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

Preuve électronique:

Modèles de lignes directrices politiques et de textes législatifs

HIPCAR

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

Avis de non-responsabilité

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

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

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

Avant-propos

Les technologies de l'information et de la communication (TIC) sont à la base du processus de mondialisation. Conscients qu'elles permettent d'accélérer l'intégration économique de la région des Caraïbes et donc d'en renforcer la prospérité et la capacité de transformation sociale, le Marché et l'économie uniques de la Communauté des Caraïbes (CARICOM) ont mis au point une stratégie en matière de TIC axée sur le renforcement de la connectivité et du développement.

La libéralisation du secteur des télécommunications est l'un des éléments clés de cette stratégie. La coordination dans l'ensemble de la région est essentielle si l'on veut que les politiques, la législation et les pratiques résultant de la libéralisation dans chaque pays ne freinent pas, par leur diversité, le développement d'un marché régional.

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

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

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

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

Je saisis cette occasion pour remercier la Commission européenne et le Secrétariat ACP pour leur soutien financier. Je remercie également le Secrétariat de la Communauté des Caraïbes (CARICOM) ainsi que celui de l'Union des télécommunications des Caraïbes (CTU) d'avoir contribué à la réalisation du projet. Sans la volonté politique des pays bénéficiaires, les résultats auraient été bien maigres. Aussi je tiens à exprimer ma profonde gratitude à tous les gouvernements des pays ACP pour leur détermination, qui a assuré le grand succès de ce projet.

Brahima Sanou
Directeur du BDT

Remerciements

Le présent document représente l'achèvement des activités régionales réalisées dans le cadre du projet HIPCAR «Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures» (Amélioration de la compétitivité dans les Caraïbes au travers de l'harmonisation des politiques, législations et procédures réglementaires en matière de TIC), officiellement lancé en décembre 2008 à Grenade.

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

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

Le comité de pilotage du projet HIPCAR, présidé par l'Union des télécommunications des Caraïbes (CTU), a fourni conseils et assistance à une équipe de consultants incluant M. Gilberto Martíns de Almeida et Mme. Pricilla Banner. Le document a ensuite été révisé, finalisé et adopté par un large consensus des participants lors des deux ateliers de consultation du Groupe de travail du projet HIPCAR 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 M. Martíns de Almeida 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. 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 global, le projet ITU-EC-ACP, qui englobe également les pays de l'Afrique sub-saharienne et du Pacifique.

L'objectif du projet HIPCAR consiste à aider la CARICOM/les pays ACP des Caraïbes à harmoniser leurs politiques, législations et 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, facilitant l'intégration des marchés, favorisant l'investissement dans l'amélioration des capacités et services liés aux TIC, et améliorant 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. Les membres du Comité de pilotage incluent 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 général, 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).

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 et des régulateurs nationaux, des points focaux nationaux TIC et des personnes chargées d'élaborer la législation nationale. Les Groupes de travail incluent 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 du projet, organisé 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 meilleures 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 et législation/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 législation nationales en matière de TIC adaptées à leurs exigences, leurs circonstances et leurs priorités spécifiques. Le projet HIPCAR a réservé des fonds pour lui 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 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.

Introduction

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 vise à 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 des 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.

Introduction

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

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

Cette évaluation régionale, publiée séparément en complément du présent rapport[2], comprenait une analyse comparative de la législation en vigueur en matière d'éléments de preuve électronique dans le commerce électronique (ou e-Commerce) 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[3] et garants de la compatibilité avec les traditions juridiques des Caraïbes, les modèles présentés dans ce rapport ont pour but de répondre aux besoins spécifiques de la région.

Le Comité de pilotage du projet HIPCAR, présidé par l'Union des télécommunications des Caraïbes (CTU), a prodigué conseils et soutien à une équipe de consultants composée notamment de M. Gilberto Martíns de Almeida et de Mme Pricilla Banner. Le modèle de texte législatif relatif à la preuve électronique dans le commerce électronique a été élaboré en trois phases: 1) rédaction d'un rapport d'évaluation, 2) élaboration de modèles de lignes directrices politiques et 3) rédaction d'un modèle de texte législatif. Le document a ensuite été révisé, discuté et adopté par consensus large des participants lors de deux ateliers de consultation du Groupe de travail du projet HIPCAR sur les questions de société de

[2] Lire «ICT Policy and Legislative Framework on Information Society Issues – Electronic Evidence in e-Commerce: Assessment Report on the Current Situation in the Caribbean », disponible sur www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

[3] Que l'on retrouve dans la boîte à outils de l'UIT, *ITU's Toolkit for Cybercrime Legislation and Understanding Cybercrime: A Guide for Developing Countries*, la Loi uniforme du Commonwealth sur la preuve électronique (LMM(02)1), la Directive 2002/58/CE et les approches nationales à l'intérieur et à l'extérieur de la région.

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 proposé dans le présent document sont l'œuvre de M. Martíns de Almeida à la suite, notamment, des questions soulevées lors du deuxième atelier. Le Comité de pilotage du projet HIPCAR et l'équipe de gestion du projet ont supervisé l'élaboration de ces documents. Le présent document contient donc les données et informations valables en août 2010.

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

1.6. Importance de l'efficacité des politiques et des lois sur la preuve électronique dans le e-Commerce

À l'instar d'autres usages contemporains des TIC, le commerce électronique, ou e-Commerce, repose sur la recevabilité des éléments de preuve électronique, condition fondamentale à l'instauration de la confiance qui lui permettra de prospérer. Ce fait est reconnu par la communauté internationale, comme en témoignent les lois-types du Commonwealth et de la CNUDCI sur la preuve électronique, ou encore les lois en la matière appliquées dans un grand nombre d'États.

En fait, les dangers croissants pour l'intégrité, la disponibilité, la confidentialité, l'authenticité et la paternité des documents électroniques découlant des actions des pirates informatiques, de la réexpédition, de la criminalité d'entreprise et de la cybercriminalité en général sont sources de nombreuses préoccupations liées aux risques et aux contraintes en matière de recevabilité judiciaire des éléments de preuve électronique.

D'un autre côté, la prolifération des normes et des cadres internationaux relatifs à la sécurité de l'information et à la gouvernance informatique, aux signatures numériques de haute sécurité, aux techniques d'horodatage et aux jugements électroniques des tribunaux ont suscité l'impression collective que les éléments de preuve électronique pourraient être encore plus sûrs et plus fiables que les preuves conventionnelles non électroniques, sous réserve du respect d'un certain nombre de précautions.

Devant ces possibilités et tendances contradictoires, la réglementation doit apporter un équilibre en conciliant les aspects techniques et procéduraux pertinents afin d'exploiter les éléments de preuve moyennant un coût raisonnable, mais aussi de respecter des principes établis tels que le principe de l'équivalence des preuves numériques et non numériques, le principe de précaution (qui implique d'adopter des mesures de prévention et de réduction des risques) et le principe d'accréditation (qui exige une certification agréée des processus afin d'inspirer davantage confiance).

La réglementation des preuves numériques est une tâche qui comporte plusieurs difficultés, notamment la protection proportionnée des droits au respect de la vie privée et du principe selon lequel on ne témoigne pas contre soi-même. La conservation et le cryptage des données sont des exemples de problématiques pour lesquelles la production de preuves numériques se situe au croisement des questions de sécurité et de protection de la vie privée.

L'absence de réglementation locale sur la preuve numérique est un élément dûment noté par les pirates et autres cybercriminels, qui ciblent les pays moins susceptibles d'engager des poursuites sur la base de preuves numériques. Les réseaux zombies sont un exemple des menaces encourues par les citoyens, les gouvernements et les entreprises qui ne disposent pas d'une législation spécifique donnant des conseils et des critères sur la recevabilité des investigations et de la production, de la collecte et de la conservation de preuves numériques.

Introduction

Pour les États, l'introduction d'une législation sur les éléments de preuve électronique ou l'amendement de la législation existant sur les moyens de preuve de manière à prendre en compte les éléments de preuve électronique sont motivés par la reconnaissance du fait que les règles de preuve traditionnellement utilisées dans la Common Law pour faire respecter les droits civils et le droit pénal ne sont pas adaptées aux progrès technologiques et doivent donc être modernisées. La nature de la preuve électronique proprement dite, y compris sa nouveauté et le fait qu'elle puisse être jugée fragile et aisément manipulable, pose des difficultés aux pays qui modernisent leur législation. La preuve électronique est fragile en ce sens qu'elle peut être altérée, endommagée ou détruite par des manipulations ou des examens inadaptés. La preuve électronique est aussi, souvent, de nature transnationale: les serveurs peuvent être situés dans différents pays, ce qui complique l'utilisation de la preuve et sa recevabilité dans un tribunal.

En 2002, le Secrétariat du Commonwealth a recommandé d'adopter ou d'adapter sa loi uniforme en la matière dans tous les pays du Commonwealth. Depuis, la rapidité des progrès technologiques et la sophistication et la diffusion croissantes de la cybercriminalité ont généré de nouvelles difficultés dans les pays cherchant à réglementer la preuve électronique. L'informatique dans le nuage, la cryptographie, l'horodatage, les procédures judiciaires électroniques et les nouvelles normes internationales sont autant d'exemples de nouveaux éléments à prendre en compte.

Dans un tel contexte, la réglementation sur les éléments de preuve électronique doit être formulée en concertation avec la réglementation dans des domaines tels que la conservation rapide des données, les ordonnances de production, les procédures de recherche et de saisie, la conservation des données, etc., afin de garantir l'efficacité nécessaire.

Partie I:
Modèle de lignes directrices politiques – Preuve électronique

Voici des modèles de lignes directrices politiques qu'un pays pourrait prendre en considération en matière de preuve électronique dans le e-Commerce.

1. LES PAYS DE LA CARICOM/DU CARIFORUM VISERONT À DÉFINIR LES INTERPRÉTATIONS COMMUNES NÉCESSAIRES POUR LES PRINCIPAUX TERMES ASSOCIÉS AUX ÉLÉMENTS DE PREUVE ÉLECTRONIQUE[4].

