

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

Transactions électroniques:

Modèles de lignes directrices politiques
et de textes législatifs

HIPCAR

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



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

Transactions électroniques:

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 prêté à ce problème, depuis les débuts du projet HIPCAR en décembre 2008. Une fois les priorités communes arrêtées, des groupes de travail réunissant des parties prenantes ont été créés pour agir concrètement. Les besoins propres à la région ont ensuite été définis, de même que les pratiques régionales pouvant donner de bons résultats, qui ont été comparées aux pratiques et normes établies dans d'autres régions du monde.

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

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



Brahima Sanou
Directeur du BDT

Remerciements

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

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

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

Le comité de pilotage du projet HIPCAR, présidé par l'Union des télécommunications des Caraïbes (CTU), a fourni conseils et assistance à une équipe de consultants incluant M. Gilberto Martins de Almeida, M. Kwesi Prescod et Mme Karen Stephen-Dalton. Le projet de document a ensuite été révisé, discuté et adopté par un large consensus des participants lors des deux ateliers de consultation du Groupe de travail du projet HIPCAR sur les questions relatives à la société de l'information, qui se sont déroulés à Sainte-Lucie du 8 au 12 mars 2010 et à la Barbade du 23 au 26 août 2010 (voir Annexes). Les Notes explicatives du modèle de texte législatif incluses dans ce document ont été préparées par M. Gilberto Martins 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 oeuvre 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, et de M. Michael Tetelman. M. Pau Puig Gabarró a réalisé une partie du pré-formatage et l'équipe du Service de composition des publications de l'UIT a été chargée de sa publication.

Table des matières

	<i>Page</i>
Avant-propos	i
Remerciements	iii
Table des matières	v
Introduction	1
1.1. Le projet HIPCAR – objectifs et bénéficiaires	1
1.2. Comité de pilotage du projet et groupes de travail	1
1.3. Mise en œuvre et contenu du projet	2
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.....	3
1.5. Ce rapport.....	7
1.6. Importance de l’efficacité des politiques et des lois sur les transactions électroniques	8
Partie I: Modèle de lignes directrices politiques – Transactions électroniques	11
Partie II: Modèle de texte législatif – Transactions électroniques	17
Organisation des articles.....	17
TITRE I – PRÉAMBULE.....	18
TITRE II – TRANSACTIONS ÉLECTRONIQUES.....	22
TITRE III – PROTECTION DES CONSOMMATEURS.....	29
TITRE IV – INTERMÉDIAIRES ET FOURNISSEURS DE SERVICES DE TÉLÉCOMMUNICATION	32
Partie III: Notes explicatives relatives au modèle de texte législatif sur les transactions électroniques 35	
INTRODUCTION	35
COMMENTAIRE DES ARTICLES	36
TITRE I – PRÉAMBULE.....	36
Article 2. Objectifs	36
Article 3. Définitions	36
Article 4. Exclusions	40
TITRE II – TRANSACTIONS ÉLECTRONIQUES.....	40
Article 5. Principe de non-discrimination	40
Article 6. Prescription d’une forme non électronique.....	40
Article 7. Exigences écrites	41
Article 8. Exigences relatives à la signature.....	41
Article 9. Exigences de reconnaissance, d’authentification, de certification notariée et de vérification.....	42
Article 10. Exigence de production d’un document original	42

Article 11. Conservation de documents écrits	43
Article 12. Intégrité des informations ou de l'enregistrement de la transaction.....	43
Article 13. Reconnaissance des documents et des signatures étrangers.....	44
Article 14. Contrats électroniques.....	44
Article 15. Contrats électroniques automatisés	45
Article 16. Effets d'une erreur lors des transactions avec un agent électronique	45
Article 17. Manifestations de volonté	45
Article 18. Heure et lieu de réception des communications électroniques	45
Article 19. Attribution des communications électroniques.....	46
Article 20. Autres règles de droit non modifiées.....	47
Article 21. Consentement.....	47
TITRE III – PROTECTION DES CONSOMMATEURS.....	48
Article 22. Données obligatoires	48
Article 23. Délai de réflexion	49
Article 24. Messages commerciaux non sollicités	49
TITRE IV – INTERMÉDIAIRES ET FOURNISSEURS DE SERVICES DE TÉLÉCOMMUNICATION	50
Article 25. Responsabilité	50
Article 26. Procédure de traitement des avis d'actes illégaux	51
Article 27. Offre de biens et de services dans un environnement sûr	51
ANNEXES.....	53
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.....	53
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	55

Introduction

1.1. Le projet HIPCAR – objectifs et bénéficiaires

Le projet HIPCAR¹ a été officiellement lancé dans les Caraïbes par la Commission européenne (CE) et l'Union internationale des télécommunications (UIT) en décembre 2008, en étroite collaboration avec le Secrétariat de la Communauté des Caraïbes (CARICOM) et l'Union des télécommunications des Caraïbes (CTU). Il fait partie intégrante d'un projet-cadre, le projet UIT-CE-ACP, qui englobe également les pays de l'Afrique subsaharienne et du Pacifique.

L'objectif du projet HIPCAR consiste à aider les pays du CARIFORUM² à harmoniser leurs politiques, leur législation et leurs procédures réglementaires en matière de technologies de l'information et de la communication (TIC), de façon à créer un environnement favorable au développement et à la connectivité des TIC, faciliter l'intégration des marchés, favoriser l'investissement dans l'amélioration des capacités et des services liés aux TIC et améliorer la protection des intérêts des consommateurs de TIC dans l'ensemble de la région. L'objectif final du projet est d'accroître la compétitivité et le développement socio-économique et culturel dans la région des Caraïbes au travers des TIC.

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

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

1.2. Comité de pilotage du projet et groupes de travail

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

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

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

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

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

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

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

1.3. Mise en œuvre et contenu du projet

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

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

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

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

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

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

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

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

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

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

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

Six modèles de cadres étroitement liés

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

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

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

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

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

Élaboration des modèles de textes législatifs

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

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

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

D'après les résultats des analyses de droit comparé, les parties prenantes régionales ont élaboré des principes politiques de départ qui, une fois approuvés par les parties prenantes, ont formé les bases d'une délibération politique approfondie et de l'élaboration des textes législatifs. Ces principes politiques ont confirmé certains sujets et tendances communs retrouvés dans la jurisprudence internationale, mais ont également identifié des considérations particulières qui devront être incluses dans le contexte d'une région constituée de petits États souverains insulaires en développement. La question de la capacité

institutionnelle pour faciliter l'administration appropriée de ces nouveaux systèmes constitue un exemple de considération circonstancielle majeure ayant eu un effet sur les délibérations à ce stade du processus et à d'autres.

