit craindre que le droit de crypter une communication ne gêne l'objectif même de l'interception. Il a toutefois été souligné que l'interdiction du cryptage devait être débattue à un niveau différent, le mandat du Groupe de travail ne couvrant pas cette question. Cependant, si le texte législatif ne contenait pas une disposition limitant l'impact de la loi sur le droit à des communications anonymes et cryptées, cette législation pouvait être interprétée comme un fondement pour interdire le cryptage. Après des discussions intenses, il a été convenu que la limitation explicite du cryptage dépassait la portée du présent modèle de texte législatif et que les lois s'appuyant sur ce modèle ne devaient pas être interprétées comme ayant un quelconque effet sur les droits à l'anonymat ou au cryptage des communications.

29. Le paragraphe (2) est construit de façon à établir une distinction entre l'interception de communications en vertu du présent texte législatif et la réglementation fournie par un autre acte législatif pour certains cas particuliers tels que l'interception effectuée par les services de renseignement. Le Groupe de travail a convenu de préciser au paragraphe (2) de l'Article 4 que le texte législatif ne s'applique pas si la communication est soumise à des procédures d'interception et des structures administratives spéciales dans le cadre d'une autre loi. Cela signifie qu'en cas d'existence d'une autre réglementation applicable à l'interception réalisée par les services de renseignement ou au cours d'activités de contre-terrorisme ou dans des situations similaires ou, comme le Groupe de travail l'a fait remarquer, si une législation relative à l'interception des services postaux existe, le texte législatif ne s'applique pas à ces procédures d'interception spéciales.

Partie III

TITRE II – INTERCEPTION DE COMMUNICATIONS

30. Ce titre du modèle de texte législatif poursuit les principaux objectifs du document: en premier lieu, interdire une interception illégale des communications et, en second lieu, établir le nombre limité de circonstances et de conditions strictes dans lesquelles l'interception peut être autorisée.

31. L'approche de l'interdiction de l'interception de communications adoptée par ce texte législatif est similaire à de nombreuses approches régionales et nationales dans ce domaine, telles que le modèle de loi de l'OECO[15], la législation de l'Australie, de Hong Kong, de l'Afrique du Sud et du Royaume-Uni. La criminalisation de l'interception illégale dans les juridictions nationales est généralement suivie par des dispositions établissant l'excuse légitime de l'interception et réglementant le processus d'autorisation.

32. Toutes les approches nationales considèrent l'interception de communications comme une mesure exceptionnelle limitée aux enquêtes relatives aux crimes graves. En outre, l'interception nécessite une autorisation judiciaire préalable, le plus souvent par ordonnance de la cour, bien que certains pays tels que le Royaume-Uni établissent le droit d'intercepter sans autorisation préalable de la cour. Enfin, l'interception peut être autorisée pour un laps de temps limité. En se fondant sur ces approches, en plus de faire une infraction de l'interception illégale, ce titre:

- explique les circonstances dans lesquelles l'interception est légale;
- établit un ensemble de conditions nécessaires pour les demandes de mandats d'interception;
- détermine la portée, la forme et la durée du mandat d'interception, ainsi que les motifs justifiant son extension et sa révocation.

33. En outre, ce titre établit également un certain nombre de mesures de protection solides visant à protéger la confidentialité des communications et à prévenir l'abus du pouvoir d'interception. Chaque article accordant une autorisation d'interférence est suivi par un ensemble de limitations et de contrôles supplémentaires destinés à s'assurer que l'interception est nécessaire et ne peut pas être évitée dans des circonstances particulières.

Article 5: Interdiction d'interception de communications

34. L'article 5 fait de l'interception illégale une infraction et explique les circonstances qui peuvent justifier la légalité de l'interception. Cette approche permet de commencer par la mise en place d'une mesure de protection stricte, puis de limiter l'interception aux crimes graves et aux questions de sécurité nationale.

35. Le principal objectif du paragraphe (1) est de protéger la vie privée des utilisateurs des services de communication en criminalisant l'interception de toute communication pendant sa transmission autrement qu'en vertu des dispositions du texte législatif. La criminalisation de l'interception illégale est une mesure nécessaire pour protéger les communications d'une intrusion. En premier lieu, l'interception de communications représente une grave atteinte à la vie privée des personnes, ce qui justifie le recours à des sanctions pénales. L'interdiction de l'interception de communications au moyen d'une sanction pénale garantit que la victime obtiendra l'aide des organismes chargés de l'application de la loi pour identifier la source de la conduite criminelle. En outre, la victime ne dispose d'aucun recours en droit civil si l'interception de communications a été réalisée sans pénétration non autorisée dans des locaux privés. Enfin, la criminalisation de l'interception illégale répond également aux attentes raisonnables des correspondants des communications: toute intrusion doit être interdite sauf en cas d'autorisation en conformité avec la loi.

36. Le paragraphe (2) énonce un ensemble d'exceptions bien précises. Cet ensemble d'exclusions est très important pour garantir la légalité de l'interception lorsqu'elle est autorisée et pour justifier l'interception dans certains cas où une autorisation judiciaire n'est pas nécessaire.

[15] Organisation des États de la Caraïbe orientale

37. Le paragraphe (2) (a) justifie le droit d'intercepter une communication conformément à l'autorisation obtenue au tribunal. Le présent modèle de texte législatif réglemente le processus d'obtention et d'exécution de cette autorisation.

38. Le paragraphe (2) (b) stipule que l'interception est légale lorsqu'il existe de bonnes raisons de penser que le correspondant de la communication a donné son consentement à l'interception. Cette disposition est importante pour exclure l'interception consensuelle du champ d'application du texte législatif. Le présent modèle de texte législatif se concentre sur des situations dans lesquelles les correspondants de la communication ne sont pas d'accord avec l'interception, car c'est le seul cas dans lequel l'interception interfère avec le droit au respect de la vie privée. Il n'y a pas interception si les parties l'acceptent. La plupart des approches existantes ne réglementent pas l'interception consensuelle et le suivi des communications des participants, le droit d'intercepter ses propres communications protégeant les intérêts privés de la personne, en particulier dans le contexte du commerce et des affaires. Un correspondant d'une communication prend le risque de divulgation de la communication par un autre correspondant. En outre, le droit du correspondant à prendre des notes précises d'une conversation, puis à les reproduire peut correspondre au droit de procéder à l'écoute téléphonique de ses propres communications comme certaines juridictions l'autorisent.

39. Le paragraphe (2) (c) exclut les données de communication stockées acquises en vertu d'une autre loi. Cette disposition établit une distinction claire entre l'interception, à savoir l'acquisition des communications pendant leur transmission et l'acquisition de données de communications stockées qui n'ont pas débuté ou ont été transmises par un réseau de communication.

40. Le paragraphe (2) (d) rend légale l'interception de communication en tant qu'incident ordinaire à la fourniture de services de communications ou à l'application d'une loi en vigueur en rapport avec l'utilisation de ces services. Cette dérogation est cruciale pour garantir l'activité commerciale régulière des opérateurs de communication. Par exemple, les prestataires de services de communication pourraient se voir demander de détecter et d'éliminer les interférences radio et de veiller au respect des conditions d'octroi de licences ou de faire des tests et des mesures des appareils de communication afin de déterminer s'ils respectent les exigences du règlement ou des conditions de la licence en vertu desquelles ils sont détenus. Ces essais peuvent inclure des interceptions. Dans la mesure où ces interceptions sont nécessaires pour garantir le bon fonctionnement du système de télécommunication, les interceptions réalisées à ces fins ne relèvent pas de la criminalisation.

41. En outre, les opérateurs de services de communication peuvent être tenus de maintenir la qualité du service fourni dans le réseau de communication. Ils peuvent également être soumis à une obligation de respecter les conditions de la licence. Par exemple, ils doivent conduire des interceptions afin de s'assurer que le bruit dans le réseau de communication est maintenu à un niveau acceptable. Par conséquent, les opérateurs de services doivent également être autorisés à intercepter des télécommunications afin de fournir un service de télécommunication, ou de réaliser des contrôles mécaniques ou un contrôle qualité du service. Le paragraphe (2) (d) protège ce droit.

42. Le paragraphe (2) (e). limite la criminalisation de l'interception d'une communication passée par l'intermédiaire d'un réseau de communication configuré de façon à rendre la communication immédiatement accessible au grand public. Cette limitation est importante pour protéger la personne qui intercepte les communications à l'origine non protégées par le droit à la vie privée, celles-ci étant immédiatement accessibles au public.

43. Le paragraphe (2) (f) prévoit une dérogation pour l'interception de communications reçues et transmises sur un réseau qui répond aux besoins d'une société privée ou d'un foyer si l'interception est effectuée par une personne qui détient le droit de contrôler l'exploitation ou l'utilisation du réseau ou qui a le consentement exprès ou implicite d'une telle personne. Cette disposition est particulièrement pertinente pour une personne qui détient le droit de contrôler un réseau de communication au sein d'une société ou d'un ménage qui autorise l'interception de leurs propres

réseaux sans commettre d'infraction. Cela peut inclure, par exemple, la surveillance des appels téléphoniques à l'aide d'un second combiné dans une maison, ou l'enregistrement des appels des clients dans les banques afin de conserver un enregistrement des transactions, l'enregistrement des appels à un service clients dans les grandes sociétés, etc.

44. Le Groupe de travail a discuté de la nécessité de définir le «réseau», auquel le paragraphe (2) (f) fait référence en tant que réseau privé, et d'inclure la définition dans le préambule du modèle de texte législatif. Il a été convenu qu'il n'y avait aucune raison de faire la distinction entre réseaux publics et privés en ce qui concerne l'interception. Une personne qui utilise un réseau de communication a le droit d'être protégée d'une interception illégale, que le réseau en question soit public ou privé. Les communications doivent être protégées d'une interception dans les deux types de réseaux. Le Groupe de travail a décidé de ne définir les réseaux internes des sociétés et les réseaux des foyers que dans le présent paragraphe pour les besoins de cette disposition.