- Des définitions adéquates doivent être fournies pour les termes «ordinateur», «dispositif», «données informatiques», «système informatique», «données relatives au contenu», «données relatives au trafic», «données de localisation», «document», «enregistrement électronique», «document électronique», «signature électronique», «signature numérique» et «horodatage».
- La formulation de la définition de ces termes doit être suffisamment large et assortie d'une liste d'exemples d'illustration.
- La terminologie laissée à l'interprétation judiciaire des juridictions de chaque État bénéficiaire doit être définie, ainsi que les modalités de suivi des activités judiciaires en ce sens afin de préserver l'harmonie des définitions législatives et judiciaires.

2. LES PAYS DE LA CARICOM/DU CARIFORUM VISERONT À INSTAURER LE CADRE NÉCESSAIRE POUR DÉFINIR L'ORIGINE PUBLIQUE OU PRIVÉE ET LE RÔLE DES PARTIES CHARGÉES DE LA COLLECTE ET/OU DE LA GESTION DES ÉLÉMENTS DE PREUVE ÉLECTRONIQUE[5].

- Des dispositions doivent être prévues dans la loi pour définir le rôle des «pouvoirs publics», des magistrats, de la police et, le cas échéant, de «l'autorité d'accréditation», des «prestataires de services de certification», des «bureaux d'enregistrement», de «l'accès permanent» en matière de collecte et/ou de gestion des éléments de preuve électronique.
- Des dispositions doivent être prévues pour stipuler que les pouvoirs publics sont tenus de respecter les règles établies en matière de collecte et de gestion des éléments de preuve électronique par les lois ou politiques relatives à la sécurité de l'information publique (par exemple concernant les limites de l'utilisation de la cryptographie, les procédures de gestion des dispositifs et autres protocoles conformes aux bonnes pratiques internationales en matière d'investigation numérique légale).
- Des dispositions doivent être prévues pour reconnaître les réglementations conjointes ou les autoréglementations sur certains secteurs de marché ou d'activités, en particulier dans les cas où les signatures numériques et l'utilisation d'autres technologies n'offrent pas une rentabilité suffisante.
- Des dispositions doivent être prévues pour définir les principes et les domaines dans lesquels la recevabilité d'une preuve électronique dépendra principalement de normes de procédure.
- Des dispositions doivent être prévues pour créer et appliquer des normes techniques destinées à favoriser la collecte et/ou la gestion appropriées des éléments de preuve électronique.
- Le cas échéant, des dispositions doivent être prévues pour instaurer le principe de réciprocité de la reconnaissance des certificats numériques émanant de pays tiers, en vertu (ou non) de lois régionales communes et d'une autorité régionale commune.

[4] Une campagne publique, laissée à l'appréciation de chaque État bénéficiaire, doit être menée en vue de sensibiliser l'opinion sur les éléments de preuve électronique, notamment en expliquant les termes principaux.

[5] Une politique publique doit être prévue pour développer les compétences du pouvoir judiciaire, afin de permettre aux juges et aux experts techniques de se familiariser avec l'utilisation des principaux concepts, termes et normes de procédure relatifs aux éléments de preuve électronique.
Une politique publique doit être prévue pour encourager la coopération institutionnelle en matière de développement d'applications s'appuyant sur les éléments de preuve électronique, et cela afin de permettre une plus grande automatisation électronique des services publics.

- Le cas échéant, des dispositions doivent être prévues pour stipuler que le pouvoir public pourra être étendu, dans certains cas, à des entités privées, sous réserve que ces entités soient désignées pour agir en tant que «notaire électronique» ou «e-notaire», à savoir des personnes assurant l'authentification numérique de tierce partie sans observer les tests techniques et de procédure d'un prestataire de services de certification enregistré.
- Le cas échéant, il doit être prévu une définition de ce qui caractérise une «notarisation» et, partant, de la mesure dans laquelle les fonctions d'e-notaire sont assorties de droits, avec les obligations qui y sont juridiquement associées.

3. LES PAYS DE LA CARICOM/DU CARIFORUM DOIVENT DÉFINIR LES MANDATS STATUTAIRES ET LES NORMES AUXQUELS SERONT SOUMISES LES ÉLÉMENTS DE PREUVE ÉLECTRONIQUE.

- La loi/le mandat statutaire doit définir un «système d'enregistrements électroniques» aux fins d'interprétation de la présente politique.
- La loi/le mandat statutaire doit être de nature à créer des conditions favorables et s'abstenir de prescriptions excessives dans ses dispositions.
- La loi/le mandat statutaire doit affirmer que l'effet juridique d'un document électronique ne pourra être nié au seul motif qu'il s'agit un document électronique.
- Le cas échéant, La loi/le mandat statutaire doit déterminer dans quelle mesure les normes de procédure relatives à la collecte, à la gestion et/ou à l'utilisation des enregistrements électroniques détermineront la recevabilité des documents électroniques et les circonstances exigeant la présentation d'éléments de preuve électronique techniques.
- La loi/le mandat statutaire doit indiquer les fondements juridiques des éléments de preuve électronique et étendre clairement leur recevabilité aux activités administratives et judiciaires (y compris en matière civile, commerciale, pénale, administrative, relevant du droit du travail et autre).
- La loi/le mandat statutaire doit établir la nature et les effets de la présomption légale associée aux éléments de preuve électronique, de manière à définir son poids vis-à-vis d'autres types de preuves (documentaire et autres).
- La loi/le mandat statutaire doit définir et prescrire la publication d'informations des normes adéquates en matière de mise à jour, de stockage et d'élimination des éléments de preuve électronique.
- La loi/le mandat statutaire doit prévoir la durée de conservation des données produites, collectées, stockées et/ou gérées en tant qu'éléments de preuve électronique, laquelle doit être équivalente aux pratiques habituelles de gestion des éléments de preuve non électronique.
- La loi/le mandat statutaire doit veiller à ce que le secteur public utilise des moyens d'encourager la transparence en ce qui concerne les ressources et les outils disponibles susceptibles de faciliter l'établissement d'éléments de preuve électronique.
- La loi/le mandat statutaire doit établir que la collecte et la gestion des éléments de preuve électronique sont guidées par les objectifs de sécurité, d'efficacité et de validité.
- Une politique publique doit être prévue pour encourager la coopération institutionnelle en matière de développement d'applications s'appuyant sur les éléments de preuve électronique, et cela afin de permettre une plus grande automatisation électronique des services publics.
- La loi/le mandat statutaire doit définir des directives ayant trait au principe de la neutralité technologique, de manière à permettre un développement flexible des outils et mécanismes de la preuve électronique.
- Le cas échéant, la loi doit établir dans quelles circonstances les impressions (ou «copies papier») de documents électroniques seront jugées conformes aux critères de la règle de la meilleure preuve.
- La loi doit établir que la recevabilité des éléments de preuve électronique sera guidée par les principes d'équivalence fonctionnelle, de précaution et d'accréditation.
- La loi doit établir que l'informatique légale sera employée dans les enquêtes préalables ayant trait aux éléments de preuve électronique.

- La loi doit réglementer les circonstances qui permettent d'établir la présomption d'intégrité d'un système d'enregistrements électroniques au moyen d'un témoignage fait au mieux des connaissances et convictions des déposants, ainsi que la possibilité de contre-interroger lesdits déposants.
- La loi doit instaurer des sanctions pour toute personne qui, dans un témoignage ou un certificat, fait une déclaration qu'elle sait être fausse ou dont elle n'est pas convaincue.
- La loi doit établir des critères afin d'harmoniser les sanctions envers une personne ayant fait de fausses déclarations dans un témoignage ou un certificat relatif à l'intégrité d'un système d'enregistrements électroniques.
- La loi/le mandat statutaire doit prévoir la mise en place de procédures de recherche et de saisie appropriées qui permettront de garantir l'intégrité des preuves collectées.
- La loi/le mandat statutaire doit prévoir la mise en place de procédures de certification et de production des données collectées, ainsi que de l'environnement numérique au moment de la collecte des données.
- La loi doit établir la reconnaissance des accords privés relatifs à la recevabilité des enregistrements électroniques (et peut prévoir de l'étendre aux procédures pénales sous réserve de certaines contraintes).
- La loi doit établir que les parties sont libres de s'entendre sur l'utilisation d'une méthode particulière de signature électronique, sauf prescription contraire de la loi.
- La loi doit établir qu'une personne se fiant à une signature électronique devra assumer les conséquences juridiques qui découleront du fait qu'elle n'aura pas pris de mesures raisonnables pour vérifier la fiabilité d'une signature électronique.
- La loi doit établir que les prestataires de services de certification tiendront à disposition pendant une période donnée les dossiers de suivi des procédures de sécurité qu'ils ont suivies.
- La loi doit établir que l'autorité de certification recevra les moyens et sera tenue de certifier également l'heure des enregistrements électroniques («l'horodatage»).

4. LES PAYS DE LA CARICOM/DU CARIFORUM VISERONT À PRÉVOIR UNE PROTECTION ADÉQUATE DES ÉLÉMENTS DE PREUVE ÉLECTRONIQUE.

- Il sera donné une définition de «l'imagerie» aux fins de la protection des éléments de preuve électronique.
- La loi/le mandat statutaire doit établir que les personnes seront protégées de tout préjudice en matière de recevabilité administrative ou judiciaire des éléments de preuve électronique.
- La loi/le mandat statutaire doit prévoir la reconnaissance de l'utilisation d'un horodatage électronique certifié.
- La loi/le mandat statutaire doit prévoir la reconnaissance des normes de procédure en tenant compte de la fiabilité, en termes de preuve, des données détenues sur un système donné d'enregistrements électroniques.
- La loi/le mandat statutaire doit également déterminer, éventuellement par réglementation, les frontières de la légalité de l'utilisation de technologies telles que la cryptographie, la stéganographie et la réexpédition en matière d'éléments de preuve électronique.
- La loi/le mandat statutaire doit prévoir la reconnaissance d'images au titre d'éléments de preuve électronique et prévoir des lignes directrices distinguant les images électroniques de «l'imagerie».
- Une politique publique doit être prévue pour encourager l'utilisation de la certification des attributs dans les certificats de signature numérique, afin d'améliorer la capacité à identifier son détenteur et d'établir une preuve électronique.
- La loi/le mandat statutaire doit encourager l'utilisation de techniques sécurisées (par exemple la transmission sécurisée par réseau IP) lors du recours à la téléconférence, pour une application dans les services publics (par exemple lors de certaines audiences menées dans le cadre d'une procédure judiciaire).