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

Interaction et chevauchement de la couverture des modèles de textes

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

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

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

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

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

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

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

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

En conclusion

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

Étant donné les natures spécifiques et étroitement liées des modèles de textes du projet HIPCAR, les pays bénéficiaires du projet auraient tout intérêt à élaborer et mettre en place une législation fondée sur ces modèles de façon coordonnée. Les modèles consacrés au commerce électronique (transactions et preuves) fonctionnent plus efficacement avec l'élaboration et l'adoption simultanées des cadres relatifs à la cybercriminalité et à l'interception de communications, si étroitement liés et dépendants les uns des autres, pour résoudre les questions d'un développement réglementaire solide. De la même façon, les

cadres relatifs à l'accès à l'information publique et au respect de la vie privée et à la protection des données présentent de telles synergies en termes de cadres administratifs et d'exigences de compétences fondamentales que leur adoption simultanée ne peut que renforcer leur mise en œuvre.

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

1.5. Ce rapport

Le présent rapport traite du Commerce électronique (Transactions), l'un des domaines de travail du Groupe de travail sur le cadre politique et législatif des TIC sur les questions relatives à la société de l'information. Il se compose d'un modèle de lignes directrices politiques et d'un modèle de texte législatif, y compris de Notes explicatives, que les pays des Caraïbes pourraient souhaiter utiliser lors de l'élaboration ou de la modernisation de leurs politiques et de la législation nationales dans ce domaine.

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

Cette évaluation régionale, publiée séparément en complément du présent rapport³, a impliqué une analyse comparative de la législation en vigueur en matière de transactions électroniques 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 reflète des bonnes pratiques et normes nationales, régionales et internationales et garants de la compatibilité avec les traditions juridiques des Caraïbes, les modèles présentés dans ce rapport ont pour but de répondre aux besoins spécifiques de la région.

Le Comité de pilotage du projet HIPCAR, présidé par l'Union des télécommunications des Caraïbes (CTU), a apporté conseils et soutien à une équipe de consultants, composée notamment de M. Gilberto Martins de Almeida, M. Kwesi Prescod et Mme Karen Stephen-Dalton. Le modèle de texte législatif sur les transactions électroniques a été élaboré en trois phases, à l'origine par les consultants pour le projet HIPCAR: (1) la rédaction d'un rapport d'évaluation; (2) l'élaboration du modèle de lignes directrices politiques et (3) la rédaction du modèle de texte législatif. Les projets de documents ont ensuite été révisés, finalisés et adoptés 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 s'est déroulé à Sainte-Lucie du 8 au 12 mars 2010 et à la Barbade du 23 au 26 août 2010 (voir Annexes). Les Notes explicatives pour le modèle de texte législatif incluses dans ce document ont été préparées par M. Gilberto Martins de Almeida en abordant, entre autres, les points soulevés lors du second atelier. Ce document contient donc des données et informations à jour 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.

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

1.6. Importance de l'efficacité des politiques et des lois sur les transactions électroniques

Dans le monde de la mondialisation économique, les échanges nationaux et internationaux connaissent un développement et une imbrication croissants. Pour l'essentiel, leur réalisation et leur intégration s'effectuent par l'intermédiaire de transactions électroniques qui permettent la circulation instantanée d'affaires sur n'importe quel marché. La confiance requise pour ce type d'affaires repose en particulier sur l'existence de droit statutaire spécifique qui établit les conditions d'une applicabilité pertinente. L'absence d'une telle législation prive le commerce électronique d'un environnement juridique sûr.

Banque en ligne, courtage électronique de titres, compensation et garde de données électroniques commerciales ou financières, paiements mobiles, commandes électroniques de placements financiers et conclusions de contrats de change bancaires électroniques liés à l'exportation représentent quelques-unes des innombrables situations que les communautés locales et internationales s'attendent à voir couvertes par les lois du commerce électronique.

Cette attente s'est traduite dans la conclusion de conventions internationales⁴ et de lois types⁵ spécifiques qui visent à inspirer les dispositions juridiques correspondantes dans chaque pays et à éviter les différences importantes dans les réglementations de chaque pays. La cohérence avec ce type de cadres de base est devenue une condition indispensable à l'existence d'une plate-forme juridique appropriée pour le commerce électronique.

Les modèles de lignes directrices politiques et de textes législatifs présentés dans ce document ont été rédigés conformément aux cadres susmentionnés de façon à fournir aux pays bénéficiaires du projet HIPCAR des projets de lignes directrices qui correspondent raisonnablement aux bonnes pratiques internationales.⁶

En outre, le commerce électronique⁷ constitue aujourd'hui une composante essentielle de la croissance économique, en garantissant l'actualité et l'exactitude des transactions contractuelles et financières. Cela permet, entre autres, la mise en œuvre de services de cybergouvernance, améliorant la qualité et réduisant les coûts des services, en augmentant la transparence et l'efficacité de l'approvisionnement et de la vente des biens et des services.

Pour que les pays bénéficiaires puissent faciliter l'innovation et renforcer leur compétitivité en devenant des acteurs actifs du commerce électronique, ils doivent créer un environnement permettant les transactions électroniques et capable d'assurer l'égalité des chances tout en offrant une protection juridique aux consommateurs, ainsi qu'aux acteurs du commerce et de l'industrie qui opèrent dans un environnement mondial.

Reconnaissant la capacité du droit des contrats traditionnels à s'adapter et à résister aux demandes changeantes du commerce, les organisations internationales qui ont entrepris de définir des modèles de cadres pour les transactions électroniques ont adopté une stratégie de définition de ce domaine et d'établissement d'équivalences juridiques avec les principaux aspects du processus de formation des contrats. Ainsi, la vaste jurisprudence du droit des contrats reste inchangée et applicable.

⁴ En particulier, la *Convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux*, 2005, signée par un certain nombre de pays, des plus grands comme la Chine et la Fédération de Russie, aux plus petits comme la Colombie, le Honduras, Madagascar, le Monténégro, Panama, le Sénégal, la Sierra Léone et le Sri Lanka.

⁵ Notamment la *Loi type du Commonwealth relative aux preuves électroniques*, dont le champ d'application s'étend pour couvrir certains aspects du commerce électronique.

⁶ Le modèle final du texte législatif reflétait également le consensus atteint parmi les pays bénéficiaires du projet HIPCAR fondé sur la perception de leurs exigences communes. La rédaction ou la révision qui s'ensuivront de la législation de chaque pays pourraient fournir l'occasion de mieux adapter le modèle aux besoins locaux, d'améliorer sa cohérence avec les normes internationales, ou d'envisager des réserves sur certains des sujets qu'il couvre.

⁷ Le commerce électronique peut avoir des significations et des portées différentes, notamment l'établissement de contrats électroniques, la communication électronique de contrats conclus hors ligne, les paiements électroniques et la fourniture de services publics électroniques.

Plusieurs organisations internationales ont favorisé l'élaboration de cadres législatifs pour le commerce électronique, notamment:

- le *Commonwealth*, dont la plupart des pays bénéficiaires du projet HIPCAR font partie, a élaboré une *Loi type relative aux preuves électroniques* qui aide à établir la reconnaissance de normes communément admises particulièrement pertinentes pour le commerce électronique.
- la *Commission des Nations Unies pour le droit commercial International (CNUDCI)*, mise en place par l'Organisation des Nations Unies (ONU) en 1966 afin d'harmoniser le droit commercial international. Principal organe juridique travaillant à créer des lois commerciales accessibles, prévisibles et unifiées, la Commission a favorisé des lois types concernant spécifiquement les transactions électroniques, ainsi que la Convention internationale susmentionnée.
- l'*Organisation de coopération et de développement économiques (OCDE)* a facilité la création d'instruments, de décisions et de recommandations internationaux qui offrent également des conseils aux pays opérant dans une économie mondialisée.
- les directives de la *Commission européenne* visent à permettre à des cadres législatifs harmonisés de soutenir, entre autres, les échanges transfrontaliers de biens et de services parmi les États membres. La *Directive sur le commerce électronique* et la *Directive sur la signature électronique* fournissent le cadre juridique global dans ce domaine pour ce bloc commercial.