45. Le paragraphe (3) prévoit un autre ensemble d'exceptions. D'après le paragraphe (3) (a) l'interception de communications envoyées par, ou destinées à une personne qui a donné son consentement pour l'interception est considérée comme légale. Cette disposition suit l'approche consistant à exclure l'interception consensuelle de la criminalisation. Les paragraphes (2) (b) et (3) (a) sont différents en ceci que ce dernier couvre le cas dans lequel un consentement a clairement été exprimé.

46. Le paragraphe (3) (b) fournit une excuse légitime pour l'interception faite en cas d'urgence. Cette disposition est importante pour garantir le droit de prendre toutes les mesures raisonnables afin de prévenir un décès, une blessure ou un dommage à la santé physique ou mentale d'une personne, ou d'atténuer une blessure ou un dommage à la santé physique ou mentale d'une personne, ou dans l'intérêt de la sécurité nationale lorsqu'il n'est pas possible de demander une autorisation à l'avance. Cependant, il convient de particulièrement insister sur le fait que cette disposition ne couvre que les cas de réelle urgence.

Article 6. Demande du mandat d'interception

47. L'article 6 vise à établir la procédure de demande initiale d'autorisation d'interception.

48. Le paragraphe (1) stipule qu'un fonctionnaire habilité peut demander *ex parte* à un [juge] un mandat pour intercepter des communications dans tous les cas où il y a de bonnes raisons de penser que les conditions de délivrance du mandat d'interception sont remplies. Cette disposition contient plusieurs implications importantes pour la procédure d'autorisation de l'interception: (1) l'interception est accordée en vertu d'un système de mandats; (2) l'interception est autorisée par la cour; (3) la demande est faite *ex parte*.

49. Le système des mandats est un mécanisme classique essentiel adopté par de nombreux pays pour approuver les intrusions, telles que l'entrée dans des locaux et leur fouille et l'interception de communications. Il présente plusieurs avantages. En premier lieu, il implique l'approbation d'une autorité indépendante avant que l'ingérence n'ait lieu. En second lieu, il fournit à l'intrus une permission écrite qu'il ne peut produire que sous certaines conditions. En outre, un système de mandats est particulièrement important lorsque l'intrusion nécessite l'assistance technique d'un tiers. Il s'agit de la situation habituelle lorsque l'interception de communications est réalisée par des réseaux de communication sur ordonnance d'un tribunal. Enfin, le système de mandats présente des avantages dans les cas où une intrusion physique dans les locaux est impliquée.

50. Lorsque l'intrusion ne nécessite aucune assistance externe ni pénétration dans des locaux, l'importance du mandat est déterminée par la gravité du type d'intrusion, tel que l'interception de communications. Si le système de mandats est uniquement mis en œuvre pour certains types d'interceptions, il est possible qu'il encourage le recours à des activités d'interception non soumises à l'exigence d'un mandat. Pour mettre en œuvre une approche intégrée, le présent modèle de texte législatif nécessite qu'un fonctionnaire habilité demande un mandat dans tous les cas où une interception est considérée nécessaire.

51. Cet article introduit l'expression «mandat d'interception» à propos de l'autorisation d'intercepter des communications. Le Groupe de travail a soulevé la question de l'utilisation du terme «mandat» au lieu d'«ordre». Bien que les deux options soient possibles, il a été convenu que le terme «mandat» était préférable pour le champ d'application du présent texte législatif, celui-ci couvrant les cas où une autorisation de pénétrer dans des locaux est nécessaire. Les tribunaux peuvent inclure une clause spéciale dans les mandats pour l'intrusion dans des locaux. Lorsque le tribunal délivre un «ordre d'interception» au lieu d'un mandat, un mandat supplémentaire pour l'entrée est nécessaire. Par conséquent, il a été convenu d'utiliser l'expression «mandat d'interception» aux fins du présent texte législatif.

52. La délivrance de l'autorisation par un tribunal est très importante, dans la mesure où l'indépendance supplémentaire offerte par une décision judiciaire fournit les contrôles et équilibres nécessaires à la gravité de l'intrusion. Conformément au modèle de texte législatif, tous les mandats autorisant l'interception sont uniquement autorisés par les tribunaux, aucune distinction n'étant faite entre les mandats en rapport avec l'application de la loi et ceux liés à la sécurité nationale. Bien que certains pays fassent une distinction entre les mandats selon que ceux-ci sont liés au crime (pour le mandat judiciaire) ou à la sécurité publique (pour le mandat exécutoire), l'approche globale qui établit un équilibre entre l'intérêt public et les droits de la personne consiste à exiger que toutes les autorisations soient données par un tribunal.

53. La mise en œuvre de l'obligation d'autoriser l'interception par le tribunal est importante pour maintenir l'équilibre entre les droits de la personne et l'intérêt de l'État. Il est essentiel pour préserver la confiance du public dans le système qu'une approbation indépendante des actes concernant un domaine aussi sensible que l'interception de communications existe. Cela ne serait pas forcément le cas si de hauts fonctionnaires étaient autorisés à approuver les demandes faites par une autre partie de l'administration. Le meilleur moyen d'assurer l'efficacité des contrôles et des équilibres est d'introduire un juge en tant qu'arbitre indépendant de la nécessité de l'interception. L'implication judiciaire au processus d'octroi de l'autorisation d'intercepter les communications garantit qu'un fonctionnaire habilité demandant un mandat examinera attentivement la question. Cela réduira également la possibilité d'abus de pouvoir.

54. Concernant le processus de demande, le Groupe de travail a modifié le paragraphe 6 (1). en ajoutant que la demande devait être faite *ex parte*. Cette modification est nécessaire pour permettre à un fonctionnaire habilité de demander le mandat d'interception en se fondant totalement sur les preuves qu'il décrit sans informer la personne dont les communications doivent être interceptées.

55. Le Groupe de travail a également eu une discussion importante sur l'éligibilité du fonctionnaire habilité à demander un mandat d'interception. De nombreuses approches nationales incluant un projet de loi régional (tel que le modèle de loi de l'OECO sur l'interception de communications) exigent que la demande soit soumise par le procureur général au nom du fonctionnaire habilité, afin de fournir un mécanisme supplémentaire de contrôle et d'équilibre. Cependant, les participants du Groupe de travail ont été d'avis que les pays, selon leurs traditions juridiques nationales, devaient avoir la possibilité de permettre à un fonctionnaire habilité de faire la demande sans avoir à se tourner vers le procureur général. Il a été convenu que chaque pays disposerait de cette option lors de la mise en œuvre de la législation relative à l'interception. Il appartient donc à chaque pays de décider si la demande doit être faite par un fonctionnaire habilité ou par le procureur général au nom du fonctionnaire habilité.

56. Le paragraphe (2) de l'Article 6 stipule qu'une demande de mandat d'interception doit être présentée sous forme écrite, accompagnée d'un affidavit précisant les circonstances dans lesquelles la demande est faite. L'objectif de ce paragraphe est d'établir les exigences relatives à la forme de la demande et de fournir un ensemble d'exigences auxquelles la demande doit satisfaire. Ces dispositions sont nécessaires pour garantir que le processus de demande d'autorisation suit certaines exigences et, dans la mesure où tous les documents doivent être fournis sous forme écrite, pour garantir la transparence du processus de la demande.

57. Selon le paragraphe (2) (a)-(i), les demandes doivent être faites par écrit et donner les raisons pour demander une autorisation d'interception. Cette disposition garantit que l'octroi du mandat d'interception repose sur une base factuelle. L'interception peut couvrir uniquement le suspect spécifique ou des contacts présumés. La demande écrite accompagnée d'un affidavit garantit qu'une interception «exploratoire» ou générale ne sera pas autorisée.

58. La forme des preuves accompagnant la demande (affidavit) a fait l'objet de discussions intenses. La plupart des approches nationales nécessitent l'autorisation préalable d'un tribunal pour pouvoir lancer l'interception de communications. Cependant, le processus de demande diffère d'un pays à l'autre. Bien qu'une majorité de pays conviennent que les demandes ont besoin d'être soumises sous forme écrite, les normes relatives aux preuves à l'appui varient de façon significative. Certains pays exigent que les preuves soient présentées sous forme d'une déclaration écrite sous serment (Canada, États-Unis, Australie, modèle de loi de l'OECO), tandis que d'autres adoptent l'approche d'une présentation des preuves de vive voix (par ex., le Danemark, la Finlande, la Slovénie).

59. Le paragraphe (2). de l'Article 6 est fondé sur la soumission des éléments de preuves à l'appui par écrit. Ce modèle a été choisi par le Groupe de travail, en premier lieu, parce qu'il était largement mis en application dans les pays où la *common law* est appliquée. En second lieu, les dispositions exigeant la soumission de déclarations écrites ont été mises en œuvre en raison de la différence possible en matière de réglementation des enregistrements et de la transcription des preuves de vive voix. L'obligation de soumettre les preuves à l'appui par écrit est une mesure nécessaire pour garantir la transparence de la demande et prévenir la possibilité de tout abus.

60. Afin de permettre à un tribunal de prendre une décision éclairée quant au bien-fondé d'une délivrance de mandat, les paragraphes (2) (a) à (2) (i) obligent un fonctionnaire habilité à fournir au tribunal les informations montrant la nécessité de l'interception pour l'objectif poursuivi. Pour garantir que l'interception n'est accordée que pour un cas particulier, la législation inclut l'obligation de présenter un affidavit détaillé, contenant tous les détails du cas, y compris les faits et autres motifs fondant la demande; la durée de validité du mandat demandée; le fondement permettant de penser que les preuves relatives au motif sur lequel la demande est faite seront obtenues au moyen de l'interception. En outre, l'exigence du paragraphe (2) (g). insiste sur la nécessité de fournir la justification selon laquelle l'interception est une mesure de «dernier recours». Ce paragraphe nécessite de fournir les détails des difficultés qui auraient surgi si l'enquête était limitée aux méthodes classiques ou les raisons expliquant pourquoi les méthodes classiques ont échoué.