- La loi/le mandat statutaire doit encourager et reconnaître l'utilisation appropriée des caméras en tant que moyen de preuve électronique.
- La loi/le mandat statutaire doit encourager et reconnaître les installations qui peuvent être couvertes par plusieurs dispositifs de télécommunications répartis afin d'établir une preuve électronique.

5. LES PAYS DE LA CARICOM/DU CARIFORUM VISERONT À ÉTABLIR LE CADRE DE LA PREUVE ÉLECTRONIQUE EN CONCERTATION AVEC LES POLITIQUES PUBLIQUES SUR DES THÈMES CONNEXES.

- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de sécurité nationale.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de cybercriminalité.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière d'interception de communications.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de conservation rapide des données.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière d'ordonnances de production.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de recherche et de saisie.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de collecte en temps réel.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de signature numérique.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de protection de la vie privée et des données.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de sécurité de l'information.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de propriété intellectuelle.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière de liberté de l'information.
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme aux traités relatifs à la reconnaissance mutuelle des documents publics officiels (conformément à la Convention de La Haye).
- La loi/le mandat statutaire réglementera les éléments de preuve électronique d'une manière conforme à la politique publique en matière d'inclusion numérique et sociale.

Partie II:
Modèle de texte législatif – Preuve électronique

Voici un modèle de texte législatif qu'un pays peut prendre en considération lors de l'élaboration d'une législation nationale en matière d'éléments de preuve électronique dans le e-Commerce. Ce modèle se fonde sur les lignes directrices politiques types présentées plus haut.

Organisation des articles

Partie II

TITRE I – PRÉAMBULE

Titre abrégé

1. La présente loi peut être citée sous la dénomination suivante: «loi relative à la preuve électronique». Elle entrera en vigueur le […] suivant sa publication au [nom de la publication].

Définitions

2. 1) Un «certificat agréé» désigne un certificat émis par un prestataire de services de certification agréé.

2) Le «destinataire» d'un enregistrement électronique désigne la personne qui, dans l'intention de l'expéditeur, est censée recevoir l'enregistrement électronique, mais non la personne qui agit en tant qu'intermédiaire pour cet enregistrement.

3) Une «signature électronique avancée» désigne une signature électronique délivrée par un prestataire de services de certification agréé.

4) Les «produits» ou «services d'authentification» désignent les produits ou services destinés à identifier le détenteur d'une signature électronique auprès d'autrui.

5) Un «certificat» désigne une attestation électronique qui lie les données relatives à la vérification de signature à une personne et confirme l'identité de cette personne, ou qui lie les données relatives à la vérification de l'heure à un enregistrement ou une communication électronique et qui confirme leur date et heure.

6) Un «ordinateur» désigne un système d'information numérique doté d'équipements et de programmes destinés à la création, à l'enregistrement, au stockage, au traitement et/ou à la transmission de données, et comprenant les ordinateurs, dispositifs informatiques et autres dispositifs électroniques d'information ou de communication destinés à remplir ces fonctions.

7) Les «données relatives au contenu» désignent toute donnée sous forme numérique, optique ou autre, y compris les métadonnées, transmettant une essence, une substance, une information, un sens, un objectif, une intention ou un renseignement, individuellement ou sous une forme combinée et sous leur forme traitée ou non traitée. Les données relatives au contenu comprennent toutes les données transmettant la signification ou la substance d'une communication, ainsi que les données traitées, stockées ou transmises par des programmes informatiques.

8) Un «service de cryptographie» désigne un service fourni à l'expéditeur ou au destinataire d'une communication électronique ou à toute personne stockant une communication électronique dans le but de faciliter l'utilisation de techniques cryptographiques permettant de garantir:

a) que les données ou la communication électronique sont accessibles ou convertibles sous une forme intelligible par certaines personnes seulement,

b) que l'authenticité ou l'intégrité des données ou de la communication électronique peuvent être déterminées,

c) l'intégrité des données ou de la communication électronique, ou

d) que la source des données ou de la communication électronique peut être déterminée avec exactitude.

9) Les «données», «données informatiques» ou «données électroniques» désignent une représentation de faits, d'informations ou de concepts dans un format adapté au traitement par un système d'information, y compris les programmes permettant à un système d'information de remplir une fonction.

10) Une «signature numérique» désigne une signature électronique basée sur une cryptographie asymétrique intégrant l'association de clés publiques et privées.

11) Le format «électronique» comprend tout format créé, enregistré, transmis ou stocké sous une forme numérique ou immatérielle autre par des moyens électroniques, magnétiques ou optiques ou par tout autre moyen offrant des capacités de création, d'enregistrement, de transmission ou de stockage similaires.

12) Un «agent électronique» désigne un programme, un ordinateur ou toute autre méthode électronique ou automatisée, configuré et activé par une personne, qui est utilisé pour entreprendre une action ou pour répondre en tout ou en partie à un enregistrement ou à un événement électronique, sans contrôle humain.

13) L'«authentification électronique» désigne une procédure employée dans le but de vérifier qu'une communication électronique émane bien de son expéditeur et qu'elle n'a pas été modifiée pendant la transmission.

14) Une «communication électronique» désigne un transfert d'enregistrements par le biais de signes, de signaux, d'écrits, d'images, de sons, de données ou de renseignements de toute nature, transmis en tout ou en partie par câble, par radiocommunication, par ondes électromagnétiques ou par un système de photographie électronique ou à fibres optiques, affectant le commerce extérieur ou international, à l'exception:

a) des communications verbales ou filaires,

b) des communications émises au moyen d'un système de radiomessagerie unilatérale avec tonalité seulement,

c) des communications émises par un dispositif de repérage.

15) Un «enregistrement électronique» désigne un jeu de données créées, produites, enregistrées, stockées, traitées, envoyées, communiquées et/ou reçues, quel que soit le support physique, par un ordinateur ou un dispositif similaire, et qui peut être lu ou perçu par une personne au moyen d'un système informatique ou d'un dispositif similaire, y compris par l'affichage, l'impression ou une autre sortie de ces données.

16) Une «signature électronique» désigne une signature basée sur un processus électronique, tel que, entre autres, la signature numérique et la signature biométrique.

17) Un «système d'information», «système informatique», «système informatisé» ou «système de traitement de données» désigne un dispositif ou un groupe de dispositifs interconnectés ou reliés, y compris Internet, qui, conformément à un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions.

18) La «loi» désigne la Common Law, les lois et le droit dérivé.

19) Une «action en justice» désigne une action engagée en matière civile, pénale ou administrative devant une Cour ou auprès d'un tribunal, d'un comité ou d'une commission.

20) Les «données de localisation» désignent toutes les données traitées sur un réseau de communications électroniques et indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public.

21) L'«expéditeur» d'un enregistrement électronique désigne une personne qui:

a) envoie un enregistrement électronique,

b) demande à quelqu'un d'envoyer un enregistrement électronique en son nom, ou

c) fait envoyer un enregistrement électronique par son agent électronique, à l'exclusion des personnes intervenant en tant qu'agent ou intermédiaire dans l'envoi de l'enregistrement électronique.

22) Les «organismes publics» comprennent:

a) les ministères ou départements du gouvernement;

b) les entreprises détenues en tout ou en partie par l'État;

c) les organismes exerçant une autorité légale de nature législative, exécutive ou judiciaire;

d) les autorités publiques territoriales ou locales, y compris les municipalités.

23) Un «enregistrement» ou «dossier» désigne une information enregistrée qui a été collectée, créée ou reçue lors du lancement, de la conduite ou de l'achèvement d'une activité et qui présente suffisamment de contenu, de contexte et de structure pour apporter la preuve de cette activité ou transaction, et qui est inscrit, stocké ou conservé par un autre moyen sur un support matériel, ou stocké sur un support électronique ou autre, et accessible sous une forme perceptible.

24) Une «procédure de sécurité» désigne une procédure instituée par la loi ou un accord ou adoptée en connaissance de cause par les parties, et qui est employée dans le but de vérifier qu'une signature, une communication ou une performance électronique est bien celle d'une personne donnée ou de déceler des modifications ou des erreurs dans le contenu d'une communication électronique.

25) Une «signature» inclut tout symbole exécuté ou adopté, ou toute méthode ou procédure employée ou adoptée par quelqu'un dans l'intention d'authentifier un enregistrement, y compris les méthodes électroniques ou numériques.

26) Les «données relatives à la création de signature» désignent des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique.

27) Les «informations sur l'abonné» désignent les informations contenues sous la forme de données informatiques ou sous une autre forme et détenues par un prestataire de services au sujet des abonnés à ses services, à l'exception des données relatives au trafic et au contenu, à partir desquelles il est possible d'établir:

a) le type de service de communication utilisé, les dispositions techniques prises en la matière et la durée du service,

b) l'identité de l'abonné, son adresse postale ou physique, son numéro de téléphone et ses autres numéros d'accès, les informations pour la facturation et le paiement, tels qu'ils sont fournis pour le contrat ou l'accord de service, et/ou

c) les informations relatives à la localisation de l'équipement de communication installé, telles qu'elles figurent dans le contrat ou l'accord de service.

28) Les «données relatives au trafic» désignent les données informatiques:

a) relatives à une communication par le biais d'un système informatique,

b) produites par un système informatique dans le cadre d'une chaîne de communication, et

c) affichant l'origine de la communication, sa destination, son itinéraire, son horodatage, sa taille, sa durée ou le type des services sous-jacents.

TITRE II – RECEVABILITÉ

Amendement aux règles d'authentification et de meilleure preuve

3. La présente loi ne modifie aucune des dispositions légales ou de la Common Law relative à la recevabilité des enregistrements, à l'exception de celles ayant trait à l'authentification et à la meilleure preuve.