Les éléments les plus importants de la loi sur le commerce électronique sont liés aux composantes fondamentales des transactions commerciales et consistent à savoir comment s'assurer qu'un contrat en ligne est aussi valide et applicable qu'un contrat conclu hors ligne. Les principes de base de la loi sur le commerce électronique s'attachent par conséquent à faire respecter la validité des contrats électroniques et à s'assurer que les parties sont tenues de respecter leurs accords. Une fois les questions contractuelles résolues, l'analyse du droit du commerce électronique se déplace sur une série de questions juridiques susceptibles de régir la transaction. Ces questions incluent la juridiction (c.-à-d., la cour ou le tribunal arbitral compétent pour juger une affaire), les questions de protection du consommateur, la fiscalité, le respect de la vie privée, les litiges relatifs à des noms de domaines, ainsi que le rôle et la responsabilité potentielle des intermédiaires tels que les fournisseurs de services Internet.

L'un des principaux facteurs à prendre en considération lors de la détermination de l'équivalence électronique-papier concerne la question de l'authenticité des documents électroniques et l'utilisation des technologies de signature appropriées pour garantir cette authenticité. L'administration des fournisseurs de ces services est donc essentielle pour garantir, au commerce et aux consommateurs, la fiabilité des transactions du commerce électronique. Pour les décideurs politiques, la difficulté est de trouver le bon équilibre entre l'impératif consistant à instaurer la confiance et la réalité du dynamisme technologique, la disponibilité des capacités internes et la nature mondiale du marché.

- Pour créer un environnement juridique plus sûr, il est impératif de supprimer tous les obstacles juridiques qui empêchent l'utilisation des communications électroniques pour communiquer des informations ayant une valeur juridique. Lors de l'établissement d'un cadre législatif pour le commerce électronique, la législation doit rester neutre d'un point de vue technologique et ne pas se limiter à des solutions technologiques spécifiques. Elle doit également être souple et adaptée afin d'être en harmonie avec les développements qui interviennent dans les règles et les lignes directrices internationales. En outre, les principes fondamentaux de la loi doivent rester intacts, et la législation doit contribuer à établir la confiance dans le commerce électronique en offrant protection et respect de la vie privée aux consommateurs.

Partie I: Modèle de lignes directrices politiques – Transactions électroniques

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

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

- Il existe une définition pour «électronique» dont l'application prévoit la neutralité technologique.
- Il existe un ensemble de réglementations connexes soumises à une construction judiciaire et à une révision régulière au niveau de l'État visant à déterminer la forme et la technologie qui permettent la validité d'un enregistrement ou d'un document.
- Il existe une définition claire des parties qui seront jugées légitimes pour les transactions conduites par des moyens électroniques, notamment l'expéditeur et le destinataire d'une communication.
- Il existe une définition claire des personnes qui seront considérées comme des «intermédiaires» dans la facilitation d'une transaction réalisée à l'aide de moyens électroniques.
- Il existe une distinction entre les «intermédiaires» et les «prestataires de services de télécommunication» nécessitant de tenir compte des contextes lorsque la terminologie désigne une entité unique ou des entités distinctes.
- Il existe une détermination des obligations de toutes les parties légitimes impliquées dans une transaction électronique, notamment le fournisseur de services Internet et/ou l'intermédiaire, l'expéditeur d'une communication et le destinataire d'une communication.
- Il existe des définitions claires des termes «système d'information» et/ou «ordinateur» en conformité avec les autres cadres juridiques en rapport avec la société de l'information.
- Il existe des définitions claires des termes «enregistrement» et/ou «message de données» permettant d'assurer une distinction conceptuelle entre les deux termes.
- Il existe une définition claire du terme «signature électronique» qui est:
 - neutre sur le plan technologique et différente d'une «signature électronique avancée» ou d'une «signature numérique», qui doit également être neutre sur le plan technologique.
 - claire pour ce qui concerne la distinction entre une signature électronique en tant qu'outil d'authentification des données opposé à l'identification de l'identité.
- Il existe une définition claire des termes «certificat» ou «certificat qualifié» et de la pertinence d'un tel certificat dans le contexte du signataire et des signatures électroniques avancées dans la société de l'information. Il existe une définition claire du «fournisseur de services de certification», de son rôle et de ses fonctions par opposition à celles d'une «autorité de certification».

2. LES PAYS DE LA CARICOM/DU CARIFORUM VISERONT À ÉTABLIR LE CADRE NÉCESSAIRE POUR DOTER LES DOCUMENTS ET LES TRANSACTIONS ÉLECTRONIQUES D'UN EFFET JURIDIQUE

- Une disposition de la loi stipule explicitement que l'État est tenu de respecter la loi/le mandat statutaire qui établit le cadre pour les transactions électroniques.
- La loi/le mandat statutaire stipule explicitement que l'utilisation de moyens électroniques dans l'exécution d'un contrat ou d'une transaction doit être une volonté des deux parties et que les conditions relatives à la formation des contrats peuvent être modifiées pour une transaction donnée sous réserve d'accord des deux parties.
- La loi/le mandat statutaire prévoit de déduire le consentement d'une personne de ses actes antérieurs. Le principe de déduction du consentement ne s'applique pas dans le cas des Pouvoirs publics, qui sont obligés d'indiquer explicitement leur consentement.
- La loi/le mandat statutaire précise les types de transactions ou les types de documents pour lesquels le cadre de transactions électroniques restera sans effet. Les types de transactions ou de documents susceptibles d'être visés par une exception doivent être caractérisés comme étant d'une valeur particulière en raison de leur existence singulière. Il peut donc s'agir:
 - d'instruments de succession, notamment des testaments et fiducies;
 - de contrats de vente ou de transfert de biens immobiliers;
 - d'instruments accordant une procuration.
- La loi/le mandat statutaire prévoit la modification de la liste des exceptions par le parlement.
- Un ensemble de réglementations envisage l'inclusion progressive des exceptions actuelles sous réserve de répondre à des exigences juridiques particulières fixées par l'instance publique compétente au sein d'une juridiction.
- Il convient de prévoir un Règlement doté de lignes directrices pour que toutes les institutions qui s'engagent dans les transactions électroniques satisfassent aux normes techniques appropriées pour le cryptage, l'authentification, la sauvegarde, la récupération et l'élimination des données.