61. Le paragraphe (3) stipule des exigences supplémentaires pour le cas où une demande est faite pour des raisons de sécurité nationale. Dans ce cas, elle doit être accompagnée d'une autorisation écrite signée par le [Ministre]. Cette disposition a pour objectif d'assurer que les détails du cas liés à la sécurité nationale sont fournis au tribunal.

62. Afin d'élaborer des mesures de protection de la confidentialité de la demande du mandat d'interception, les paragraphes (4) et (5) introduisent un ensemble de mesures visant à restreindre l'accès à la demande de mandat d'interception. Ils établissent les exigences de confidentialité de la demande et les procédures assurant la non-divulgation des informations de la demande. Ces mesures sont importantes, car le traitement des demandes et la gestion des dossiers par le tribunal peuvent donner lieu à des problèmes pour préserver la confidentialité des informations pendant le processus de demande si l'accès à la demande n'est pas limité à un certain nombre de fonctionnaires. Le tribunal doit s'assurer que tous les documents liés aux demandes de mandats sont conservés sous bonne garde. Il est essentiel que ces documents (y compris les mandats eux-mêmes) restent confidentiels. La notion même d'interception en tant qu'enquête clandestine pourrait être ébranlée si des informations concernant les demandes étaient divulguées.

63. Le Groupe de travail a décidé d'ajouter une disposition supplémentaire à l'Article 6 – paragraphe (6). en criminalisant les fausses déclarations faites sciemment par une personne dans une demande de mandat d'interception ou un affidavit. Cette disposition est une mesure de protection visant à empêcher tout abus découlant du processus de demande *ex parte* lorsque la décision du juge est

totalement fondée sur les preuves présentées par le demandeur. La personne dont les communications doivent être interceptées n'a pas la possibilité de mettre en cause les éléments de preuve à l'appui au moment de la demande. Par conséquent, le fonctionnaire habilité qui fait des déclarations sous serment doit faire l'objet de poursuites si de fausses preuves sont fournies sciemment.

Article 7. Divulgation de la demande

64. Pour protéger le secret de l'enquête et fournir une protection de la confidentialité de la demande, l'Article 7 criminalise la divulgation de l'existence de la demande de mandat d'interception. Cette criminalisation est nécessaire, car une violation délibérée de la sécurité de la demande pourrait conduire à un complot visant à miner l'enquête et à entraver l'administration de la justice.

65. Cependant, pour maintenir l'équilibre et protéger le droit de toute personne de demander un avis juridique, les paragraphes (2) et (3) exemptent de l'application de criminalisation la divulgation faite à un conseiller juridique.

Article 8. Délivrance du mandat d'interception

66. L'objectif du présent article est de fournir un cadre pour l'octroi d'une autorisation d'intercepter les communications après avoir demandé un mandat d'interception. La démarche consistant à restreindre le pouvoir d'intercepter à un nombre limité de circonstances, le présent article s'assure de la mise en place d'une protection solide et de la conviction du [juge] de la nécessité de procéder à l'interception.

67. En mesure de protection contre le pouvoir d'intercepter les communications, le paragraphe (1) établit un ensemble de circonstances qui doivent être analysées et confirmées par un [juge] avant la délivrance du mandat d'interception. Le premier ensemble d'exigences fourni par le paragraphe (1) (a) (i), (ii) et (iii) est lié à la nature de l'activité criminelle qui justifie l'autorisation d'intercepter. Un [juge] autorisant l'interception doit être convaincu que l'obtention de l'information est nécessaire à l'intérêt de la sécurité nationale ou à la prévention ou à la détection d'un crime grave particulier, y compris les cas d'assistance juridique mutuelle ou lorsque l'information obtenue grâce à l'interception est susceptible d'aider les enquêtes concernant un sujet ci-dessus.

68. Sécurité nationale –: le paragraphe (1) (a) (i) décrit un motif particulier de violation des droits de la personne à la confidentialité des communications. Ce motif justifiant l'autorisation d'intercepter peut soulever la question de l'équilibre des intérêts de l'État et du respect de la vie privée individuelle. Le droit de ne pas faire l'objet d'ingérences dans sa vie privée n'est pas absolu, dans la mesure où il doit être opposé à l'intérêt public concurrent. La limitation de ce droit est être nécessaire à l'exercice des intérêts concurrents, la sécurité nationale étant l'un d'eux. L'exigence d'une autorisation du tribunal peut assurer l'équilibre nécessaire et empêcher tout abus de l'interception pour des raisons de sécurité nationale.

69. L'expression «sécurité nationale» n'est pas définie pour les besoins du présent texte législatif, dans la mesure où celle-ci doit être conforme à la juridiction nationale de chaque pays. Il est important d'éviter une interprétation large de ce motif et de le limiter aux cas particuliers qui, bien entendu, dépendent de la mise en œuvre par l'État de ce modèle de texte législatif.

70. Le paragraphe (1) (a) (ii) fournit le second motif pour accorder un mandat d'interception: la prévention ou la détection d'une infraction précisée dans l'Annexe, lorsqu'il existe de bonnes raisons de croire que cette infraction a été, est, ou pourrait être commise. Ce paragraphe fait référence à l'Annexe introduite pour établir un ensemble de crimes graves particuliers justifiant une interception. Le principe directeur de l'application de cette disposition est que les moyens

d'enquête doivent être proportionnés à la gravité des faits faisant l'objet d'une enquête. L'interception de communications sans le consentement des parties constituant une ingérence grave dans la vie privée, ce type de mesure ne peut se justifier que si l'infraction faisant l'objet d'une enquête est d'une nature grave.

71. Le paragraphe (1) (a) (iii) est essentiel pour traiter de la question de l'entraide judiciaire lors des enquêtes sur les crimes graves. Cette disposition est essentielle, car les nouveaux moyens de communication peuvent entraîner des transmissions de données transnationales, ce qui rend la coopération internationale importante. Le pays doit être capable de répondre aux demandes d'entraide judiciaire nécessitant l'interception de communications.

72. La disposition du paragraphe (1) (b) est essentielle pour garantir que l'interception est uniquement autorisée pour l'enquête dans un cas particulier. Il est nécessaire de prévoir qu'un juge pourrait n'autoriser l'interception que pour un crime spécifique, une question de sécurité nationale ou une demande d'entraide judiciaire et uniquement si l'interception étaye l'enquête. Des motifs de suspicion doivent exister et l'interception ne doit pas être autorisée si elle repose uniquement sur la possibilité de découvrir un crime.

73. La délivrance du mandat d'interception est en outre limitée en vertu du paragraphe (1) (c) aux cas où d'autres procédures pour obtenir les informations n'ont pas réussi, ont peu de chances de réussir, sont trop dangereuses pour être appliquées aux circonstances existantes, ou sont irréalisables en raison de l'urgence du cas. Cette disposition est nécessaire afin de s'assurer que les interceptions ne sont pas autorisées, sauf si l'information n'est pas raisonnablement disponible par des méthodes moins invasives. L'autorisation doit être justifiée, non pas au motif de la simplicité relative du déploiement des techniques d'interception, mais en raison du caractère raisonnable de sa mise en œuvre. Cette justification assure l'équilibre entre l'efficacité et l'intérêt public concurrent en fournissant une protection pour la confidentialité des communications. Elle garantit le recours à des moyens d'enquête proportionnés à l'immédiateté et à la gravité du crime.

74. Le paragraphe (1) (d) prévoit la délivrance d'un mandat d'interception uniquement s'il peut servir au mieux l'administration de la justice. Il oblige le juge à tenir compte de ces intérêts pour accorder son autorisation. Il s'agit là d'une protection supplémentaire visant à imposer des contrôles plus rigoureux si l'organisme chargé de l'application de la loi souhaite uniquement collecter des renseignements.

75. En guise de mesure de protection supplémentaire visant à s'assurer que chaque demande fait l'objet d'une décision au cas par cas, le paragraphe (2) permet au juge de demander des informations supplémentaires en rapport avec la demande.

Article 9. Portée et forme du mandat d'interception

76. L'article 9 énonce des règles sur la portée et la forme du mandat d'interception. Pour s'assurer que l'ingérence dans la vie privée est limitée au minimum, il est nécessaire d'établir l'exigence formelle de l'autorisation et de ne la permettre que si elle est conduite par une personne particulière et uniquement pour une certaine adresse/personne/communication. Un ensemble d'exigences relatives à la portée et à la forme du mandat d'interception vise à fournir un certain cadre formel pour chaque cas d'interception, à limiter le pouvoir d'interception et à réduire l'impact de l'interception sur les tiers.

77. Aucune interception ne pouvant avoir lieu sans mandat d'interception, celui-ci doit être précis quant à ce que la personne chargée de l'exécution de l'interception peut faire. En outre, pour préserver la vie privée, le juge doit avoir le pouvoir d'imposer les conditions qu'il considère comme appropriées.

78. Conformément au paragraphe (1), un mandat d'interception est délivré sous la forme prescrite (par écrit). La forme écrite est essentielle pour équilibrer deux composantes importantes: en premier lieu, pour garantir le droit d'intercepter et de demander assistance et, en second lieu, pour limiter

ce droit à une personne/adresse/communication particulière. Par conséquent, la forme écrite du mandat d'interception compense la nécessité d'effectuer une intrusion particulière avec la nécessité d'éliminer la perspective d'éventuels abus. Il est très important qu'un mandat d'interception soit aussi précis que possible. Les paragraphes (1) (a), (b), (c) et (d) énoncent la portée de l'autorisation concernant l'autorité de la personne qui l'exécute.