Common Law et règlements

4. Lors de l'application d'une disposition légale ou de la Common Law relative à la recevabilité des enregistrements, la Cour peut prendre en considération les principes directeurs de la recevabilité des enregistrements électroniques prescrits par la présente loi.

Recevabilité générale des éléments de preuve électronique

5. Aucune des règles de preuve ne pourra être appliquée pour contester la recevabilité d'un enregistrement électronique comme moyen de preuve au seul motif qu'il s'agit d'un enregistrement électronique.

Application de la règle de la meilleure preuve

6. 1) Sous réserve des dispositions du paragraphe 2, lorsque la règle de la meilleure preuve concerne un enregistrement électronique dans une action en justice, ladite règle est satisfaite dès lors qu'est établie l'intégrité de l'ordinateur sur lequel ou par lequel les données ont été enregistrées ou stockées.

2) En l'absence de preuve contraire, l'intégrité de l'ordinateur sur lequel un enregistrement électronique est enregistré ou stocké est présumée lors d'une action en justice:

a) lorsqu'il est apporté des preuves étayant la conclusion que le système informatique ou un autre dispositif similaire fonctionnait correctement au moment des faits ou, dans le cas contraire, que, lorsqu'il ne fonctionnait pas correctement ou se trouvait hors service, l'intégrité de l'enregistrement n'en a pas été affectée, et lorsqu'il n'existe aucun motif raisonnable de contester l'intégrité de l'enregistrement;

b) lorsqu'il est établi que l'enregistrement électronique a été enregistré ou stocké par une partie adverse à la partie cherchant à le présenter; ou

c) lorsqu'il est établi que l'enregistrement électronique a été enregistré ou stocké dans le cadre normal et ordinaire des activités d'une personne qui ne participe pas à la procédure et qui ne l'a pas enregistré ou stocké sous le contrôle de la partie cherchant à présenter l'enregistrement.

Intégrité de l'information et règles particulières de recevabilité

7. 1) Toute déclaration contenue sur un enregistrement électronique produit par un ordinateur qui constitue un ouï-dire ne sera pas recevable au titre de preuve des faits qui y sont indiqués, à moins que l'ordinateur ne soit présumé intègre en vertu des dispositions du paragraphe 2.

2) En l'absence de preuve contraire, l'ordinateur sur lequel un enregistrement électronique est enregistré ou stocké est présumé intègre lors d'une action en justice si cet enregistrement:

a) est resté complet et n'a pas été altéré, à l'exception:

i) de l'ajout d'une mention ou

ii) d'une modification immatérielle,

intervenant dans le cours normal de la communication, du stockage ou de l'affichage;

b) bénéficie d'un certificat ou d'une signature électronique selon une méthode fournie par des entités de certification agréée;

c) dont l'intégrité et le contenu ont été notariés,

d) a été enregistré sur un dispositif de stockage non réinscriptible, ou selon un autre moyen électronique empêchant toute altération des enregistrements électroniques,

e) a été examiné et a vu son intégrité confirmée par un expert désigné par la Cour, ou

f) en rapport avec lequel:

i) il est apporté des preuves étayant la conclusion que le système informatique ou un autre dispositif similaire fonctionnait correctement au moment des faits ou, dans le cas contraire, que, lorsqu'il ne fonctionnait pas correctement ou se trouvait hors service, l'intégrité de l'enregistrement n'en a pas été affectée, et il n'existe aucun motif raisonnable de contester l'intégrité de l'enregistrement,

ii) il est établi que l'enregistrement électronique a été enregistré ou stocké par une partie adverse à la partie cherchant à le présenter, ou

iii) il est établi que l'enregistrement électronique a été enregistré ou stocké dans le cadre normal et ordinaire des activités d'une personne qui ne participe pas à la procédure et qui ne l'a pas enregistré ou stocké sous le contrôle de la partie cherchant à présenter l'enregistrement.

3) Lorsqu'une déclaration contenue sur un enregistrement électronique produit par un ordinateur ne constitue pas un ouï-dire, cette déclaration doit être recevable si les conditions relatives à cet enregistrement électronique et énumérées au paragraphe 2 sont remplies.

Impressions 8. Dans une action en justice, lorsque l'on s'est référé, fié ou fondé de façon manifeste et constante à l'impression d'un enregistrement électronique en tant qu'enregistrement d'une information enregistrée ou stockée sur papier, cette version imprimée constitue l'enregistrement aux fins de la règle de la meilleure preuve.

Charge de la preuve de l'authenticité d'une preuve électronique 9. La charge de prouver l'authenticité d'un enregistrement électronique lors d'une action en justice revient à la personne qui souhaite l'introduire, en présentant des faits susceptibles d'étayer la conclusion que l'enregistrement électronique est bien ce que cette personne prétend. Dans le cas où une législation particulière protégeant des personnes vulnérables, notamment les consommateurs et les enfants, attribue la charge de la preuve en fonction de ce qui est le plus profitable à ces personnes, cette législation prévaut sur le présent article.

Normes 10. Afin de déterminer la recevabilité d'un enregistrement électronique en vertu d'une autre loi, il est possible de présenter des preuves concernant les normes, procédures, usages ou pratiques ayant trait à l'enregistrement ou à la conservation des enregistrements électroniques, en tenant compte du type d'activité ou d'entreprise qui utilise, enregistre ou conserve l'enregistrement et de la nature et de la finalité de l'enregistrement. Les pouvoirs publics chargés de l'élaboration ou de la validation des normes techniques ou des procédures de sécurité pertinentes doivent publier des lignes directrices indiquant les critères applicables pour se conformer au présent article.

Témoignages 11. Lorsqu'il est prévu de présenter pour preuve un enregistrement électronique, il est autorisé de présenter cet enregistrement sous forme de témoignage.

Accord sur la recevabilité d'une preuve 12. 1) Sauf disposition réglementaire contraire, un enregistrement électronique est recevable, sous réserve d'une décision de la Cour, si les parties à la procédure acceptent expressément que sa recevabilité ne puisse pas être contestée.

2) Nonobstant les dispositions du paragraphe 1, un accord entre les parties sur la recevabilité d'un enregistrement électronique n'induit pas la recevabilité de l'enregistrement dans une action pénale au nom de l'accusation si, au moment de l'accord, l'accusé ou l'une des personnes accusées ne bénéficiait pas d'une assistance ou d'une représentation légale.

Signature électronique 13. 1) Une signature électronique ne peut pas être privée de sa force et de ses effets juridiques au seul motif qu'elle est au format électronique.

2) Une signature électronique peut être prouvée par tout moyen, y compris en démontrant l'existence d'une procédure imposant, pour conclure une transaction, d'exécuter un symbole ou une procédure de sécurité visant à vérifier qu'un enregistrement électronique émane bien de la personne présumée.

Conditions relatives aux signatures électroniques 14. 1) Lorsque la loi exige la signature d'une personne, cette exigence est satisfaite s'il est fait usage d'une signature électronique dont la fiabilité est suffisante au regard de l'objet pour lequel elle a été créée ou communiquée, compte tenu de toutes les circonstances, y compris toute convention en la matière.

2) Le paragraphe 1 s'applique, que l'exigence d'une signature ait la forme d'une obligation ou que la loi prévoie certaines conséquences en l'absence de signature.

3) Les parties peuvent convenir d'utiliser une méthode particulière de signature électronique, sauf disposition contraire de la loi.

4) Lorsqu'une signature électronique est requise par les parties à une transaction électronique et que les parties n'ont pas convenu du type de signature électronique à utiliser, cette exigence est satisfaite dans le cas d'un message de données si:

a) les données relatives à la création de signature sont liées exclusivement au signataire,

b) les données relatives à la création de signature étaient, au moment de la signature, sous le contrôle exclusif du signataire,

c) toute modification apportée à la signature électronique après le moment de la signature est décelable, et

d) dans le cas où l'exigence légale de signature a pour but de garantir la validité de l'information à laquelle elle se rapporte, toute modification apportée à cette information après le moment de la signature est décelable.

5) Le paragraphe 4 ne limite pas la possibilité pour toute personne:

a) d'établir de toute autre manière, aux fins de satisfaire l'exigence visée au paragraphe 1, la fiabilité d'une signature électronique, ou

b) d'apporter la preuve de la non-fiabilité de la signature électronique.

6) Une personne se fiant à une signature électronique assume les conséquences juridiques découlant du fait qu'elle s'est abstenue de prendre des mesures raisonnables pour vérifier la fiabilité d'une signature électronique.

7) La Cour tient compte de toute loi régissant l'authenticité de la paternité et de l'intégrité des enregistrements électroniques signés numériquement.

Autres techniques et procédures de production d'éléments de preuve électronique

15. Outre les moyens de preuve visés dans les articles précédents du présent texte de loi, des éléments de preuve électronique pourront être produits concernant certains enregistrements électroniques au moyen d'autres techniques et procédures, notamment l'attestation d'un notaire, d'un juge de paix ou d'une autorité similaire, l'enregistrement sur un support non réinscriptible et l'informatique légale dans le cadre d'enquêtes préalables.

TITRE III – DISPOSITIONS GÉNÉRALES

Recevabilité des enregistre-ments électroniques émanant d'autres pays

16. Lorsque les éléments de preuve électronique proviennent d'une autre juridiction, leur recevabilité n'est pas remise en cause si l'intégrité de l'ordinateur associé aux éléments de preuve électronique en question est prouvée ou présumée conformément à des normes comparables à celles prévues à l'Article 6, paragraphe 2, alinéa a et à l'Article 7, paragraphe 2 de la présente loi.

Partie II

Reconnaissance des documents et signatures électroniques étrangers

17. 1) Afin de déterminer si ou dans quelle mesure une information au format électronique produit légalement des effets, il ne sera tenu aucun compte du lieu de création ou d'utilisation de l'information ou du siège de sa création, pour autant que l'enregistrement électronique se trouve dans une juridiction nationale.