3. LES PAYS DE LA CARICOM/DU CARIFORUM DÉFINIRONT LES NORMES QUE LES DOCUMENTS ÉLECTRONIQUES DOIVENT RESPECTER POUR ÊTRE CONSIDÉRÉS COMME JURIDIQUEMENT VALABLES

- La loi/le mandat statutaire doit être de nature habilitante et s'abstenir de comporter des dispositions trop prescriptives.
- La loi/le mandat statutaire dispose que la validité des documents électroniques ne peut leur être contestée uniquement parce qu'ils sont de nature électronique.
- La loi/le mandat statutaire dispose que l'effet juridique des informations ne peut leur être contesté uniquement parce que ces informations sont mentionnées, mais ne font pas partie d'un document électronique.
- La loi/le mandat statutaire prévoit qu'un document électronique est considéré comme juridiquement valable s'il peut garantir son authenticité en restant fondamentalement inchangé et être conservé par la partie destinataire.
- La loi/le mandat statutaire prévoit qu'un document électronique juridiquement valable et satisfaisant à toutes les exigences légales ou au principe de légalité présente les informations par écrit.
- La loi/le mandat statutaire prévoit qu'un document électronique juridiquement valable est recevable avec valeur probante appropriée.

- La loi/le mandat statutaire prévoit qu'un document électronique satisfaisant à toutes les obligations statutaires ou au principe de légalité et nécessitant la présentation d'informations sous leur forme d'origine si l'information a initialement été collectée par des moyens électroniques et s'il existe une garantie fiable que l'information reste inchangée. La loi/le mandat statutaire prévoit la norme de fiabilité à évaluer selon les fins pour lesquelles l'information est requise.
- La loi/le mandat statutaire prévoit qu'un document électronique incluant une signature électronique valable sera considéré comme un document électronique valable et tout aussi applicable qu'un document ne contenant pas de signature électronique.

4. LES PAYS DE LA CARICOM/DU CARIFORUM DÉFINIRONT DES CONSIDÉRATIONS PAR DÉFAUT À APPLIQUER DANS LA FORMATION DES CONTRATS PAR DES MOYENS ÉLECTRONIQUES

- La loi/le mandat statutaire doit être de nature habilitante et s'abstenir de comporter des dispositions trop prescriptives.
- La loi/le mandat statutaire doit présumer qu'un document électronique ou un message de données est envoyé par l'expéditeur lorsqu'il existe des raisons suffisantes de penser que le document ou le message a été envoyé par l'expéditeur ou par une personne ou un agent électronique agissant au nom de l'expéditeur.
- La loi/le mandat statutaire doit présumer qu'un document ou un message électroniques est reçu, dans les cas généraux dans lesquels il peut y avoir accord ou non entre les parties à propos de l'envoi d'avis d'accusé de réception.
- La loi/le mandat statutaire doit fournir des orientations générales quant aux conditions à satisfaire lorsque l'une des deux parties peut ne pas appliquer la présomption générale de l'attestation.
- La loi/le mandat statutaire doit prévoir de déterminer que l'heure à laquelle un message électronique de données est considéré avoir été envoyé est l'heure indiquée comme étant celle où le message a quitté le système d'information ou la ressource sous le contrôle de l'expéditeur.
- La loi/le mandat statutaire doit prévoir de déterminer que l'heure à laquelle un message électronique de données est considéré reçu est l'heure indiquée comme étant celle où le message a pénétré dans un système d'information ou une ressource sous le contrôle de l'expéditeur.
- La loi/le mandat statutaire doit prévoir de déterminer l'adresse effective de l'une ou l'autre des parties, l'expéditeur ou le destinataire, dans une transaction électronique.
- La loi/le mandat statutaire prévoit la façon dont les erreurs de préparation ou de transmission d'un document électronique ou d'un message de données doivent être traitées, en tenant particulièrement compte:
 - du cas général dans lequel l'erreur est notée avant l'adoption de toute mesure ultérieure par l'une ou l'autre des parties;
 - du cas général dans lequel l'erreur est notée après que l'une ou l'autre partie a adopté une mesure ultérieure, mais avant que cette mesure puisse raisonnablement être inversée par les mesures prises par les parties;
 - du cas général dans lequel l'erreur est notée après l'adoption d'une mesure ultérieure qui peut difficilement être inversée.

5. LES PAYS DE LA CARICOM/DU CARIFORUM ÉTABLIRONT DES CADRES POUR L'UTILISATION DES SIGNATURES ÉLECTRONIQUES ET PRÉVOIRONT LA BONNE ADMINISTRATION DES PRESTATAIRES DE CES SERVICES DANS LEURS JURIDICTIONS

- La loi/le mandat statutaire doit être neutre sur le plan technologique.
- La loi/le mandat statutaire s'assure que les signatures électroniques sont liées à l'authentification des données ou des informations contenues dans un document ou un enregistrement électroniques.
- La loi/le mandat statutaire identifie les signatures électroniques de façon à fournir une large applicabilité des technologies, tout en réalisant l'objectif:
 - d'identifier convenablement le signataire et d'indiquer l'approbation des signataires des informations auxquelles la signature est liée; et
 - de garantir une fiabilité adéquate aux fins pour lesquelles elle a été utilisée.
- La loi/le mandat statutaire indique clairement l'obligation de la personne qui se fie à une signature électronique d'en vérifier la fiabilité.
- La loi/le mandat statutaire peut préciser les types de signatures électroniques «avancées», qui sont plus sophistiquées par nature et nécessitent des tests d'applicabilité plus poussés. L'identification de ces signatures électroniques avancées doit autant que possible s'abstenir de recourir à des technologies ou des méthodologies spécifiques de signature numérique.
- La loi/le mandat statutaire peut spécifier une reconnaissance supérieure des capacités d'authentification des signatures électroniques avancées. Lorsque cette reconnaissance existe, la loi/le mandat statutaire détermine des exigences légales spécifiques que seules les signatures avancées doivent satisfaire.
- La loi/le mandat statutaire prévoit la reconnaissance des «certificats» qui fournissent l'attribution de signatures électroniques à des signataires particuliers dans des conditions données. La loi/le mandat statutaire prévoit une validité supérieure pour les certificats considérés comme étant délivrés conformément aux normes et pratiques du secteur afin de renforcer la fiabilité associée aux signatures électroniques avancées.
- La loi/le mandat statutaire prévoit la reconnaissance des certificats délivrés par les parties quel que soit le lieu de délivrance du certificat ou le lieu d'établissement de la partie.
- La loi/le mandat statutaire prévoit, au sein de la juridiction, l'établissement de personnes qui fournissent des services de génération de signatures électroniques à des tiers, ainsi que de génération, de délivrance et de gestion des certificats qui y sont associés (ci-après désignés comme les «fournisseurs de services de certification»).
- La loi/le mandat statutaire limite au strict nécessaire les obstacles non tarifaires à l'entrée de ces fournisseurs de services afin d'assurer la surveillance d'une pratique commerciale générale appropriée.
- La loi/le mandat statutaire prévoit la définition d'exigences opérationnelles appropriées afin de garantir la confiance du public dans les activités des fournisseurs de services de certification établis dans la juridiction.
- La loi/le mandat statutaire s'assure que le fournisseur de service délivrant un certificat est responsable des éventuels dommages causés par la confiance en ce certificat lorsque les lignes directrices relatives à une utilisation appropriée du certificat sont respectées par la personne qui se fie au certificat.
- La loi/le mandat statutaire peut créer un organisme désigné chargé de vérifier en permanence la conformité du fonctionnement des fournisseurs de services établis dans la juridiction au regard des bonnes pratiques industrielles et commerciales .