79. Le paragraphe (2) sert de mesure visant à équilibrer l'autorité accordée en vertu du paragraphe (1). Afin de strictement limiter l'autorisation à une certaine personne et de prévenir tout type d'abus, le paragraphe (2) requiert que le mandat nomme ou décrive la personne ou l'ensemble de locaux qui doivent être interceptés. Pour se conformer à cette disposition, le mandat d'interception identifie les communications qui doivent être interceptées en provenance ou à destination d'une personne particulière désignée dans le mandat d'interception ou d'une adresse particulière indiquée dans le mandat d'interception. Cette disposition est nécessaire pour garantir que l'interception est uniquement autorisée afin d'enquêter sur un crime particulier et non en tant que mesure de surveillance générale.

80. Le Groupe de travail a eu une discussion concernant l'identification de l'ensemble de locaux ou de dispositifs de communication à partir desquels/vers lesquels la communication est transmise. Le Groupe de travail a convenu que le terme «adresse» devait être utilisé afin d'identifier un ensemble particulier de locaux, un numéro de téléphone ou une adresse électronique pour l'interception. Suite à cette discussion, le Groupe de travail a convenu que la définition d'«adresse» devait être la suivante: Article 9 «adresse» comprend les locaux, l'adresse électronique, le numéro de téléphone, ou les éventuels numéros ou désignation utilisés pour identifier les réseaux, les prestataires ou les appareils de communication.

81. Le paragraphe (3) prévoit la possibilité d'inclure une clause d'intrusion dans le mandat d'interception. L'exécution du mandat d'interception peut nécessiter de pénétrer dans des locaux privés. En l'absence d'un pouvoir pour pénétrer dans les locaux, un fonctionnaire habilité serait tenu de demander un mandat distinct conformément à la législation nationale existante l'autorisant à pénétrer dans les locaux ciblés. Cependant, dans la mesure où une interception ne peut être accordée qu'à des fins d'enquête sur des crimes graves, une demande distincte n'est pas souhaitable en raison des retards que cela entraînerait dans l'exécution du mandat d'interception.

82. Pour protéger le droit à la vie privée, la clause autorisant l'intrusion dans les locaux a pour unique objet de procéder à l'interception et rien d'autre. La disposition du paragraphe (3) permet de donner l'autorisation de pénétrer dans tous les locaux indiqués dans le mandat afin d'installer, d'entretenir, d'utiliser ou de récupérer tout équipement utilisé pour intercepter les communications indiquées dans le mandat. Pour garantir l'élimination de toute perspective d'abus, ce paragraphe exige que tous les locaux soient précisément indiqués dans la clause d'intrusion, et un fonctionnaire habilité ne peut y pénétrer que pour l'objectif particulier précisé.

83. Le paragraphe (4) requiert l'identification du fonctionnaire habilité au nom duquel la demande est faite, la personne qui exécutera le mandat d'interception et le prestataire de communication auquel le mandat d'interception doit être adressé. Cette disposition constitue une protection importante pour limiter le nombre de personnes habilitées à exécuter l'interception. En outre, elle satisfait au principe général selon lequel les mandats doivent être aussi précis que possible pour prévenir toute possibilité d'abus.

84. Le modèle de texte législatif permet aux pays de sélectionner une personne effectivement chargée d'exécuter l'interception. Pour les pays aux capacités d'application de la loi limitées, et pour les cas où la police ne dispose pas de ressources suffisantes, une option permet de décider d'obliger le prestataire de communication à intercepter les communications. Cependant, la construction du paragraphe (4) permet au juge de désigner la personne chargée d'exécuter l'interception dans chaque cas particulier.

85. En outre, un mandat d'interception contenant une disposition d'entrée doit préciser l'heure à laquelle l'entrée est autorisée et les éventuelles mesures supplémentaires à prendre pour réaliser la mesure.

86. Le mandat d'interception étant exclusivement délivré sur la base de motifs particuliers, spécifiques pour chaque cas, le [juge] dispose du pouvoir d'imposer des conditions supplémentaires qui refléteront la nature de chaque cas particulier. Les paragraphes (5) et (6) sont mis en œuvre pour permettre au [juge] de définir des dispositions, conditions ou restrictions accessoires liées à l'interception de communications autorisées dans le mandat.

Article 10. Durée et renouvellement du mandat d'interception

87. L'Article 10 est en rapport avec la durée et le renouvellement d'un mandat d'interception. Le principal objectif de cet Article est de limiter l'autorisation d'intercepter les communications à un certain laps de temps afin d'éviter les interceptions illimitées.

88. En outre, cet Article énonce une réglementation pour le renouvellement du mandat d'interception lorsque la période de validité établie par le présent modèle de texte législatif et/ou précisée dans le mandat d'interception s'avère trop courte pour atteindre l'objectif de l'interception. Cette dernière option est vitale s'il est nécessaire de poursuivre l'interception sans l'interruption que provoque une nouvelle demande.

89. La limitation de la durée du mandat d'interception à un certain laps de temps (relativement court) est une approche commune dans la majeure partie des pays. Cependant, le délai établi varie de façon significative, par ex.: 3 ou 6 mois (Australie), 6 mois (modèle de loi de l'OECO), 3 mois (Hong Kong).

90. La durée nécessaire de l'interception a fait l'objet de discussions intenses et divers aspects ont été étudiés. D'une part, il est nécessaire qu'elle tienne compte du fait que l'interception est une mesure sévère à laquelle on ne doit pas recourir sauf si c'est absolument essentiel. Par conséquent, la durée du mandat doit être limitée. En outre, plus la durée d'un mandat est longue, plus il est probable que des informations à caractère personnel, non pertinentes pour une enquête, soient interceptées. Ce facteur doit également être pris en compte lors de l'établissement de la période de validité.

91. D'autre part, les enquêtes sur les crimes graves peuvent prendre du temps. Si la durée maximale est trop courte, cela pourrait générer un grand nombre de demandes de renouvellement et bloquer les ressources.

92. Le paragraphe (1) stipule que la période de validité d'un mandat d'interception ne doit pas être supérieure à [90] jours. La durée suggérée (90 jours) est un délai moyen tiré des diverses approches nationales. Chaque pays peut décider de changer cette durée lors de la mise en œuvre. La période de validité doit être précisée par un juge. Ce paragraphe traite également de la demande de renouvellement d'un mandat existant.

93. L'autorisation d'interception étant soumise à un processus de demande *ex parte*, il est nécessaire de fournir les mêmes protections pour le renouvellement du mandat d'interception que celles mises en œuvre pour les demandes initiales. Par conséquent, la forme et le contenu de la demande doivent être les mêmes. Un renouvellement de mandat peut être accordé par un juge d'après une demande faite par le procureur général au nom d'un fonctionnaire habilité à tout moment avant l'expiration du mandat (ou de tout renouvellement en cours du mandat). Chaque pays pourra, en fonction de sa législation nationale, autoriser un fonctionnaire habilité à demander un renouvellement sans la participation du procureur général.

94. Le Groupe de travail a eu une discussion pour savoir si le renouvellement devait passer par la même procédure et se présenter sous la même forme que la demande initiale. Il a finalement décidé que les procédures de renouvellement devaient être aussi proches que possible des procédures de demande initiale de façon à conserver toutes les protections et à prévenir le risque

d'abuser du pouvoir d'interception. La demande de renouvellement doit justifier les circonstances du renouvellement, donner les raisons justifiant la période de renouvellement et préciser ce qui a été fait pour exécuter le mandat existant. Voilà pourquoi les paragraphes (3) et (4) établissent les mêmes exigences pour la demande de renouvellement que pour la demande initiale. En outre, pour fournir tous les détails du cas, la demande doit contenir des informations sur l'exécution du mandat d'interception en cours. Ces informations sont nécessaires pour garantir que l'interception est raisonnable et concentrée sur un crime particulier. Pour permettre un examen régulier de chaque demande de renouvellement, le paragraphe (5) fournit au juge le pouvoir de requérir des informations supplémentaires pour traiter la demande.

95. Le paragraphe (6) fournit une protection liée aux motifs d'une interception: un juge ne peut renouveler un mandat d'interception que s'il est convaincu que les circonstances qui ont motivé l'autorisation d'interception s'appliquent toujours.

96. Selon le paragraphe (7) la durée de chaque renouvellement de mandat d'interception ne peut être supérieure au délai général de validité (comme le suggère le texte législatif, [90] jours) et doit être précisée par un juge dans le renouvellement. Chaque pays peut préciser un autre terme de l'interception renouvelée.

97. Dans la mesure où l'interception représente une sérieuse intrusion dans la vie privée, il est très important de s'assurer qu'il y sera mis un terme dès que la nécessité d'intercepter n'existera plus. Pour garantir ce principe, le paragraphe (8) exige du fonctionnaire habilité auquel le mandat est délivré ou d'une personne agissant en son nom, qu'il demande la révocation du mandat d'interception s'il apparaît qu'un mandat d'interception n'est plus nécessaire.

Article 11: Modification du mandat d'interception

98. L'Article 11 permet à un fonctionnaire habilité de demander la modification d'un mandat d'interception existant si les circonstances ont changé. Cette modification peut être applicable aux cas où l'adresse des locaux du suspect, les numéros de téléphone, ou tout autre critère d'identification précisé dans le mandat d'interception, changent. Le processus de demande reste le même afin de s'assurer que toutes les mesures de protection sont applicables. Une demande de modification d'un mandat d'interception existant doit être effectuée par le procureur général au nom d'un fonctionnaire habilité ou par un fonctionnaire habilité, en fonction de l'approche choisie par le pays concerné pour la procédure de la demande initiale. Les motifs d'exécution de l'interception restent les mêmes.