2) Lorsque l'enregistrement électronique se trouve dans une juridiction étrangère, le paragraphe 1 ci-dessus ne s'applique pas, à moins que:

a) la partie apportant la preuve du contenu de l'enregistrement électronique ait remis aux autres parties, au plus tard 14 jours avant la date de présentation de la preuve, une copie de l'enregistrement électronique visé,

b) la Cour ait décidé de son applicabilité, ou

c) il existe un traité international en vigueur instaurant la reconnaissance des enregistrements électroniques ou des signatures électroniques se trouvant dans cette juridiction étrangère.

Interprétation conforme aux principes acceptés sur le plan international

18. Les dispositions du présent texte de loi doivent être interprétées et appliquées à la lumière des principes acceptés sur le plan international de la neutralité technologique et de l'équivalence fonctionnelle.

Réglementation

19. Le Ministre compétent peut réglementer l'entrée en vigueur des objectifs de la présente loi et toute prescription requise ou autorisée par lui. Pour cela, le Ministre peut tenir compte des bonnes pratiques et normes internationales en la matière.

Partie III:
Notes explicatives relatives au modèle de texte législatif sur les éléments de preuve électronique

INTRODUCTION

1. Le présent texte législatif définit un cadre légal de recevabilité des enregistrements électroniques. Il a pour principaux objectifs d'établir la recevabilité générale des éléments de preuve électronique, d'amender les règles juridiques d'authentification et de la meilleure preuve, de définir les critères permettant de présumer de l'intégrité des ordinateurs et des enregistrements électroniques, d'établir la charge de la preuve pertinente, de réglementer la recevabilité des signatures électroniques, de déterminer l'interprétation en fonction des principes acceptés sur le plan international et d'envisager la reconnaissance d'enregistrements électroniques créés ou situés dans d'autres pays.

2. Les présentes Notes visent à expliquer le contenu de la loi et doivent être lues en parallèle à celle-ci. Elles expliquent l'importance des dispositions principales et attirent l'attention, s'il y a lieu, sur certaines discussions du Groupe de travail, en soulignant les différentes options de réglementation débattues. Elles ne constituent pas une description détaillée de la loi et ne sont pas destinées à l'être. Par conséquent, lorsqu'un article ou une partie d'un article ne semble nécessiter aucun éclaircissement, commentaire ou référence ou lorsqu'une disposition n'a donné lieu à aucune discussion, il n'est donné aucune explication détaillée.

3. La présente loi se décompose en trois parties:

   - Le **Titre I** fournit des définitions;
   - Le **Titre II** amende les règles juridiques d'authentification et de la meilleure preuve, établit le principe de non-discrimination à l'égard des enregistrements électroniques, réglemente l'application de la règle de la meilleure preuve, définit les critères de présomption de l'intégrité des ordinateurs et des enregistrements électroniques, attribue la charge de la preuve, détermine la publication de lignes directrices relatives à la conformité aux normes techniques et aux procédures de sécurité, reconnaît les accords sur la recevabilité des éléments de preuve électronique dans les actions en justice, admet les signatures électroniques comme moyen de preuve et évoque les autres techniques et procédures de production d'une preuve électronique;
   - Le **Titre III** établit les dispositions générales ayant trait à la recevabilité des enregistrements électroniques d'autres pays, à la reconnaissance des documents et signatures électroniques étrangers, à l'interprétation conforme aux principes acceptés sur le plan international et aux réglementations possibles conformément aux normes et aux bonnes pratiques internationales.

Partie III

COMMENTAIRE ARTICLE PAR ARTICLE

TITRE I: PRÉAMBULE

4. Le Titre I fournit les dispositions préliminaires telles que le titre abrégé et l'entrée en vigueur dans l'**Article 1** et les définitions dans l'**Article 2**.

5. Le Titre I a donné lieu à une discussion au sein du Groupe de travail concernant le style de rédaction selon les juridictions. Une question portant sur la nécessité d'inclure un article définissant les objectifs de la loi a été débattue, et un consensus a été trouvé sur le fait que cette question devait être laissée à la discrétion des États bénéficiaires.

Article 2: Définitions

6. La définition de l'**ordinateur** apportée par le paragraphe 6 permet d'englober tout dispositif électronique susceptible de remplir les fonctions typiques d'un ordinateur.

7. Le Groupe de travail a discuté de la possibilité d'inclure une référence explicite à des équipements de télécommunications tels que les Smartphones. Il a été convenu que, compte tenu du rythme rapide des progrès technologiques et du principe de la neutralité technologique, il était préférable de conserver une formulation large mentionnant des «dispositifs électroniques d'information ou de communication» en complément des références aux «ordinateurs» et aux «dispositifs informatiques».

8. Les **données relatives au contenu** (ainsi que les données de localisation et les données relatives au trafic, qui sont définies, respectivement, aux paragraphes 20 et 28) sont les données dont la production, la communication, le traitement et le stockage sont les cibles naturelles de la production d'éléments de preuve électronique, puisqu'elles donnent corps aux communications et transactions à leur origine.

9. La définition des données relatives au contenu a été formulée de manière à englober toutes les formes de contenu d'un enregistrement électronique («une essence, une substance, une information, un sens, un objectif, une intention ou un renseignement»).

10. Cette définition évoque à la fois les formes traitées et non traitées des données relatives au contenu, l'objectif étant ici d'englober non seulement le contenu «brut» destiné à être transformé par traitement des données, mais aussi les différentes données produites à l'issue de ce traitement.

11. La définition en question évoque également les «métadonnées», qui sont une deuxième couche de données contenant des «données sur les données» (par exemple le langage utilisé pour rédiger du contenu, l'heure de sa création, les sources possibles de renseignements complémentaires sur ce contenu, etc.). Dans la mesure où l'utilisation de métadonnées et de méta-balises est de plus en plus populaire (avec, en particulier, l'usage répandu des moteurs de recherche sur Internet, alimentés par ces métadonnées et méta-balises), les métadonnées peuvent fournir des éléments importants pour la production d'éléments de preuve électronique ayant trait aux données relatives au contenu.

12. Les **données** sont définies au paragraphe 9 comme représentant des faits, des informations ou des concepts sous une forme adaptée au traitement par un système d'information.

13. Le terme «données» a été choisi pour la définition de préférence à «information», car ce dernier terme figure dans la législation nationale de certains pays en rapport avec les preuves d'ordre général, et pas nécessairement les éléments de preuve électronique. La présente loi portant uniquement sur les éléments de preuve électronique, l'objectif était ici de désigner exclusivement les faits, informations et concepts représentés sous forme d'éléments binaires électroniques.

14. Le Groupe de travail a débattu de l'utilité d'inclure ou non l'expression «état» dans cette définition, dans le but de souligner que ces données pouvaient ne pas être uniquement conçues comme une séquence logique de «0» et de «1» (représentant des chiffres ou des nombres), mais aussi représenter la variation tangible de l'état électromagnétique ou optique d'un ordinateur que le système d'information «lit» comme correspondant aux éléments binaires respectifs. Bien que l'expression «état» puisse aider les profanes (dont les magistrats) à prendre également en compte l'aspect tangible des données et ainsi contribuer à la qualification des données en tant qu'«objets» sur un plan légal (afin d'établir qu'elles peuvent être possédées ou détournées, entre autres finalités), la dernière partie de la définition retenue, qui précise «y compris les programmes permettant à un système d'information de remplir une fonction», permet d'atteindre indirectement, dans une certaine mesure, l'objectif de désigner également leur caractère tangible (puisque que l'exécution d'une fonction sur un système d'information est censée produire des changements concrets). Par conséquent, le choix du niveau de mise en évidence du caractère tangible des données a été laissé à la discrétion des États bénéficiaires.

15. Enfin, cette définition établit clairement que «données» est un synonyme de «données informatiques» et de «données électroniques», des termes que l'on retrouve dans la législation en la matière au niveau national et international. La correspondance entre les premières et les dernières est ainsi garantie, par souci de cohérence, notamment avec la législation d'autres pays: la terminologie employée étant très diverse, il est d'autant plus nécessaire de jeter des ponts facilitant une interprétation et une application communes.

16. La **signature numérique** est définie dans le paragraphe 10 comme une catégorie particulière de signature électronique. Avec les autres expressions définies (dont **certificat agréé, signature électronique avancée, produits et services d'authentification, certificat, service de cryptographie, signature électronique, signature** et **données relatives à la création de signature**) dans les paragraphes de l'Article 2, elle donne un sens cohérent à un système essentiel de production d'éléments de preuve électronique, le système d'authentification, de certification et d'accréditation des signatures numériques, qui permet d'identifier l'auteur, l'origine, l'heure et d'autres éléments.

17. Les définitions adoptées pour ces expressions tiennent compte du fait que l'État bénéficiaire peut ne pas avoir mis en place de technologie ou de structure définie pour construire un système de signatures électroniques certifiées qui serait établi au niveau local ou engagé à l'étranger. C'est la raison pour laquelle ces définitions se concentrent sur les aspects fondamentaux, les options spécifiques éventuelles étant laissées à une réglementation complémentaire (structure différente des rôles et des pouvoirs, allocation de ressources régionales ou nationales, etc.).

18. Grâce à cette approche, la définition des signatures numériques facilite leur intégration dans d'autres dispositions du texte, notamment celles relatives à la conformité à la règle de la meilleure preuve ou à d'autres moyens de production d'éléments de preuve électronique, puisque la formulation générale adoptée offre la souplesse nécessaire pour prendre en compte différentes manières d'utiliser des signatures numériques en vue de prouver l'intégrité et la fiabilité d'un ordinateur ou d'un enregistrement électronique, ou pour refléter ou intégrer d'autres formes d'éléments de preuve électronique.

19. La réponse électronique automatisée utilisée en tant qu'interface d'interaction entre les êtres humains et les ordinateurs caractérise l'**agent électronique**, défini dans le paragraphe 12. Cette définition est l'une des celles qui intègrent les concepts d'expéditeur et de destinataire d'une communication électronique et qui permettent de déterminer si un envoi ou une réception ont effectivement eu lieu, ainsi que les modalités et les conditions régissant la démonstration de la preuve.