6. LES PAYS DE LA CARICOM/DU CARIFORUM PRÉVOIENT LES EXIGENCES MINIMALES S'APPLIQUANT AUX PERSONNES QUI COMMERCENT À L'AIDE DE MOYENS ÉLECTRONIQUES AFIN DE FACILITER UNE PROTECTION ADÉQUATE DES CONSOMMATEURS DANS UN ENVIRONNEMENT ÉLECTRONIQUE

- La loi/le mandat statutaire oblige les personnes qui offrent des biens et des services à échanger (les «vendeurs») par l'intermédiaire de moyens électroniques, à fournir un minimum d'informations au consommateur, notamment:
 - La dénomination, l'adresse géographique principale et les formes de contacts du vendeur,
 - les détails spécifiques des articles proposés à la vente ou du service offert;
 - les conditions et moyens de paiement;
 - les moyens par lesquels les requêtes peuvent être présentées et les litiges résolus.
- La loi/le mandat statutaire oblige les vendeurs qui font du commerce par l'intermédiaire de moyens électroniques à fournir au consommateur la possibilité, avant l'achèvement d'une transaction, d'examiner un résumé de l'accord de vente, notamment la vérification et/ou la correction des objets de la transaction.
- La loi/le mandat statutaire fournit au consommateur la possibilité d'annuler sans pénalité tout contrat passé avec un vendeur qui ne fournit pas l'occasion d'examiner, de vérifier et/ou de corriger l'accord électronique avant l'achèvement dudit accord.
- La loi/le mandat statutaire oblige les personnes qui envoient des communications commerciales non sollicitées aux consommateurs à leur offrir explicitement la possibilité d'accepter ou de refuser de recevoir ce type de communications de ces personnes.

7. LES PAYS DE LA CARICOM/DU CARIFORUM ÉTABLISSSENT LE CADRE DE RESPONSABILITÉ DES INTERMÉDIAIRES D'UNE TRANSACTION ÉLECTRONIQUE

- La loi/le mandat statutaire reconnaît l'existence de parties, dénommées intermédiaires, qui facilitent les transactions électroniques entre deux parties, sans être elles-mêmes impliquées dans l'objet du contrat. Ces personnes incluent les prestataires de télécommunication, les hébergeurs de sites Internet et les hébergeurs d'applications.
- La loi/le mandat statutaire distingue l'intermédiaire ou le prestataire de télécommunication des parties impliquées dans les transactions par leur intermédiaire en les considérant comme un simple canal: un agent passif qui fournit le transport, le stockage ou d'autres services techniques automatiques qui ne modifient en rien le contenu du document électronique.
- La loi/le mandat statutaire prévoit l'exonération de la responsabilité de l'intermédiaire de toute sanction civile ou pénale associée à un document électronique pour lequel il n'a eu d'autre rôle que celui d'un simple canal.
- La loi/le mandat statutaire oblige l'intermédiaire à signaler aux autorités compétentes tous les cas dans lesquels il croit ou a des raisons de croire qu'un document électronique pour lequel il agit comme un canal enfreint une loi.
- La loi/le mandat statutaire peut identifier l'enregistrement pertinent que l'intermédiaire doit produire dans le cas où une enquête serait menée sur ses agissements concernant un document électronique donné.
- La loi/le mandat statutaire prévoit la limitation de la responsabilité d'un intermédiaire dans toute poursuite civile dans le cas où, de bonne foi, l'intermédiaire supprime ou rend indisponible un document électronique qui était conservé dans ses locaux en vertu d'une ordonnance de la Cour, ou dans le cas où il aurait connaissance d'une activité illégale.
- La loi/le mandat prévoit la responsabilité de l'intermédiaire lorsqu'il existe des motifs raisonnables de penser que ladite partie est responsable de l'interférence d'une transmission électronique.

Partie II:

Modèle de texte législatif – Transactions électroniques

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

Organisation des articles

TITRE I. PRÉAMBULE	18
1. Titre abrégé	18
2. Objectif	18
3. Définitions	18
4. Exclusions	21
TITRE II. TRANSACTIONS ÉLECTRONIQUES	22
5. Principe de non-discrimination.....	22
6. Prescription d'une forme non électronique	22
7. Exigences écrites.....	22
8. Exigences relatives à la signature	23
9. Exigences de reconnaissance, d'authentification, de certification notariée et de vérification .	24
10. Exigence de production d'un document original.....	24
11. Conservation de documents écrits	25
12. Intégrité des informations ou de l'enregistrement de la transaction	25
13. Reconnaissance des documents et des signatures étrangers	26
14. Contrats électroniques	26
15. Contrats électroniques automatisés	26
16. Effets d'une erreur lors des transactions avec un agent électronique.....	26
17. Manifestations de volonté.....	27
18. Heure et lieu de réception des communications électroniques	27
19. Attribution des communications électroniques.....	28
20. Autres règles de droit non modifiées	28
21. Consentement	28
TITRE III. PROTECTION DES CONSOMMATEURS.....	29
22. Données obligatoires.....	29
23. Délai de réflexion.....	31
24. Messages commerciaux non sollicités.....	32
TITRE IV. INTERMÉDIAIRES ET FOURNISSEURS DE SERVICES DE TÉLÉCOMMUNICATION	32
25. Responsabilité	32
26. Procédure de traitement des avis d'actes illégaux.....	33
27. Offre de biens et de services dans un environnement sûr	34

TITRE I – PRÉAMBULE

- Titre abrégé** 1. La présente Loi peut être désignée sous le titre de «Loi relative aux transactions électroniques» et entrera en vigueur le [xxx/ après publication au [nom de la publication].
- Objectif** 2. (1) Les objectifs de la présente loi sont les suivants:
- a. éliminer les obstacles juridiques à une utilisation efficace des enregistrements et des communications électroniques dans les transactions commerciales;
 - b. promouvoir l’harmonisation des règles juridiques sur les transactions électroniques par delà les frontières nationales et/ou internationales;
 - c. faciliter l’utilisation appropriée des transactions électroniques;
 - d. promouvoir la confiance des entreprises, des consommateurs et de la communauté dans les transactions électroniques; et
 - e. faciliter le remplissage électronique de documents avec les organismes et les entreprises publics et promouvoir la fourniture efficace des services gouvernementaux au moyen d’enregistrements électroniques fiables.
- Définitions** 3. (1) «Autorité d’accréditation» désigne l’autorité habilitée à établir des normes, des réglementations et des politiques pour les principales infrastructures publiques locales, en exerçant la fonction de l’autorité de certification de base et en gérant le processus d’approbation et de vérification des fournisseurs de services de certification, des fournisseurs de services d’authentification et des fournisseurs de services cryptographiques.
- (2) «Certificat accrédité» désigne un certificat délivré par un fournisseur de services de certification accrédité.
- (3) «Fournisseur de services de certification accrédité» désigne une entité ou une personne physique ou morale qui délivre des certificats électroniques ou fournit d’autres services liés aux signatures électroniques, qui ont été accrédités par l’autorité d’accréditation (certificats accrédités).
- (4) «Destinataire», dans le cadre d’un enregistrement électronique, désigne une personne destinée à recevoir de l’expéditeur d’un enregistrement électronique ledit enregistrement électronique; cette définition ne comprend pas une personne agissant en tant qu’intermédiaire en ce qui concerne cet enregistrement électronique.
- (5) «Signature électronique avancée» désigne une signature électronique fournie par un fournisseur de services de certification accrédité.
- (6) «Produits ou services d’authentification» désigne les produits ou les services conçus pour identifier le titulaire d’une signature électronique auprès d’autres personnes.