Article 12. Révocation du mandat d'interception

99. Cet article est mis en œuvre afin de s'assurer que le mandat d'interception est révoqué en cas d'abus du droit d'intercepter ou si l'interception n'est plus nécessaire. Il s'agit là d'un mécanisme essentiel visant à garantir que l'interception respecte totalement les exigences du modèle de texte législatif. En outre, il doit s'assurer que l'ingérence est uniquement utilisée en tant que mesure exceptionnelle. L'Article fournit les motifs et la procédure pour une révocation de l'autorisation d'interception. Le Groupe de travail a modifié le terme suggéré de «résiliation» en «révocation».

100. D'après le paragraphe (1), le mandat d'interception peut être révoqué par un juge si un fonctionnaire habilité ne soumet pas un rapport sur les progrès conformément à l'Article 15; si le juge, dès réception de ce rapport sur les progrès, est convaincu que les objectifs du mandat d'interception ont été atteints; que les motifs sur lesquels le mandat d'interception a été délivré ont expiré; ou que les conditions de la demande initiale ont changé de telle sorte qu'une demande ne serait plus possible.

101. Pour établir les exigences formelles en rapport avec la révocation et s'assurer qu'un fonctionnaire habilité est immédiatement informé de la révocation, le paragraphe (2) stipule que la notification de révocation du mandat doit être transmise sous forme écrite au fonctionnaire habilité.

102. L'objectif du paragraphe (3) est de garantir que la révocation d'un mandat d'interception en arrête immédiatement l'exécution. Il exige qu'un fonctionnaire habilité retire tout dispositif intercepté ayant été installé pour effectuer l'interception. La désinstallation doit avoir lieu dès que possible après réception de l'information à propos de la révocation.

Article 13. Conséquences de la révocation

103. Cet article fournit une mesure de protection dans le cas d'une révocation du mandat d'interception. Dans la mesure où le mandat d'interception est révoqué, si les exigences d'une interception, établies par le texte législatif, ne sont plus satisfaites, il convient de s'assurer que les données interceptées ne sont pas utilisées dans une procédure pénale. L'Article 13 déclare irrecevables les preuves collectées alors qu'un mandat était révoqué, sauf si la cour décide que l'admission de ces preuves ne rendrait pas le procès inéquitable.

Article 14. Demande urgente

104. L'Article 14 est essentiel pour les cas urgents qui nécessitent l'exécution d'une interception dès que possible, tout délai risquant de nuire à l'enquête. Il énonce les fondements et la procédure à suivre pour ces demandes urgentes.

105. Dans ces cas, les demandes verbales sont autorisées. Il est hautement improbable qu'un fonctionnaire habilité ait, dans les cas urgents, le temps de rédiger et de soumettre une demande écrite au tribunal. Le Groupe de travail a par conséquent décidé qu'un mécanisme d'urgence, permettant à un fonctionnaire habilité d'obtenir un mandat dans ces circonstances, devait être mis en place.

106. Presque toutes les approches nationales permettent, dans certains cas, les autorisations d'interception urgentes. Les procédures ont été rédigées en se fondant sur le modèle de loi de l'OECO et sur la législation néo-zélandaise.

107. Selon le paragraphe (1) un juge peut, dans une situation urgente, déroger aux exigences de demande écrite et permettre au procureur général au nom d'un fonctionnaire habilité de faire une demande verbale de mandat d'interception. Le juge délivre le mandat s'il est convaincu que les circonstances justifient l'octroi d'un mandat d'interception en vertu de l'Article 8.

108. Afin de garantir la procédure formelle de la demande, le paragraphe (2) établit les exigences auxquelles doit répondre toute demande de mandat d'urgence. En premier lieu, celle-ci doit contenir les informations mentionnées au paragraphe (2) de l'Article 6 qui sont requises pour la demande d'un mandat d'interception; en second lieu, la demande doit indiquer les détails de l'urgence du cas ou les autres circonstances exceptionnelles qui, de l'avis du fonctionnaire habilité, justifie une demande verbale. Une demande verbale doit également respecter toute autre directive susceptible d'être délivrée par le [juge].

109. Conformément au paragraphe (3) un juge délivre un mandat d'interception d'urgence uniquement s'il est convaincu qu'il existe de bonnes raisons de croire que le mandat d'interception doit être délivré et qu'il n'est pas raisonnablement possible de faire une demande sous forme écrite. Cette disposition vise à s'assurer qu'un mandat urgent ne peut être accordé que dans des circonstances exceptionnelles.

110. Le Groupe de travail a eu une discussion sur l'opportunité d'appliquer les règles de la demande urgente à la procédure de renouvellement du mandat d'interception existant. La principale préoccupation était de savoir comment les contrôles et équilibres appropriés offerts par les clauses relatives à la demande urgente pouvaient s'appliquer dans ce cas. Le Groupe de travail a convenu de ne pas autoriser les demandes verbales pour les cas normaux de renouvellement.

111. Afin de s'assurer que des enregistrements sont conservés pour chaque demande de mandat, le paragraphe (4) requiert du juge qu'il conserve une note écrite des détails de la demande si un mandat d'urgence est délivré.

112. Le paragraphe (5) stipule qu'un mandat d'interception délivré sur la base d'une demande verbale doit avoir la même portée que les mandats d'interception standard. Cette disposition vise à éviter différents standards pour les demandes urgentes et les procédures normales. Le Groupe de travail a discuté du fait de savoir si le mandat urgent devait être délivré par écrit ou verbalement. Il a été convenu que le mandat d'interception délivré sur demande verbale devait se présenter sous la forme écrite requise par l'Article 9.

113. La période de validité pour chaque mandat d'interception d'urgence est fournie par le paragraphe (6) et doit être de [48] heures à partir de l'heure à laquelle il est délivré. Chaque pays peut choisir de prévoir une autre période de validité pour le mandat d'interception urgent. Après cette période, le mandat expire. Conformément au paragraphe (7) une demande écrite et un affidavit doivent être soumis, conformément aux dispositions de l'Article 6, dans les [48] heures. Cette disposition a pour objet de s'assurer que chaque demande de mandat d'interception est transparente et faite, en fin de compte, sous forme écrite. En outre, elle vise à donner au juge la possibilité de réexaminer la décision urgente lorsque les preuves pour accorder l'autorisation d'interception ne sont pas suffisantes.

114. La procédure (demande écrite) à suivre après la délivrance d'un mandat d'interception urgent a fait l'objet d'une discussion au sein du Groupe de travail. Certains participants de l'atelier de consultation s'inquiétaient de la nécessité de procédures administratives dans un délai si court. Cependant, le Groupe de travail a convenu de la nécessité d'exiger une demande écrite afin d'éliminer toute perspective d'abus. Dans la mesure où le délai de 48 heures n'est que la durée recommandée pour les mandats urgents, chaque pays peut choisir de donner une période de validité plus longue aux mandats délivrés dans l'urgence.

115. Le paragraphe (8) établit une procédure de réexamen de la décision d'accorder un mandat urgent. Cette procédure est nécessaire pour garantir que la dérogation par rapport à la procédure de demande formelle est justifiée. Dans le cas contraire, le mandat est révoqué.

Article 15: Rapport sur les progrès

116. Le rapport sur les progrès est une mesure nécessaire pour contrôler l'exécution du mandat d'interception. Il permet au juge qui a délivré le mandat d'être sûr que l'interception se déroule conformément à la loi et à l'autorisation légale. Cette approche est, par exemple, utilisée dans le modèle de loi de l'OECO sur l'interception de communications. L'Article 15 donne au juge qui a délivré un mandat d'interception, le pouvoir d'ordonner au fonctionnaire habilité au nom duquel la demande concernée a été faite, d'établir un rapport par écrit sur les progrès réalisés ou sur tout autre sujet que le juge considère nécessaire. Cet ordre est contraignant et peut entraîner la révocation du mandat d'interception telle que définie par l'Article 12. La demande en vertu de l'Article 15 peut être faite par le juge au moment de la délivrance du mandat d'interception, ou à tout autre stade avant la date d'expiration.

117. L'obligation de rapport sur les progrès vise également à équilibrer les systèmes de contrôle administratif et judiciaire.

Article 16: Rapport final

118. Cet article est une option que chaque pays peut choisir de mettre en œuvre en tant que mesure de protection supplémentaire. L'exigence d'un rapport final sur les résultats de l'interception est mise en œuvre dans certains pays tels que l'Australie et la Nouvelle-Zélande. Il demande au fonctionnaire habilité de soumettre un rapport final sur les détails de l'interception, y compris les résultats qui ont été obtenus. À cet égard, le rapport final sert également d'instrument supplémentaire afin de garantir le respect des règles de confidentialité des communications interceptées prévues par l'Article 23.

119. Le paragraphe (2) établit un ensemble d'exigences liées à la forme et au contenu du rapport final. Il convient de noter l'attention particulière accordée à la destruction des informations non pertinentes en tant que mesure de protection.

120. Cependant, certains pays risquent d'éprouver des difficultés à mettre en œuvre cette disposition, l'obligation s'accompagnant de tâches administratives supplémentaires et de possibles préoccupations sur le respect de la vie privée. Après une discussion intense, le Groupe de travail a décidé que chaque pays devait décider s'il souhaitait demander un rapport final.

TITRE III – EXÉCUTION D'UNE INTERCEPTION

121. Le Titre III établit les devoirs et les responsabilités des organismes publics (fonctionnaire habilité) et des personnes pour l'exécution de l'interception. Cet article fournit un cadre essentiel pour le processus d'exécution de l'interception. Il inclut des réglementations liées à l'obligation de fournir une assistance. Il contient également des dispositions traitant de la confidentialité des informations interceptées et de l'obligation de détruire les enregistrements de l'interception. Des réglementations et mesures de protection strictes sont fournies pour veiller à ce que les informations restent confidentielles et les données non pertinentes soient détruites.