20. La fiabilité des communications étayée par des moyens électroniques est fondamentale à la finalité de production des éléments de preuve électronique pertinents. Le concept de l'**authentification électronique**, défini au paragraphe 13, permet de déterminer les procédures qu'il est possible d'utiliser pour vérifier si une communication donnée a été modifiée au cours de la transmission et pour s'assurer de son expéditeur.

21. La définition de la **communication électronique**, au paragraphe 14, est importante, car elle s'intéresse au transfert des enregistrements, y compris l'envoi et la réception, alors que les définitions d'«ordinateur» et de «système d'information» se limitent aux activités internes effectuées par l'ordinateur ou par le système d'information.

22. Le Groupe de travail a discuté de l'utilité d'inclure une référence aux «communications verbales ou par fil». Certains membres s'inquiétaient du fait que ces expressions puissent chevaucher d'autres expressions existantes dans les lois relatives à la communication de certains pays, en particulier en termes de téléphonie, de radiomessagerie et de dispositifs de repérage. Le Groupe a décidé de laisser à la discrétion des États bénéficiaires la possibilité de conserver ou non cette formulation.

23. Le paragraphe 4 définit l'**enregistrement électronique** comme un jeu de données qui peut être lu ou perçu par une personne au moyen d'un système informatique ou d'un dispositif similaire.

24. Si les données sont représentées sous forme binaire et ont pour vocation d'être «lues» par un ordinateur ou «traduites» par un programme informatique, l'enregistrement électronique est l'apparence ou la production d'un système d'information qui est perceptible par un être humain.

25. La distinction entre ces expressions complémentaires, «données» et «enregistrement électronique», est nécessaire afin de légiférer sur la preuve électronique, car la preuve de certains faits, informations ou concepts peut reposer sur la perception d'une personne (ou sur sa capacité à les percevoir) et pas uniquement sur la possibilité d'une enquête technique.

26. La définition d'un enregistrement électronique est également utile pour déterminer la signification d'un dispositif électronique d'information (mentionné dans certaines dispositions de la loi sous la formulation «dispositif électronique d'information ou de communication»), qui est destiné de toute évidence à désigner un dispositif utilisé par des personnes pour accéder à des enregistrements électroniques ou pour les percevoir.

27. En outre, la définition de l'enregistrement électronique comprend l'expression «quel que soit le support physique», qui doit contribuer à élargir le champ d'application des supports associés aux enregistrements électroniques à d'autres supports que les supports traditionnels, pour inclure, par exemple, les supports biométriques (empreintes digitales, iris, etc.), qui sont de plus en plus utilisés dans le contexte des éléments de preuve électronique.

28. De même, la référence aux versions imprimées clarifie le fait que les enregistrements électroniques ne sont pas nécessairement perceptibles sur un système informatique, mais peuvent aussi être perçus, plus fréquemment, comme des éléments extérieurs à celui-ci.

29. La définition du **système d'information** (paragraphe 17) revêt une importance identique pour comprendre les phénomènes entourant les éléments de preuve électronique. Si la définition de l'ordinateur désigne un équipement électronique unique, la définition du système d'information est destinée à intégrer des groupes de dispositifs interconnectés, caractéristiques des réseaux électroniques.

30. Cette définition large peut inclure des réseaux de différents niveaux, y compris Internet, qui est considéré d'un point de vue technique comme un «réseau de réseaux». Étant donné l'importance d'Internet comme lieu de production et de collecte d'éléments de preuve électronique, il y a été fait spécialement référence. Le concept de groupe de dispositifs interconnectés est suffisamment complet pour intégrer tous les équipements reliés à Internet.

31. Le Groupe de travail a discuté de l'utilisation des expressions «système informatique» ou «système d'information» dans le texte. Le fait que «système d'information» (et «système de traitement d'informations») soit l'expression la plus fréquente dans les législations nationales a joué en sa faveur. Bien qu'il existe des différences techniques de sens entre «système d'information» et «système informatique», elles ont été jugées accessoires dans le contexte des éléments de preuve électronique; l'option adoptée a donc été d'utiliser «système d'information» en ajoutant «système informatique» et «système de traitement de données» comme expressions équivalentes. Le niveau de précision technique désiré pour traiter ces concepts dans le contexte de la présente loi a été laissé à l'appréciation des États bénéficiaires.

32. La définition de l'**action en justice** (paragraphe 19) comprend les actions en matière aussi bien civile que pénale et administrative. Si les éléments de preuve électronique ont tendance à être bien acceptés dans les procédures civiles, ils sont souvent contestés dans les procédures pénales au motif que leur nature «virtuelle» ne constitue pas une preuve suffisante pour justifier une condamnation pénale. De même, il peut ne pas être tenu compte de l'aspect «immatériel» habituellement associé aux éléments de preuve électronique dans les milieux administratifs, laissant aux procédures judiciaires la charge d'évaluer ces preuves. Il est donc important d'affirmer sans ambiguïté qu'une preuve électronique produite en bonne et due forme doit être valide quelle que soit la procédure, civile ou pénale, judiciaire ou administrative.

33. Le lieu où est situé l'équipement est un élément important pour la production d'éléments de preuve électronique, car il peut entraîner des conclusions et des conséquences différentes, notamment en termes de juridiction compétente et de lois applicables, de détermination du niveau de sécurité requis et de la responsabilité y afférent, d'indication sur l'expéditeur des documents ou des communications, de preuve de leur envoi ou réception effectifs, etc. La définition des **données de localisation** (paragraphe 20) reconnaît l'importance de la position géographique de l'équipement pour la production de preuves dans le contexte des réseaux de communications électroniques.

34. La définition a retenu l'équipement terminal comme paramètre de définition de la position géographique, car cette expression est suffisamment souple pour englober non seulement les ordinateurs, mais aussi les dispositifs susceptibles d'être utilisés dans le contexte d'un service de communication électronique.

35. Il est également important de noter que cette définition limite le champ d'application de la définition de la position géographique aux services de communications électroniques «publiquement disponibles», ce qui peut contribuer à concilier les questions de sécurité liées à la nécessité d'identifier la position géographique et les exigences de respect de la vie privée, le cas échéant.

36. Le concept d'**expéditeur** défini au paragraphe 21 est suffisamment vaste pour inclure non seulement la personne qui envoie véritablement une communication électronique, mais aussi la personne qui demande à quelqu'un de l'envoyer en son nom ou celle qui utilise un agent électronique pour l'envoyer.

37. L'exhaustivité de ce concept revêt une importance croissante dans la mesure où le volume des communications électroniques «envoyées» par des tiers (les «centres d'appels électroniques», par exemple) ou par des agents électroniques (dans les contrats dits «d'achat en ligne», notamment) augmente rapidement.

38. Le Groupe de travail a décidé d'inclure une remarque visant à préciser que «l'agent électronique» n'intégrait pas les personnes. Cette remarque rejoint la définition de l'agent électronique donnée dans le paragraphe 12.

39. Les **organismes publics**, définis au paragraphe 22, comprennent les ministères et services gouvernementaux, les entreprises détenues par l'État, les organismes exerçant une autorité légale et les autorités publiques territoriales ou locales.

40. Cette définition complète est conforme à la définition de la **loi** (paragraphe 18), qui intègre la Common Law, les lois et le droit dérivé, et rejoint également l'observation faite au point 16 ci-dessus, qui évoque la possibilité d'une réglementation complémentaire instaurant un système d'authentification et/ou de certification des signatures numériques. En l'occurrence, les éléments de preuve électronique présentent un large éventail d'implications pour les organismes publics et pour l'ensemble des citoyens, de sorte que le nombre de lois susceptibles de les réglementer, ainsi que le nombre d'autorités ou d'entreprises publiques susceptibles de les utiliser ou de les réglementer, est loin d'être négligeable. La définition se devait donc d'être suffisamment complète.

41. Bien que la présente loi ne contienne pas un grand nombre de dispositions s'appuyant sur cette définition (ou y recourant indirectement, à l'instar de l'Article 10 qui mentionne les «pouvoirs publics»), elle préétablit le large éventail d'organismes publics appelés à émettre une réglementation complémentaire ou à en bénéficier (comme dans l'exemple cité de création d'un système d'authentification et/ou de certification des signatures numériques), apportant ainsi des bases adéquates à la future législation dérivée.

42. La définition des **procédures de sécurité** (paragraphe 24) ne s'arrête pas au contenu des définitions des «produits ou services d'authentification» et de «l'authentification électronique», fournies respectivement aux paragraphes 4 et 13, dans la mesure où la présomption d'intégrité d'un ordinateur dépend de l'adoption de procédures de sécurité indépendamment des tests éventuels basés sur l'authentification électronique, mais aussi dans la mesure où les normes techniques relatives à la sécurité de l'information sont essentiellement d'ordre procédural et n'imposent pas nécessairement de recourir à des produits ou services d'authentification. Par conséquent, la définition d'une procédure de sécurité est un ingrédient supplémentaire important pour légitimer la production d'éléments de preuve électronique.

43. La formulation de cette définition englobe non seulement les procédures de sécurité soumises à des normes techniques, mais aussi celles instaurées par la loi, par des contrats ou par des pratiques courantes reconnues, car il est important de reconnaître le libre arbitre des parties intéressées, qui peuvent négocier le niveau souhaité des procédures de sécurité, ou encore l'existence de bonnes pratiques sur le terrain au niveau national et/ou international.

44. Les **informations sur l'abonné** sont un concept défini au paragraphe 27 dans le but d'intégrer les données relatives à l'inscription des abonnés et toutes les données relatives aux documents ou aux communications impliquant l'abonné à un service de communication électronique.

45. Les données relatives à l'inscription peuvent être un élément essentiel de la production d'éléments de preuve électronique, en particulier dans le cas d'une communication anonyme, qui renforce la nécessité de connaître le nom, les pièces d'identité et l'adresse de l'abonné.

46. À l'instar de la définition des **organismes publics**, les informations sur l'abonné sont un concept utile aux réglementations ultérieures sur les éléments de preuve électronique (et/ou sur des thèmes connexes comme la responsabilité qui incombe aux fournisseurs de services Internet de conserver et de vérifier les données sur les abonnés). Le fait de le prédéfinir dans la présente loi permet de garantir une signification uniforme lors de son utilisation ultérieure.