(7) «Fournisseur de services d'authentification» (ou autorité d'authentification ou autorité d'enregistrement) désigne une entité ou une personne physique ou morale dont les produits ou services d'authentification ont été accrédités par l'autorité d'accréditation; il effectue la reconnaissance (authentification) et l'enregistrement des titulaires de certificats électroniques délivrés par un fournisseur de services de certification ou un fournisseur de services de certification accrédité et peut revendre ces certificats en vertu d'un contrat avec ce dernier.

(8) «Fournisseur de service de certification» désigne une personne physique ou morale qui délivre des certificats électroniques ou fournit d'autres services en rapport avec les signatures électroniques.

(9) «Ordinateur» désigne un système d'information numérique intégré par du matériel et des programmes destinés à la création, à l'enregistrement, au stockage, au traitement et/ou à la transmission de données, incluant tout ordinateur, dispositif informatique ou autre dispositif électronique d'information ou de communication prévu pour effectuer ces fonctions.

(10) «Fournisseur de services cryptographiques» désigne une personne qui fournit ou propose de fournir des services ou produits de cryptographie.

(11) «Données» (ou «données informatiques» ou «données électroniques») désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête au traitement dans un système d'information, y compris un programme de nature à faire en sorte qu'un système d'information exécute une fonction.

(12) «Électronique» désigne tout support créé, enregistré, transmis ou stocké sous forme numérique ou sous une autre forme immatérielle par un moyen électronique, magnétique, optique ou par tout autre moyen doté de capacités de création, d'enregistrement, de transmission ou de stockage similaires.

(13) «Agent électronique» désigne un programme ou un autre moyen électronique ou automatisé, configuré et activé par une personne, utilisé pour entreprendre une action ou pour répondre en tout ou en partie à un enregistrement ou à un événement électronique, sans contrôle humain.

(14) «Certificat électronique» désigne une attestation électronique qui lie des données de vérification de signature à une personne ou un organisme public et confirme l'identité de cette personne ou de cet organisme public, ou lie des données de vérification du temps à un enregistrement électronique ou à une communication électronique et confirme la date et l'heure qui y sont associées.

(15) «Communication électronique» désigne un transfert d'enregistrements au moyen de signes, de signaux, d'écritures, d'images, de sons, de données ou de renseignements de quelque nature que ce soit transmis en tout ou en partie par fil, liaison radio, ou système électromagnétique, photoélectronique ou photo-optique qui influe sur le commerce intérieur ou extérieur, mais ne comprend pas:

- a. les communications par fil ou verbales;
- b. les communications émises au moyen d'un système de radiomessagerie unilatérale avec tonalité uniquement; ou

c. les communications émises par un dispositif de repérage.

(16) «Enregistrement électronique» désigne un ensemble de données créées, générées, 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 d'information ou d'un autre dispositif similaire, y compris par l'affichage, l'impression ou une autre sortie de ces données. Aux fins de la présente loi, «enregistrement électronique» fait référence aux informations en général et «enregistrements de transactions» (ou «enregistrement d'une transaction») fait plus particulièrement référence aux transactions (que celles-ci soient commerciales ou non).

(17) «Signature électronique» désigne les données sous forme électronique qui sont attachées, intégrées ou logiquement associées à d'autres données électroniques et qui servent de méthode d'authentification.

(18) «Transaction électronique» désigne la communication unique ou le résultat de plusieurs communications impliquées dans la vente ou l'achat de biens et de services conduits par l'intermédiaire de réseaux informatiques ou de systèmes d'informations, dans lesquels les biens et les services peuvent être commandés par l'intermédiaire de ces réseaux ou systèmes, mais dont le paiement et la livraison finale des biens et des services peuvent être effectués sans recourir à ces réseaux ou systèmes.

(19) «Système d'information» (ou «système informatique») désigne un dispositif ou un ensemble de dispositifs interconnectés ou reliés, y compris Internet, dont un ou plusieurs éléments assurent, en exécution d'un programme, le traitement automatique des données ou une autre fonction.

(20) «Intermédiaire», dans le cadre d'un enregistrement électronique, désigne une personne qui envoie, reçoit, stocke, traite ou fournit d'autres services qui concernent l'enregistrement électronique pour une autre personne, y compris la fourniture de services de contenu, de courrier électronique, de mise en cache et d'hébergement.

(21) «Expéditeur», dans le cadre d'un enregistrement électronique, désigne une personne qui:

- a. envoie un enregistrement électronique;
- b. charge une autre personne d'envoyer un enregistrement électronique en son nom; ou
- c. fait envoyer un enregistrement électronique par son agent électronique,

mais ne comprend pas une personne qui agit en tant qu'intermédiaire en ce qui concerne cet enregistrement électronique.

(22) «Organisme public» désigne:

- a. un ministère ou un département 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 pouvoirs publics territoriaux ou locaux, y compris les municipalités.

(23) «Enregistrement» désigne une information enregistrée créée, collectée ou reçue lors du lancement, de la conduite ou de l'achèvement d'une activité et qui comporte un contenu, un contexte et une structure permettant de fournir la preuve de cette activité ou de cette transaction, et qui est inscrit, stocké ou conservé sur un autre support, ou stocké sur un support électronique ou tout autre support, et accessible sous une forme visible et audible.

(24) «Signature» désigne tout symbole exécuté ou adopté, ou toute méthodologie ou procédure employée ou adoptée par une personne dans l'intention d'authentifier un enregistrement, y compris les méthodes électroniques ou numériques.

(25) «Fournisseur de services de télécommunication» désigne un fournisseur de services de télécommunication au sens des lois sur les télécommunications applicables.

(26) «Données relatives au trafic» désigne les données informatiques:

- a. relatives à une communication réalisée au moyen d'un système informatique;
- b. générées par un système informatique intégré à 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 de services sous-jacents.

(27) «Transaction» désigne une action ou un ensemble d'actions en rapport avec la conduite d'interactions commerciales ou non commerciales, telles que la vente, la location, l'échange, l'octroi de licences ou la disposition de biens personnels, y compris des produits et des biens immatériels, des services, ou une combinaison de ce qui précède entre deux personnes ou plus, notamment, mais pas exclusivement, des entités commerciales, des consommateurs ou des organismes publics.