Article 17: Exécution d'un mandat d'interception

122. L'Article 16 vise à permettre à un fonctionnaire habilité d'intercepter les communications précisées dans le mandat et conformément à ses termes. En outre, il accorde au fonctionnaire habilité le pouvoir d'exiger d'une personne désignée dans le mandat qu'elle intercepte des communications ou qu'elle l'aide dans l'exécution de l'interception. Ce devoir d'assistance est crucial dans la mesure où les organismes chargés de l'application de la loi dépendent très souvent du soutien de la personne qui possède des connaissances spécifiques sur les réseaux de communication ou qui les fait fonctionner. Cependant, l'obligation d'assistance est limitée au champ d'application de l'autorisation et aux devoirs précisés dans le mandat d'interception. Cette disposition est essentielle pour veiller à ce qu'aucune demande déraisonnable ne soit faite en ce qui concerne la personne qui doit prêter assistance. Elle fournit le droit de refuser une demande d'assistance non conforme au mandat d'interception.

123. Le paragraphe (3) est nécessaire, car l'interception interfère souvent avec la vie privée, et pas uniquement celle de la personne dont les communications sont soumises à l'interception. Le droit des tiers à des communications privées est également souvent affecté par le mandat d'interception. Afin de limiter l'intrusion des intérêts légitimes de tiers, ce paragraphe oblige le fonctionnaire habilité ou la personne qui intercepte ou favorise l'interception de communications à prendre toutes les mesures raisonnables pour minimiser l'impact de l'interception sur les tiers.

124. Le Groupe de travail a décidé d'ajouter une disposition supplémentaire à l'Article 17: le paragraphe (4) dispose qu'un fonctionnaire habilité ou une personne agissant en vertu d'un mandat ne voient pas leur responsabilité pénale ou civile engagée s'ils agissent conformément au mandat d'interception. La même disposition s'applique à quiconque aide de bonne foi une personne dont il a de bonnes raisons de croire qu'elle agit conformément à une autorisation d'interception. Cette disposition est introduite pour protéger la personne qui exécute légalement l'interception.

Article 18: Intrusion dans un local pour l'exécution du mandat d'interception

125. L'Article 18 fournit le cadre pour l'exécution de la clause d'entrée prévue dans le mandat d'interception, le cas échéant. La demande d'un mandat d'interception contenant une disposition permettant au fonctionnaire habilité de pénétrer dans des locaux doit être effectuée conformément à l'Article 18, qui permet à un fonctionnaire habilité de pénétrer dans des locaux à l'heure précisée dans le mandat d'interception et d'effectuer tout acte en rapport avec l'objet du mandat d'interception.

Article 19: Devoir d'assistance

126. Cet article prévoit une mesure coercitive pour faciliter l'interception de communications. Il oblige une personne qui fournit des services de communication, à permettre à un fonctionnaire habilité d'exercer un mandat d'interception et à l'aider si cela s'avère nécessaire et raisonnable. Pour empêcher tout abus du pouvoir de demander assistance, le paragraphe (2) stipule que le devoir d'une personne d'intercepter des communications doit être précisé par le juge dans le mandat d'interception. Cette disposition est essentielle pour éliminer toute perspective d'abus, en particulier en raison de l'Article 20, qui fait du défaut d'assistance une infraction.

Article 20: Défaut d'assistance

127. Conformément à l'article 20, toute personne tenue de fournir assistance à un fonctionnaire habilité en vertu d'un mandat d'interception qui refuse de le faire commet une infraction. La criminalisation du refus de fournir une assistance est nécessaire, car le mandat d'interception est accordé dans des circonstances exceptionnelles afin d'enquêter sur des crimes graves et le succès de l'exécution du mandat repose souvent sur l'assistance des opérateurs de communication. Lorsqu'une demande d'assistance est refusée, cela peut saper l'enquête et entraver l'administration de la justice en général.

Article 21: Confidentialité de la communication interceptée

128. Les préoccupations relatives au respect de la vie privée et la nécessité de préserver le secret de l'interception justifient l'exigence de confidentialité et l'obligation de détruire les données non pertinentes. Il est également nécessaire de protéger autant que possible la vie privée des tiers dont les communications sont interceptées sans leur consentement. Pour répondre à ce besoin de confidentialité, les lois de nombreux pays, tels que l'Australie, le Canada, la Nouvelle-Zélande et l'Afrique du Sud, contiennent toutes des dispositions interdisant l'usage ou la divulgation non autorisés des matériaux interceptés.

129. Adoptant cette approche, le paragraphe (1) de l'Article 21 fixe des mesures de protection strictes sur la mesure dans laquelle les matériaux interceptés peuvent être divulgués, copiés et conservés, en requérant que chacun de ces actes soit limité au strict minimum et en obligeant le fonctionnaire habilité à prendre un ensemble de dispositions nécessaires pour garantir la confidentialité de l'interception. Fournissant de solides mesures de protection pour le processus d'exécution du mandat d'interception en ce qui concerne la confidentialité de l'information, le paragraphe (2) précise les informations particulières de l'interception de communications et de l'exécution du mandat d'interception qui doivent rester confidentielles.

Article 22: Infraction à la confidentialité des informations sur l'interception

130. L'Article 22 renforce la protection de la confidentialité des communications interceptées en établissant une infraction de toute divulgation, intentionnellement et sans excuse ou justification légitime, de tout élément qu'une personne est tenue de conserver confidentielle conformément aux dispositions de l'Article 21.

Article 23: Destruction des enregistrements

131. Cette disposition réglemente la suppression des enregistrements. Elle est essentielle, car toutes les données glanées grâce à l'interception ne sont pas pertinentes. Dans la mesure où l'interception de communications dure en principe plusieurs semaines, voire plusieurs mois, il est très probable que des informations à caractère personnel, non pertinentes pour l'enquête soient obtenues. La plupart des informations obtenues en conséquence de l'interception sont liées à des tiers qui ont des contacts avec les personnes ciblées par l'interception. La possibilité de conserver ces données se traduirait certainement par une intrusion dans la vie privée, tant de tiers que de la cible de l'interception. Du point de vue du respect de la vie privée, la personne dont les droits ont été lésés par une interception doit être informée de cette violation. Ce qui comporte le problème du sujet, du moment et des circonstances d'une telle notification. Tous ces problèmes pourraient être évités si la vie privée de la personne lésée par une interception pouvait être protégée par la destruction du matériel intercepté.

132. Pour protéger la vie privée, l'Article 23 contient l'obligation de détruire immédiatement tout enregistrement sans rapport avec l'objet du mandat d'interception. En outre, le paragraphe (2) requiert la destruction de tout enregistrement dès qu'il apparaît qu'aucune poursuite, ou qu'aucune autre poursuite, ne sera engagée dans laquelle ces informations sont susceptibles de devoir être données comme preuves. Le paragraphe (2) doit s'appliquer avec les exclusions établies dans le paragraphe (3), qui énonce que l'obligation de destruction ne doit pas s'appliquer à un quelconque enregistrement d'information présentée dans une procédure devant un tribunal.

133. Afin de contrôler l'exigence de préservation de la confidentialité des communications interceptées et de détruire les informations non pertinentes, le paragraphe (4) oblige une personne autorisée à fournir les informations conformément au paragraphe (2) à un [juge] dans le rapport final sur l'exécution du mandat d'interception. Cette disposition est uniquement pertinente pour les pays qui décident d'inclure l'obligation liée au rapport final dans leur législation relative à l'interception (voir la note explicative de l'Article 16: Rapport final).

Article 24:

134. **La non-destruction des enregistrements** criminalise le non-respect des exigences de destruction des enregistrements. L'objectif de cette disposition est de mettre en œuvre des mesures de protection solides afin de préserver la confidentialité des communications et de veiller à ce que toutes les informations non pertinentes aux fins de l'interception soient détruites.

TITRE IV – ÉQUIPEMENTS D'INTERCEPTION

135. Il est essentiel de réglementer les équipements d'interception, dans la mesure où l'utilisation de dispositifs électroniques pour intercepter les communications constitue la menace à première vue du droit à des communications privées. La nécessité d'interdire l'utilisation d'un équipement doté de capacités d'interception a été largement acceptée dans le Groupe de travail. Cependant, il n'existe pas de réponse exacte quant au mécanisme le plus efficace pour l'interdiction et la surveillance de l'utilisation d'équipements d'interception. Deux options possibles ont fait l'objet de discussions par le Groupe de travail. La première option consiste à interdire la possession, la vente et l'acquisition de dispositifs principalement conçus pour intercepter les communications et à établir un nombre limité de dérogations pour les organismes chargés de l'application de la loi, le gouvernement et les opérateurs de communication. Cependant, cette approche soulève le problème des dispositifs «à double emploi» sans le résoudre. En outre, pendant la discussion, il a été noté que la portée d'une telle interdiction est incertaine.

136. La seconde approche consiste à répertorier l'équipement doté de capacités d'interception afin de préciser l'étendue de la restriction. Cette approche suit le modèle de l'Afrique du Sud et du modèle de loi de l'OECO sur l'interception de communications. Cependant, le principal argument contre ce cadre a été la mise en œuvre pratique de cette disposition et la faisabilité de la création et de l'entretien de la liste.

137. Si le Groupe de travail s'est mis d'accord sur la limitation du commerce et de l'utilisation des équipements d'interception, l'approche appropriée concernant la mise en œuvre a donné lieu à un débat intense. Le Groupe de travail a discuté des deux options susmentionnées, mais aucun consensus n'a été atteint sur cette question. Par conséquent, les dispositions du Titre IV doivent être considérées comme une recommandation pour les pays qui décident d'adopter cette approche et de créer et d'entretenir une liste de l'équipement doté de capacités d'interception.