47. Le paragraphe 28 traite des **données relatives au trafic** destinées à englober les données pertinentes pour la production d'éléments de preuve électronique relatives à la circulation des communications électroniques. Des renseignements tels que l'origine, l'itinéraire, la destination, la date, l'heure, la taille et la durée sont essentiels pour déterminer l'auteur, le lieu et l'heure de certaines actions, en particulier lorsque les flux de communications électroniques sont divisés en «paquets» qui peuvent prendre des chemins différents pour atteindre la destination voulue, comme sur Internet.

Partie III

TITRE II: RECEVABILITÉ

Article 3: Amendement aux règles d'authentification et de meilleure preuve

48. Cet article a pour objectif principal de déterminer l'intégration de la présente loi dans la Common Law et dans les dispositions réglementaires qui régissent la recevabilité des enregistrements, en précisant que les seules règles modifiées par le texte sont celles ayant trait à l'authentification et à la règle de la meilleure preuve.

49. En indiquant les lois qui sont amendées, l'article implique automatiquement que les lois qui ne sont pas modifiées par le texte doivent aussi s'appliquer aux questions qu'il réglemente. Les questions traitées dans le texte de loi doivent donc être considérées comme un chapitre particulier du domaine de l'application des principes plus généraux de la recevabilité de la preuve.

Article 4: Common Law et règlements

50. L'objectif de cet article est d'établir que, dans leur application de la Common Law et des règlements relatifs à la recevabilité des enregistrements, les tribunaux doivent tenir compte des dispositions de la présente loi dès lors que des enregistrements électroniques doivent être pris en considération. Il est important que les tribunaux reconnaissent la spécificité de cette question et des dispositions prévues par la loi. L'Article 4 est donc destiné à attirer l'attention des magistrats sur la nécessité de l'appliquer.

Article 5: Recevabilité générale des éléments de preuve électronique

51. Cet article établit le principe de la non-discrimination des enregistrements électroniques. Le format électronique d'un enregistrement n'a aucune incidence sur sa fiabilité comme moyen de preuve. Par conséquent, il n'y a aucune raison de faire preuve de discrimination *a priori* à l'encontre des enregistrements électroniques. On peut même dire que certains enregistrements électroniques (dans le cas de signatures numériques certifiées, par exemple) peuvent être plus fiables que des enregistrements non électroniques.

52. L'Article 5 est important en ce sens qu'il établit le principe général de la recevabilité des enregistrements électroniques, sous réserve des conditions énumérées dans les articles suivants.

Article 6: Application de la règle de la meilleure preuve

53. La règle de la meilleure preuve étant un principe juridique traditionnel du système de la Common Law, il est important que la législation relative aux éléments de preuve électronique soit compatible avec ce principe.

54. Afin d'harmoniser l'application de ce principe avec les caractéristiques des ordinateurs, l'Article 6 établit que la règle de la meilleure preuve est considérée satisfaite lorsque l'on peut apporter la preuve de l'intégrité de l'ordinateur sur lequel ou grâce auquel certaines données ont été enregistrées ou stockées.

55. Étant donné que la règle de la meilleure preuve exige de présenter les originaux d'un document donné et qu'il est difficile d'établir si des données électroniques sont des originaux ou une copie, la preuve de l'intégrité d'un ordinateur est une adaptation *mutatis mutandis* de l'intention traditionnelle de cette règle.

56. Cette adaptation procède de raisons juridiques, techniques et économiques. Sur le plan juridique, la philosophie à l'origine de la règle de la meilleure preuve vise à assurer que la meilleure preuve possible est apportée (en temps normal, il s'agit des originaux du document). D'un point de vue technique et économique, il n'est pas possible d'appliquer des technologies et procédures qui pourraient être équivalentes à un original (une signature numérique certifiée, par exemple) à tous les enregistrements électroniques d'un système d'information. Par conséquent, les motifs juridiques, techniques et économiques concourent pour indiquer que l'intégrité prouvée d'un ordinateur constitue la meilleure preuve possible dans des circonstances normales.

57. Les situations qui autorisent la présomption d'intégrité d'un ordinateur sont énumérées au paragraphe 2. Elles se résument aux cas où, *primo*, il est apporté des preuves étayant la conclusion que l'ordinateur fonctionnait correctement, *secundo*, où l'enregistrement électronique a été enregistré ou stocké par une partie adverse à la partie qui cherche à le présenter en justice et, *tertio*, où l'enregistrement électronique a été enregistré ou stocké par une partie extérieure à la procédure qui ne l'a pas enregistré ou stocké sous le contrôle d'une partie cherchant à le présenter. En bref, cette présomption s'applique lorsque le bon fonctionnement de l'ordinateur est prouvé ou lorsque la partie qui cherche à présenter l'enregistrement électronique en justice n'a pas d'intérêt contradictoire ou suspect.

Article 7: Intégrité de l'information et règles particulières de recevabilité

58. La présomption d'intégrité des ordinateurs évoqués en termes généraux dans l'Article 6 se retrouve dans une disposition de l'article 7, dans lequel le paragraphe 2 énumère la liste des situations dans lesquelles l'intégrité d'un enregistrement électronique induit la présomption d'intégrité de l'ordinateur dans une action en justice, indépendamment du fait que l'enregistrement électronique puisse constituer ou non un ouï-dire (en vertu, respectivement, des paragraphes 1 et 3).

59. Cette liste commence par mentionner les enregistrements de transactions (c'est-à-dire les enregistrements électroniques) qui sont restés complets et non modifiés à l'exception des modifications immatérielles découlant des procédures normales de communication, de stockage ou d'affichage. Cette formulation est importante, car il serait difficile de «geler» les ordinateurs et les enregistrements électroniques et de les prémunir de toute modification; elle limite toutefois l'étendue des changements qui pourraient véritablement compromettre la fiabilité d'un enregistrement électronique.

60. La deuxième situation évoquée a trait aux enregistrements certifiés ou signés électroniquement selon une méthode fournie par des organismes de certification agréés. L'utilité d'établir des autorités ou organismes de certification agréés ressort clairement ici, puisque cette accréditation constitue en soi une présomption formelle et contribue donc à induire la présomption d'intégrité de l'enregistrement électronique sur les points importants.

61. La liste se poursuit avec la solution d'une intégrité et d'un contenu notariés, qui constitue une autre option à la disposition des parties intéressées présentant un intérêt dans la mesure où les notaires peuvent apporter foi à l'intégrité et au contenu dont ils sont appelés à être témoins.

62. La quatrième hypothèse porte sur l'enregistrement sur un support non réinscriptible qui, par définition, interdit tout changement dès que l'enregistrement électronique est stocké. Cela peut être une solution pratique et utile pour les parties intéressées recherchant une option aisément accessible et moins coûteuse.

63. La cinquième situation est celle de l'enquête technique dans le cadre d'une action en justice, au cours de laquelle l'expert nommé par le juge peut confirmer l'intégrité de l'enregistrement électronique.

64. La diversité des situations autorisant la présomption d'intégrité d'un enregistrement électronique, qui s'étendent à la présomption d'intégrité d'un ordinateur, est importante, car toutes les parties intéressées doivent avoir accès à différents moyens pratiques de produire des éléments de preuve électronique.

Article 8: Impressions

65. Bien qu'une impression ne soit pas en soi électronique, elle est générée par des moyens électroniques. Par conséquent, si les parties intéressées l'ont constamment acceptée comme représentation authentique de l'enregistrement électronique correspondant, la fiabilité qui peut être induite de ce comportement autorise à conclure que l'impression satisfait la règle de la meilleure preuve. C'est ce qui est prévu par l'Article 8, important dans la mesure où la plupart des gens ont l'habitude d'imprimer les enregistrements électroniques en rapport avec des éléments de preuve électronique.

Article 9: Charge de la preuve de l'authenticité d'une preuve électronique

66. En règle générale, il incombe à la personne cherchant à présenter pour preuve un enregistrement électronique de prouver son authenticité dans le cadre d'une action en justice.

67. Cependant, les personnes plus vulnérables, telles que les consommateurs et les enfants, peuvent être protégées par des dispositions réglementaires inversant la charge de la preuve. Dans ce cas, elles prévalent sur la règle générale établie par l'Article 9.

68. Cette remarque est importante, car les personnes plus vulnérables n'ont généralement pas les moyens techniques et/ou économiques de produire des preuves fondées sur des enregistrements électroniques. Néanmoins, leur accès à la justice et à la possibilité de compter sur une défense appropriée doit être encouragé et garanti.

Article 10: Normes

69. Les pratiques et usages répandus sont des indicateurs importants du comportement que l'on peut attendre en matière d'enregistrement ou de préservation des enregistrements électroniques. Par conséquent, des preuves peuvent se fonder sur des normes, des procédures, des usages ou des pratiques en vigueur qui reflètent ce comportement et qui fournissent des indications sur les attentes en matière de recevabilité des enregistrements électroniques.

70. L'Article 10 traite de la reconnaissance de ces indications et les relie au type d'entreprise ou d'activité auxquelles elles se réfèrent, ainsi qu'à la nature et à la finalité de l'enregistrement électronique. Cette mise en relation est importante, car les normes applicables sur un marché donné peuvent viser des objectifs différents de celles applicables sur un autre marché (comme c'est le cas en matière de sécurité de l'information).

71. L'article s'achève en confiant aux autorités publiques concernées la charge de publier des normes techniques ou de définir des procédures de sécurité offrant une orientation adéquate sur la conformité à l'Article 10. Ce point est important, car les autorités compétentes peuvent et doivent fournir une orientation générale ainsi qu'une orientation personnalisée selon les marchés ou les circonstances, le cas échéant.

Article 11: Témoignages

72. L'Article 11 prescrit que les éléments de preuve électronique puissent être présentés sous la forme de témoignages. Cela constitue une solution supplémentaire de production d'éléments de preuve électronique à la disposition des parties intéressées.