(28) «Enregistrement de transactions» (ou «enregistrement d'une transaction») désigne un enregistrement électronique reflétant l'un des stades d'une transaction électronique commerciale ou non commerciale.

Exclusions

4. La présente Loi ne s'applique pas:
- a. à la création ou au transfert d'intérêts dans des biens immobiliers;
 - b. aux instruments négociables;
 - c. aux titres;
 - d. aux testaments, fiducies créées par testament ou tout autre instrument testamentaire;
 - e. aux procurations;
 - f. aux passeports et documents d'immigration;
 - g. à toute procédure régie par les règles de procédure civile ou par les règles des tribunaux;
 - h. à toute catégorie de documents, de transactions ou de lois exclue par la réglementation en vertu de la présente loi;

- i. à tout autre instrument susceptible d'être désigné par le Ministre par ordonnance.

TITRE II – TRANSACTIONS ÉLECTRONIQUES

Principe de non-discrimination

- 5. L'effet juridique, la validité ou l'application des informations et des transactions ne peuvent être refusés au seul motif qu'elles sont représentées sous forme électronique, à condition que les exigences établies dans la présente Loi soient satisfaites.

Prescription d'une forme non électronique

- 6. (1) Lorsqu'une loi exige qu'une personne fournisse des informations ou conclue une transaction en prescrivant une forme non électronique, cette exigence est satisfaite par la fourniture des informations ou la conclusion de la transaction sous une forme électronique:
 - a. organisée de la même manière ou essentiellement de la même manière que la forme non électronique prescrite;
 - b. accessible à l'autre personne (ou à des tiers, selon le cas) de façon à pouvoir être consultée ultérieurement; et
 - c. permettant sa conservation par l'autre personne (ou par un tiers, selon le cas).
- (2) Dans le paragraphe (1), la fourniture d'informations comprend, mais pas exclusivement, les suivantes:
 - a. faire une demande;
 - b. faire, produire ou déposer une réclamation;
 - c. donner, envoyer ou signifier un avis;
 - d. produire ou déposer une déclaration;
 - e. faire une requête;
 - f. faire une déclaration;
 - g. produire, déposer ou délivrer un certificat;
 - h. faire, modifier ou annuler un vote électronique.
- (3) Lorsqu'une loi mentionnée au paragraphe (1) exige plusieurs exemplaires de l'information ou de la transaction à soumettre à une personne, cette exigence est satisfaite en fournissant par voie électronique l'enregistrement de l'information ou de la transaction à la personne concernée conformément aux dispositions du présent article.

Exigences écrites

- 7. (1) Toute loi qui exige des informations ou des transactions écrites est satisfaite par des enregistrements électroniques si les exigences énoncées à l'Article 6, (1) (b) et (c) des présentes sont satisfaites.
Le paragraphe (1) ne s'applique pas lorsque la partie intéressée consent à renoncer à ces exigences.

8. (1) Toute loi qui exige la signature d'une personne concernant des informations ou une transaction est satisfaite lorsque les informations ou la transaction présentent une signature électronique et
- a. qu'une méthode est utilisée pour identifier la personne et montrer son approbation de la transaction;
 - b. compte tenu de toutes les circonstances pertinentes au moment où cette méthode a été utilisée, y compris un accord pertinent, la méthode était fiable et appropriée aux fins pour lesquelles la transaction a été conclue;
 - c. si la signature doit être donnée à un organisme public qui exige que la méthode utilisée soit en conformité avec certaines exigences technologiques particulières et que l'exigence de l'organisme public a été satisfaite; et
 - d. si la signature doit être donnée à une personne différente d'un organisme public, cette personne consent à ce que cette exigence soit satisfaite par le recours à la méthode mentionnée à l'alinéa (a).
- (2) Sous réserve du paragraphe (3), une signature numérique est présumée satisfaire aux exigences du paragraphe (1) (a) et (b) si la signature
- a. est liée de façon unique à la personne dont la signature est demandée;
 - b. permet d'identifier cette personne;
 - c. est créée par des moyens que cette personne peut garder sous son contrôle exclusif; et
 - d. est liée à la transaction à laquelle elle se rapporte de telle sorte que toute modification ultérieure de la transaction soit détectable.
- (3) Le paragraphe (2) ne saurait être interprété comme limitant de quelque manière que ce soit l'aptitude d'une personne à:
- a. établir de toute autre manière, afin de satisfaire l'exigence mentionnée au paragraphe (1), la fiabilité d'une signature électronique avancée ou d'une autre méthode d'indication de l'identité et de l'approbation;
 - b. apporter des preuves du manque de fiabilité d'une signature électronique avancée.
- (5) Pour déterminer si, ou dans quelle mesure, un certificat ou une signature électronique délivré dans la juridiction soumise à la présente Loi produit légalement ses effets, il n'est pas tenu compte du lieu
- a. de délivrance ou d'utilisation du certificat électronique; ou
 - b. d'établissement du fournisseur de services de certification ou du signataire,
- à condition que l'autorité nationale et/ou régionale chargée d'administrer le système de signatures électroniques avancées accrédite le fournisseur de services de certification.

Exigences de reconnaissance, d'authentification, de certification notariée et de vérification

- (6) Le présent article ne fait pas obstacle à l'application d'un autre principe de légalité qui exige qu'une
- a. transaction conclue par voie électronique contienne une signature électronique (quelle que soit sa description);
 - b. transaction conclue par voie électronique contienne une identification unique sous une forme électronique; ou qu'une
 - c. méthode électronique particulière soit utilisée pour la transaction conclue par voie électronique afin d'identifier l'expéditeur et de montrer que l'expéditeur a approuvé la transaction conclue.

9. Lorsqu'une loi exige qu'un enregistrement ou qu'une signature électronique soit produit, reconnu, authentifié, notarié ou vérifié par une personne, cette exigence est satisfaite si les éléments suivants sont joints ou logiquement associés à l'enregistrement électronique;
- a. la signature électronique avancée de cette personne;
 - b. dans le cas d'une signature ou d'un enregistrement électronique nécessitant une signature, une déclaration de cette personne attestant son identité;
 - c. une déclaration de cette personne certifiant la réalisation de toutes les obligations imposées par une loi régissant la validité juridique de l'enregistrement électronique; et
 - d. toutes les autres informations devant être incluses en vertu d'une autre loi.

Exigence de production d'un document original

10. (1) Lorsqu'une loi exige que l'enregistrement d'une transaction soit présenté sous sa forme d'origine ou soit mis à disposition en vue d'une inspection, ou qu'elle le permet, cette exigence est satisfaite lorsque l'enregistrement de la transaction est produit par voie électronique si:
- a. compte tenu de toutes les circonstances pertinentes à ce moment, la méthode de production électronique de l'enregistrement de la transaction a fourni un moyen fiable d'assurer le maintien de l'intégrité de cet enregistrement;
 - b. lorsque l'enregistrement de la transaction ou de l'information a été utilisé, il était raisonnable de penser qu'il serait immédiatement accessible de façon à pouvoir être consulté ultérieurement;
 - c. lorsque l'enregistrement de la transaction doit être produit auprès d'un organisme public et que l'organisme public nécessite qu'une:
 - i. forme électronique de l'enregistrement de la transaction soit produite de façon particulière, conformément à des exigences particulières relatives à la technologie de l'information; ou qu'une
 - ii. mesure particulière soit prise afin de vérifier la réception de l'enregistrement de la transaction

l'exigence de l'organisme public a été satisfaite; et

- d. lorsque l'enregistrement d'une transaction doit être produit auprès d'une personne différente d'un organisme public, cette personne consent à l'enregistrement de la transaction produite par voie électronique.