138. Le modèle de texte législatif suggère de créer une approche fondée sur une liste. L'objectif de cette approche est d'interdire certains actes et d'établir un contrôle sur la fabrication et la possession illégales d'équipements d'interception. En outre, il cherche à réglementer le processus d'autorisation pour ce type d'équipement. Il vise également à protéger toutes les parties intéressées en requérant un processus de consultations avant que l'utilisation d'un équipement particulier soit restreinte ou interdite.

Article 25: Équipement recensé doté de capacités d'interception

139. Pour engager l'approche consistant à répertorier l'équipement doté de capacités d'interception, l'Article 25 stipule que le ministre peut, par avis publié au Journal officiel, déclarer tout équipement ou dispositif électronique, électromagnétique, acoustique, mécanique ou autre, principalement utilisé à des fins d'interception de communications, dans les circonstances précisées dans l'avis, comme étant un équipement recensé. Le processus de publication d'un tel avis est établi par les paragraphes (2) à (7). L'Article (4) fournit une mesure de protection pour toutes les parties intéressées en obligeant le ministère à les inviter à soumettre leurs commentaires écrits sur la proposition. Cette disposition garantit la transparence de la procédure et la participation de toutes les parties intéressées. Elle vise également à protéger le développement de la technologie.

Article 26. Interdiction de fabrication, de possession et d'utilisation d'équipement recensé doté de capacités d'interception

Article 27. Autorisation d'utiliser un équipement recensé doté de capacités d'interception

140. Pour définir les restrictions relatives à l'équipement contenu dans la liste, l'Article 26 interdit la fabrication, la possession et l'utilisation de l'équipement recensé doté de capacités d'interception sauf pour les personnes autorisées. L'autorisation peut être donnée en vertu de l'Article 27 qui dote un ministère du pouvoir d'accorder une dérogation si celle-ci est dans l'intérêt public ou dans les cas où la fin pour laquelle l'équipement recensé sera fabriqué, assemblé, possédé, vendu, acheté, ou médiatisé est raisonnablement nécessaire, ou lorsque des circonstances spéciales justifient cette dérogation. L'Article 27 établit également les exigences relatives à la forme et à la durée du certificat d'exemption.

Article 28. Infraction

141. Afin de limiter la fabrication et la possession de l'équipement doté de capacités d'interception, l'Article 28 criminalise certains agissements liés aux dispositifs recensés.

Partie III

TITRE V – DIVULGATION DE DONNÉES DE COMMUNICATION STOCKÉES

142. Le Titre V a été élaboré pour fournir aux pays la possibilité de divulguer les données de communications stockées dont la transmission est terminée qui, par définition, ne sont donc plus considérées comme susceptibles d'interception.

143. Ce titre a été construit de façon à protéger la confidentialité des données des communications stockées. Il a été inclus, car, dans un certain nombre de cas, il peut être nécessaire d'obtenir des informations stockées, telles que des données de localisation lorsque les communications ne peuvent pas être interceptées, celles-ci ayant déjà été acheminées par le processus de transmission. Le Groupe de travail a donc convenu que la non-inclusion de cet instrument dans le modèle de texte législatif pouvait forcer les pays à introduire cet instrument nécessaire dans une seconde approche. Le modèle de loi de l'OECO sur l'interception de communications, ainsi que la législation en Australie et au Royaume-Uni suivent la même approche et combinent une législation sur l'interception et une législation liée à la divulgation de données de communications stockées.

144. Le Groupe de travail a eu une discussion intense à ce sujet. Si ces dispositions sont jugées utiles à l'application de la loi dans certains pays, il est communément admis qu'elles sortent du champ d'application du modèle de texte législatif et que, de ce fait, il convient de mentionner clairement que la mise en œuvre de cette partie par les États bénéficiaires est facultative.

145. Par conséquent, les dispositions suivantes doivent être considérées comme facultatives et sont davantage des recommandations destinées aux pays qui décideraient d'adopter cette approche.

146. Le Titre V du modèle de texte législatif interdit l'accès aux données des communications stockées et établit un ensemble limité de conditions dans lesquelles une ordonnance de divulgation peut être délivrée. La nature de l'accès à des données de communications stockées est différente de celle de l'interception de communications. L'accès aux communications stockées ne consiste pas en une collecte de données pendant leur transmission ni ne nécessite l'installation d'équipements d'interception. C'est ce qui explique que des règles moins strictes soient appliquées lorsqu'un accès à des données stockées est nécessaire. Cependant, les données stockées sont protégées en vertu de la même loi que les communications pendant leur transmission. L'accès illégal à des données de communications stockées est interdit par l'Article 29.

Article 29: Interdiction d'accès aux communications stockées

147. De la même façon que la criminalisation de l'interception illégale, cet Article criminalise l'accès illégal aux données de communication stockées et explique les circonstances dans lesquelles un tel accès peut être considéré comme légal. Le Groupe de travail a décidé d'inclure la criminalisation afin d'assurer une protection solide de la vie privée et une protection contre les intrusions illégales.

Article 30: Divulgation de données de communication stockées

148. L'Article 30 permet à la personne désignée de demander au prestataire de communication d'obtenir et/ou de divulguer des données de communication stockées au moyen d'une ordonnance de divulgation. Pour garantir la protection de la confidentialité des données de communication stockées, les paragraphes (2) et (3) limitent les conditions dans lesquelles les ordonnances de divulgation peuvent être délivrées aux cas suivants:

- intérêt de la sécurité nationale;
- empêcher ou détecter un crime, ou prévenir des troubles publics;
- intérêt de la sécurité publique;
- protéger la santé publique;

- en cas d'urgence, prévenir un décès, une blessure ou un dommage à la santé physique ou mentale d'une personne ou atténuer une blessure ou un dommage à la santé physique ou mentale d'une personne;

et interdisent la délivrance d'une ordonnance de divulgation sauf si la personne désignée est convaincue de sa nécessité pour obtenir les données et les divulguer à un fonctionnaire habilité.

149. Le paragraphe (4) prévoit un ensemble d'exigences relatives à l'ordonnance de divulgation. Il exige que les circonstances et la raison de son octroi soient précisées, ainsi que les données de communications auxquelles elle s'applique et la manière dont la divulgation doit être faite. En outre, le fonctionnaire habilité doit être identifié. Les exigences relatives à l'ordonnance de divulgation sont établies afin de rendre la procédure transparente et de limiter la divulgation à un cas particulier en précisant tous les détails de l'autorisation.

150. Le paragraphe (5) établit un ensemble de restrictions à l'autorisation qui peuvent passer par l'interdiction de toute exigence liée aux données de communications à obtenir, au-delà du délai d'un mois à compter de la date de délivrance de l'ordonnance. Il interdit également la divulgation de données de communications dont le fournisseur du service de communication n'est pas en possession, ou qu'il doit obtenir, après la fin de ce délai.

151. Pour préserver la confidentialité de l'ordonnance de divulgation, le paragraphe (6), sous réserve des exclusions limitées prévues au paragraphe (7), requiert du prestataire de communication qui reçoit cette ordonnance qu'il préserve la confidentialité de l'existence et de l'application de l'ordonnance, ainsi que des informations qui y sont liées. Pour garantir le droit du prestataire de communication à obtenir des conseils juridiques, le paragraphe (7), entre autres dérogations, permet à l'opérateur de communication de divulguer des informations à un conseiller juridique dans le cadre d'une consultation juridique.

Article 31. Non-respect de la confidentialité de l'information figurant sur l'ordonnance de divulgation

152. Afin de protéger le secret de l'ordonnance de divulgation, l'Article 31 criminalise le non-respect des exigences de confidentialité.

TITRE VI – COÛTS DE L'INTERCEPTION

153. La répartition des coûts est l'un des points de discussion essentiels dans le contexte de l'exécution de l'interception. Il s'agit d'un point particulièrement pertinent pour l'application du devoir d'assistance des prestataires. Les organismes chargés de l'application de la loi s'appuient très souvent sur l'aide du prestataire de communication pour l'exécution de l'interception. En outre, le modèle de texte législatif permet aux pays de fixer l'obligation d'intercepter les communications qui doit être respectée par les prestataires. Par conséquent, la question de la répartition des coûts doit être résolue dans chaque pays qui introduit l'interception de communications.

Article 32: Répartition des coûts

154. Cet article suggère que les coûts générés par le développement des capacités techniques destinées à intercepter les communications au niveau du prestataire (y compris les coûts d'investissement, les coûts techniques, les coûts d'entretien et les coûts d'exploitation) incombent au prestataire de communication. Cependant, un pays peut établir le modèle de remboursement des coûts directs engagés par le prestataire de communication en matière de personnel et d'administration nécessaires à la fourniture d'une aide pour l'exécution du mandat d'interception.

155. L'approche suggérée a fait l'objet d'un débat au sein du Groupe de travail et des participants de la séance plénière de l'atelier de consultation. Le débat s'est concentré sur les fluctuations de la politique publique et sur l'impact qu'une telle position pouvait avoir sur la charge des coûts. À cet égard, le débat a tenu compte du fait que les opérateurs devaient déjà assumer le coût d'autres services. Il a été noté qu'une telle position serait fondée sur la situation fiscale de chaque État, ce qui pourrait influer sur l'attrait exercé par un pays pour les investissements dans le secteur des TIC. Suite à ce débat controversé, le Groupe de travail a décidé de laisser la décision des coûts aux États membres.

156. Par conséquent, chaque pays décidera lui-même de l'approche à adopter sur la façon de répartir les coûts entre les opérateurs et l'État.

TITRE VII – MESURES DE PROTECTION

157. Le Titre VII a été élaboré en conformité avec le modèle de lignes directrices politiques qui exige de protéger le secret professionnel et de mettre en place les mécanismes de suivi et de contrôle à l'égard de l'interception de communications.

158. Cependant, concernant les différences de législations nationales et la capacité des différents pays à créer des organismes de suivi et de contrôle, le Groupe de travail a décidé que cette partie représenterait un ensemble de recommandations que les pays peuvent choisir de suivre ou non.