73. Le Groupe de travail a débattu de l'utilité d'inclure d'autres dispositions dans cet article, notamment la déclaration que tout déposant a le devoir de témoigner au mieux de ses connaissances ou convictions, sous peine de sanctions infligées par la Cour dans le cas où son témoignage se révèlerait faux, en plus d'une disposition relative au contre-interrogatoire des témoignages.

74. Étant donné que les enregistrements électroniques sont de nature volatile, le fait de dépendre de témoignages peut constituer un sujet de préoccupation et doit donc être contrebalancé par la mise en avant de la responsabilité du déposant. Cependant, une réglementation en la matière pourrait empiéter sur les normes de procédures existantes. Par conséquent, le groupe de travail a décidé que l'adoption de l'approche mentionnée serait laissée à la discrétion des États bénéficiaires.

Article 12: Accord sur la recevabilité d'une preuve

75. En règle générale, sauf dispositions légales contraires, les parties à une action en justice peuvent s'entendre sur la recevabilité d'un enregistrement électronique donné, sous réserve d'une décision de la Cour.

76. Cette disposition ne s'applique pas aux procédures pénales lorsque les accusés ne bénéficiaient pas d'une assistance ou d'une représentation légales au moment de la conclusion de cet accord.

77. L'importance de l'article 12 tient au fait qu'il favorise les accords privés en évitant des controverses qui pourraient occasionner des retards et des frais de justice inutiles.

Article 13: Signature électronique

78. À l'instar des dispositions de l'Article 5 relatif aux enregistrements électroniques, l'Article 13 établit dans son paragraphe 1 que les signatures électroniques ne doivent pas faire l'objet d'une discrimination au seul motif qu'elles sont sous une forme électronique.

79. Le paragraphe 2 exprime la possibilité de prouver des signatures électroniques par tout moyen. Étant donné la rapidité des progrès technologiques dans le domaine des signatures électroniques et l'importance de respecter le principe de la neutralité technologique, il semble peu probable que l'on puisse circonscrire convenablement les différents moyens de preuve d'une signature électronique.

80. Une illustration de la diversité des moyens de preuve des signatures électroniques est donnée dans le même paragraphe, qui mentionne la preuve de l'existence d'une procédure permettant à une personne d'exécuter un symbole dans le but de vérifier qu'un enregistrement électronique émane bien d'elle (une procédure relativement courante sur les sites Internet, tenant lieu de condition d'accès à certaines parties de ces sites Web).

Article 14: Conditions relatives aux signatures électroniques

81. En vertu du paragraphe 1 de l'article 14, les signatures électroniques remplissent les conditions légales relatives à la signature d'une personne lorsqu'elles sont fiables et appropriées. Il s'agit d'une disposition importante, car les signatures électroniques peuvent effectivement être fiables et appropriées, voire plus, dans certains cas, que les signatures non électroniques.

82. Le paragraphe 3 établit que les parties sont libres de convenir d'utiliser une méthode particulière de signature électronique, sauf dispositions légales contraires. Cette disposition est importante, car elle est conforme aux principes généraux de libre établissement de la preuve, tout en fournissant une remarque qui peut s'appliquer, par exemple, dans les cas où l'utilisation de signatures électroniques cryptographiques pourrait aller à l'encontre des lois relatives au respect de la vie privée des personnes ou à la sécurité nationale.

83. Les parties à un contrat ne sont pas tenues de spécifier le type de signature électronique qu'elles utiliseront. Cette situation étant assez courante en pratique, le paragraphe 4 y répond en fournissant une liste de critères permettant de respecter les exigences conventionnelles en matière de signature électronique des messages de données. On y trouve notamment le lien entre le signataire et les données relatives à la création de signature (qui doivent être sous le contrôle du signataire) et la possibilité de déceler toute altération de la signature électronique au moment de la signature ou après celui-ci.

Article 15: Autres techniques et procédures de production d'éléments de preuve électronique

84. L'article 15 porte sur les autres techniques et procédures de production d'éléments de preuve électronique concernant certains de ces enregistrements électroniques. Il cite, d'une part, l'attestation de notaires, de juges de paix ou d'une autre autorité; d'autre part, l'enregistrement sur un support non réinscriptible; et, enfin, l'informatique légale dans le cadre d'une enquête préalable.

85. La reconnaissance de l'informatique légale, qui est un domaine de compétence spécialisé dans les éléments de preuve électronique, est très importante, en particulier parce qu'elle est associée aux enquêtes préalables; cela ajoute encore à leur fiabilité, puisque l'expert nommé par le juge est censé être un professionnel neutre et qualifié.

TITRE III: DISPOSITIONS GÉNÉRALES

Article 16: Recevabilité des enregistrements électroniques émanant d'autres pays

86. L'Article 16 établit la recevabilité des enregistrements électroniques émanant d'une autre juridiction, sous réserve que l'intégrité de l'ordinateur puisse être prouvée ou présumée selon les mêmes normes que pour la preuve de l'intégrité des enregistrements électroniques émanant de la juridiction nationale (à savoir la preuve que l'ordinateur fonctionnait correctement et que l'intégrité de l'enregistrement électronique était préservée).

87. Cette disposition est importante pour l'échange sécurisé de communications électroniques avec d'autres pays, indispensable à l'extension des intérêts de l'État bénéficiaire aux transactions et aux communications électroniques avec d'autres pays.

88. Étant donné que chaque pays a ses propres règles en matière d'éléments de preuve électronique, la définition d'une condition minimum imposant simplement la preuve de l'intégrité de l'ordinateur ou de l'enregistrement électronique peut faciliter la tâche d'établir un dénominateur commun.

Article 17: Reconnaissance des documents et signatures électroniques étrangers

89. Si l'Article 16 porte sur les dossiers électroniques émanant d'autres pays, le paragraphe 2 de l'Article 17 porte, lui, sur les informations électroniques situées dans d'autres pays.

90. Ce paragraphe énumère les situations appelant au traitement équivalent des informations situées dans une juridiction étrangère par rapport aux informations situées dans la juridiction nationale. Parmi celles-ci figurent une décision de la Cour en ce sens et l'existence de traités internationaux garantissant la reconnaissance nécessaire.

91. Cette disposition est importante, car elle peut renforcer la sécurité des échanges de communications et de transactions électroniques entre l'État bénéficiaire et d'autres pays. Étant donné qu'il peut s'avérer plus difficile d'accéder à des enregistrements électroniques situés à l'étranger en vue de vérifier leur intégrité, cette disposition prévoit des procédures et des situations permettant de surmonter les éventuelles contraintes techniques.

Article 18: Interprétation conforme aux principes acceptés sur le plan international

92. En vertu de l'Article 18, le texte de loi doit être interprété et appliqué à la lumière des principes, acceptés sur le plan international, de la neutralité technologique et de l'équivalence fonctionnelle.

93. Ces principes ont été adoptés par presque tous les pays ayant réglementé les éléments de preuve électronique et leurs aspects connexes. Le principe de la neutralité technologique favorise l'inclusion numérique et sociale, car il améliore la possibilité de développer ou d'utiliser des technologies comparables, permettant ainsi d'élargir l'accès à celles-ci et d'en baisser les prix. Selon le principe de l'équivalence fonctionnelle, il ne peut être imposé aucune restriction à l'environnement en ligne qui ne soit présente dans l'univers hors ligne, ce qui tend à stimuler la migration des communications et des transactions vers l'environnement en ligne.

94. L'importance de cette disposition tient au fait qu'elle établit que ces principes s'appliquent à toutes les dispositions du texte et qu'ils doivent influencer son interprétation et son application en vue d'atteindre les objectifs sociaux et économiques visés par ces principes.

Article 19: Réglementation

95. L'Article 19 autorise le Ministre compétent à réglementer l'entrée en vigueur des dispositions du texte de loi et toute prescription requise ou autorisée par celui-ci; il ajoute que le Ministre pourra tenir compte des bonnes pratiques et des normes internationales en la matière.

96. L'objectif de cet article est de reconnaître l'utilité d'une réglementation complémentaire afin d'assurer l'application appropriée du texte de loi et d'attirer l'attention sur cette utilité.

97. À cet égard, le Groupe de travail a discuté des sujets qui devaient relever des traités internationaux ou de la réglementation nationale.

98. Il a été conclu que des sujets tels que le système d'accréditation pour les signatures électroniques (y compris l'authentification, la certification et l'accréditation des signatures électroniques, des attributs et de l'heure), l'incorporation dans les lois de procédure (pour garantir par exemple que l'exécution des recherches et des saisies, l'ordonnance de production, la collecte en temps réel, les interrogatoires en vidéoconférence, les procédures judiciaires électroniques, la conservation rapide des données et l'interception de communications sont conformes à la présente loi) et l'intégration dans le droit matériel connexe (sur la conservation des données, la responsabilité des prestataires de services Internet et la cybercriminalité, entre autres) devaient retenir l'attention des organismes de réglementation nationaux.

99. Il a été estimé que des tendances problématiques telles que l'informatique dans le nuage, la stéganographie, le liveCD, etc., susceptibles de constituer un sujet de préoccupation en matière de production et de reconnaissance des enregistrements électroniques, méritaient des études particulières. La réalisation de ces études, tout comme la réglementation mentionnée, sont importantes, car sans cela l'application du texte de loi pourrait s'en trouver affaiblie ou obsolète.

100. L'élaboration de lois régionales et l'harmonisation avec les traités internationaux ont été jugées utiles pour l'État bénéficiaire afin de garantir une coopération formelle avec d'autres pays ainsi qu'un suivi et un alignement réguliers sur les bonnes pratiques internationales actualisées. Cette élaboration et cette harmonisation sont importantes, car sans cela le texte de loi pourrait être limité dans son application ou réduit à une coopération «informelle».

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	Bureau du Premier ministre	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 TI, 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
Saint-Vincent-et-les-Grenadines	Ministère des Télécommunications, des Sciences, de la Technologie et de l'Industrie	FRASER	Suenel

Annexe 1

Pays	Organisation	Nom	Prénom
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[6]	J Paul
PRESCOD	Kwesi

[6] 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
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

Annexe 2

Pays	Organisation	Nom	Prénom
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 Services 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[7]	J Paul
PRESCOD	Kwesi

[7] Président de l'Atelier.