Article 33. Secret professionnel

159. Le modèle de lignes directrices politiques demandait l'adoption de dispositions protégeant le secret professionnel comme des mesures de protection nécessaires. Cette recommandation fait référence à certains types de communications professionnelles qui sont soumises à l'obligation de secret professionnel aux termes des lois ou réglementations nationales établies par les organismes nationaux compétents. Les dispositions garantissant le secret professionnel doivent être strictement limitées à ces types de communications privilégiées protégées par les lois nationales en vigueur, telles que les communications entre un conseiller juridique et un client, ou entre un médecin et un patient, les communications protégées par la loi réglementant le secret financier et bancaire. La loi elle-même n'établit aucun privilège pour les communications en général, les membres du Groupe de travail estimant que cet aspect n'est pas couvert par leur mandat.

160. La protection du secret professionnel ne signifie pas que les communications de cette personne particulière ne peuvent pas du tout être soumises à une interception. Par exemple, si un conseiller juridique est suspecté d'un crime qui autorise l'interception, l'autorisation de l'interception doit être accordée. Cependant, les données recueillies par cette interception ne doivent pas être présentées comme preuves au tribunal et devront rester protégées si elles contiennent un secret professionnel.

161. Si un pays décide de suivre l'approche suggérée par l'Article 33 et de mettre en œuvre ces mesures de protection, la liste de secrets professionnels protégés en vertu de la loi sera constituée conformément à la législation nationale.

Article 34: Suivi de l'interception de communications

162. L'Article 34 recommande la création d'une autorité de contrôle indépendante conformément aux exigences du modèle de lignes directrices politiques sous-jacent. La possibilité d'un suivi indépendant de l'interception est nécessaire pour renforcer le système de contrôles et d'équilibres relatif à une mesure aussi intrusive que l'interception.

163. À titre d'option, un pays peut investir une autorité qui ne participe pas activement au processus d'enquête et qui est dotée de la capacité de réaliser les fonctions nécessaires à la supervision de l'interception avec les fonctions de l'autorité de contrôle indépendante. Cette option est plus particulièrement pertinente pour les petits pays qui peuvent manquer de ressources.

164. Cet Article donne également des recommandations relatives aux fonctions d'une autorité de contrôle indépendante. Chaque pays peut les préciser.

165. Il a été convenu pendant la discussion dans le Groupe de travail et lors de la séance plénière de l'atelier de consultation, qu'un pays peut décider de mettre ou de ne pas mettre en œuvre cette recommandation selon son système national et selon les ressources dont il dispose.

Article 35. Commissaire indépendant à l'interception de communications

166. Cet article fournit un ensemble de recommandations relatives à la création d'un organisme de contrôle indépendant (le commissaire indépendant à l'interception de communications). Comme expliqué ci-dessus, cet Article ne constitue qu'une recommandation, qui ne doit être mise en œuvre par les pays que si elle est considérée comme nécessaire. Au lieu de créer un poste de commissaire, un pays peut également créer une commission destinée à équilibrer le pouvoir de contrôler l'interception et à prévenir une situation dans laquelle une seule personne en charge peut abuser de cet accès à l'information.

TITRE VIII – ADMISSIBILITÉ DES PREUVES

167. Le groupe de travail a débattu pour savoir si le modèle de texte législatif devait couvrir la question de l'admissibilité des données interceptées en tant qu'éléments de preuve si aucune autre législation ne le faisait.

168. Le Groupe de travail a décidé de laisser une option pour inclure une réglementation sur l'admissibilité des preuves. Cependant, il a été convenu que chaque pays devait développer ces dispositions conformément à sa législation nationale. Par conséquent, la seule recommandation consiste donc à s'assurer que (1) la législation nationale couvre la question de l'admissibilité des preuves obtenues du fait d'une interception; ou que (2) des dispositions sont élaborées en conformité avec l'approche nationale de l'admissibilité des preuves afin de couvrir cette question dans la loi réglementant l'interception.

TITRE IX – ANNEXE

169. L'Annexe représente une liste d'infractions graves qui, sous réserve de l'Article 8, peuvent justifier l'interception comme mesure d'enquête.

170. Le Groupe de travail a introduit une nouvelle disposition autorisant un ministère à ajouter des infractions ou à en supprimer de la liste présente dans l'Annexe. Cette ordonnance doit faire l'objet d'une résolution de ratification.

171. Le Groupe de travail a également convenu de la disposition relative au règlement qui permet à un ministre de promulguer un règlement afin d'appliquer l'objet de ce modèle de texte législatif. Le règlement promulgué en vertu de cet article doit faire l'objet d'une résolution de ratification du parlement.

172. L'Annexe fournit la liste suivante d'infractions recommandées:

- [Meurtre, homicide involontaire ou trahison].
- [Enlèvement ou rapt].
- [Blanchiment d'argent] contraire à la [Loi sur le produit du crime et le blanchiment d'argent (prévention)].
- [Production, fabrication, fourniture ou autre trafic de drogue dangereuse] en violation de la [Loi relative aux drogues dangereuses].
- [Importation ou exportation d'une drogue dangereuse] en violation de la [Loi relative aux drogues dangereuses].
- [Importation, exportation ou transbordement de toute arme à feu ou munitions] en violation de la [Loi sur les armes à feu].
- [Fabrication ou trafic d'armes à feu ou de munitions] en violation de la [Loi sur les armes à feu].
- [Détention illégale d'une arme prohibée ou de toute autre arme à feu ou munition] contraire à un [article de la Loi sur les armes à feu].
- Infraction contraire à un [article de la Loi sur la prévention de la corruption].
- [Incendie criminel].
- [[Convention internationale sur le détournement, infractions terroristes, etc.].
- [Loi sur la prévention du terrorisme].
- Tentative ou complot pour commettre une infraction relevant de l'un des alinéas qui précèdent, ou aide, concours, conseils, ou autre forme d'assistance à la commission d'une telle infraction.

ANNEXES

Annexe 1

Participants au premier Atelier de consultation pour les Groupes de travail du projet HIPCAR traitant du cadre législatif relatif aux TIC – Questions relatives à la société de l'information. Gros Ilet, 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[16]	J Paul
PRESCOD	Kwesi

[16] Président de l'Atelier

Annexe 2

Participants au second Atelier de consultation (stade B) pour les Groupes de travail du projet HIPCAR traitant du cadre législatif relatif aux TIC – Questions relatives à la société de l'information Crane, Saint Philippe, Barbade, du 23 au 26 août 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 Affaires économiques, de l'Autonomisation, de l'Innovation et du Commerce	NICHOLLS	Anthony
Barbade	Ministère des Finances, des Investissements, des Télécommunications et de l'Énergie	BOURNE	Reginald
Barbade	Ministère de la Fonction publique	STRAUGHN	Haseley
Barbade	Université des Antilles	GITTENS	Curtis
Belize	Commission des services publics	PEYREFITTE	Michael
Dominique	Gouvernement de la Dominique	ADRIEN-ROBERTS	Wynante
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
Guyana	Bureau du Président	RAGHUBIR	Gita
Guyana	Commission des services publics	PERSAUD	Vidiahar
Jamaïque	Cabinet du Procureur général	SOLTAU-ROBINSON	Stacey-Ann
Jamaïque	Groupe Digicel	GORTON	Andrew
Jamaïque	LIME	SUTHERLAND CAMPBELL	Melesia
Jamaïque	Ministère de la Sécurité nationale	BEAUMONT	Mitsy
Jamaïque	Bureau du Premier ministre	MURRAY	Wahkeen
Saint-Kitts-et-Nevis	Cabinet du Procureur général	POWELL WILLIAMS	Tashna
Saint-Kitts-et-Nevis	Département de la Technologie, Centre national des TIC	HERBERT	Christopher
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	Cabinet du Procureur général	VIDAL-JULES	Gillian

Annexe 2

Pays	Organisation	Nom	Prénom
Sainte-Lucie	Ministère des Communications, des Travaux publics, des Transports et des Services publics	FELICIEN	Barrymore
Saint-Vincent-et-les-Grenadines	Ministère des Télécommunications, des Sciences, de la Technologie et de l'Industrie	ALEXANDER	Kelroy Andre
Saint-Vincent-et-les-Grenadines	Ministère des Télécommunications, des Sciences, de la Technologie et de l'Industrie	FRASER	Suenel
Suriname	Ministère du Commerce et de l'Industrie	SAN A JONG	Imro
Suriname	Ministère des Transports, des Communications et du Tourisme	STARKE	Cynthia
Suriname	Telecommunicatie Autoriteit Suriname/Autorité des télécommunications du Suriname	PELSWIJK	Wilgo
Suriname	Telecommunicatiebedrijf Suriname/Telesur	JEFFREY	Joan
Trinité-et-Tobago	Ministère de la Sécurité nationale	GOMEZ	Marissa
Trinité-et-Tobago	Ministère de l'Administration publique, Secrétariat des TIC	SWIFT	Kevon
Trinité-et-Tobago	Ministère de l'Administration publique, Division des services juridiques	MAHARAJ	Vashti
Trinité-et-Tobago	Ministère du Procureur général, Cabinet du Procureur général	EVERSLEY	Ida
Trinité-et-Tobago	Autorité des télécommunications de Trinité-et-Tobago	PERSAUD	Karina
Trinité-et-Tobago	Telecommunications of Trinidad and Tobago Limited	BUNSEE	Frank

Participants des organisations régionales/internationales

Organisation	Nom	Prénom
Centre d'administration du développement pour les Caraïbes(CARICAD)	GRIFFITH	Andre
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
Union des télécommunications des Caraïbes (CTU)	WILSON	Selby
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
ALMEIDA	Gilberto Martíns de
GERCKE	Marco
MORGAN[17]	J Paul
PRESCOD	Kwesi

[17] 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