Conservation de documents écrits

(2) Aux fins du paragraphe (1) (a), les critères d'évaluation de l'intégrité sont les suivants:

- a. l'enregistrement de la transaction est resté complet et sans altération, exception faite des ajouts de toute approbation et de tout changement qui se produisent dans le cours normal de la communication, du stockage et de l'affichage;
- b. l'objet pour lequel l'enregistrement de la transaction est produit; et
- c. tout autre facteur pertinent.

11. (1) Lorsqu'une loi exige qu'une personne conserve des informations ou l'enregistrement d'une transaction pendant une période donnée, cette exigence est satisfaite par la conservation électronique des informations ou de l'enregistrement de la transaction si les conditions suivantes sont satisfaites:

- a. lorsque les informations ou l'enregistrement de la transaction ont, à l'origine, été générés sous forme électronique, il était raisonnable de penser que les informations ou l'enregistrement de la transaction seraient immédiatement accessibles de façon à pouvoir être consultés ultérieurement;
- b. compte tenu de toutes les circonstances pertinentes au moment où les informations ou l'enregistrement de la transaction ont, à l'origine, été générés sous forme électronique, la méthode de conservation des informations ou de l'enregistrement de la transaction sous forme électronique fournissait un moyen fiable d'assurer le maintien de l'intégrité des informations ou de l'enregistrement de la transaction qui ont été générés;
- c. les données relatives au trafic liées aux informations ou à l'enregistrement des transactions sont également conservées sous forme électronique pendant la période indiquée;
- d. lorsque les données relatives au trafic ont été initialement générées sous forme électronique, il était raisonnable de penser qu'elles seraient immédiatement accessibles de façon à pouvoir être consultées ultérieurement; et
- e. si la loi exige que les informations ou l'enregistrement de la transaction soient conservés sous forme électronique sur un type de support de stockage particulier, cette exigence est satisfaite tout au long de la période spécifiée.

(2) Une personne peut satisfaire l'exigence mentionnée au paragraphe (1) en recourant aux services d'une autre personne, si les conditions énoncées au paragraphe (1) (a) à (e) sont satisfaites.

Intégrité des informations ou de l'enregistrement de la transaction

12. (1) Aux fins des articles 10 et 11, l'intégrité des informations d'un enregistrement électronique ou de l'enregistrement d'une transaction est considérée comme fiable et préservée lorsque l'enregistrement électronique ou l'enregistrement de la transaction est resté complet et sans altération, hormis:

- a. l'ajout de toute approbation; ou
- b. tout changement négligeable,

qui se produit dans le cours normal de la communication, du stockage ou de l'affichage.

<p>Reconnaissance des documents et des signatures étrangers</p>	13.	<p>(2) La fiabilité au sens du paragraphe (1) est déterminée au regard de toutes les circonstances, notamment l’objet pour lequel l’information, l’enregistrement de la transaction ou l’enregistrement électronique a été créé.</p> <p>(1) Pour déterminer si, ou dans quelle mesure, des informations au format électronique ou l’enregistrement de transactions de sources étrangères sont juridiquement valables, il n’est pas tenu compte du lieu de création ou d’utilisation des informations ou de l’enregistrement de transactions ou du lieu d’établissement de leur créateur.</p> <p>[(2) Si l’autorité d’accréditation ou un organisme public habilité à réglementer les signatures électroniques dans la juridiction soumise à la présente Loi considère que les politiques et les pratiques d’une autorité d’accréditation, d’un fournisseur de service de certification et/ou d’un fournisseur de services d’authentification étrangers garantissent des niveaux de fiabilité au moins équivalents aux niveaux requis dans la juridiction de ce premier, il peut reconnaître les certificats électroniques et les services d’authentification étrangers comme juridiquement équivalents à ceux qui sont accrédités par ce premier].</p>
	<p>Contrats électroniques</p>	14.
<p>Contrats électroniques automatisés</p>		15.
	<p>Effets d’une erreur lors des transactions avec un agent électronique</p>	16.

- c. dès qu'elle s'aperçoit de l'erreur, la personne concernée informe rapidement l'autre personne; et
 - d. dans le cas où une contrepartie est reçue en conséquence de l'erreur, la personne concernée renvoie ou élimine la contrepartie conformément aux indications de l'autre personne ou, en l'absence de telles indications, prend des mesures raisonnables pour renvoyer ou éliminer la contrepartie et ne bénéficie donc pas du fait d'avoir reçu la contrepartie.
- Manifestations de volonté** 17. Entre l'expéditeur et le destinataire d'une communication sous forme électronique, l'effet juridique, la validité ou l'application d'une déclaration de volonté ou de toute autre déclaration ne peuvent être refusés au seul motif qu'elle est sous forme électronique.
- Heure et lieu de réception des communications électroniques** 18. (1) Une communication électronique est envoyée lorsqu'elle pénètre dans un système d'information hors de contrôle de l'expéditeur ou, si l'expéditeur et le destinataire utilisent le même système d'information, lorsque le destinataire peut la récupérer et la traiter.
- (2) Une communication électronique est présumée reçue par le destinataire:
- a. si le destinataire a désigné ou utilise un système d'information afin de recevoir les communications du type envoyé lorsqu'elles pénètrent dans le système d'information [et que le destinataire peut la récupérer et la traiter]; ou
 - b. si le destinataire n'a pas désigné ou n'utilise pas un système d'information afin de recevoir les communications du type envoyé, si le destinataire a désigné ou utilisé un tel système, mais que la communication a été envoyée vers un autre système, lorsque le destinataire se rend compte de l'existence de la communication dans son système d'information et qu'il peut la récupérer et la traiter.
- (3) Les paragraphes (1) et (2) s'appliquent sauf si les parties en conviennent autrement.
- (4) Une communication électronique est considérée comme étant envoyée à partir de l'établissement de l'expéditeur et reçue dans l'établissement du destinataire, sauf s'il existe des éléments de preuve raisonnables indiquant que l'expéditeur a envoyé la communication électronique d'un autre lieu.
- (5) Si l'expéditeur ou le destinataire dispose de plusieurs établissements commerciaux, l'établissement aux fins du paragraphe (4) est celui présentant le rapport le plus étroit avec la transaction sous-jacente à laquelle la communication électronique est liée ou, en l'absence d'une transaction sous-jacente, l'établissement principal de la personne concernée.
- (6) Si l'expéditeur ou le destinataire ne dispose pas d'établissement commercial, le lieu de résidence habituel de la personne concernée est considéré comme étant l'établissement commercial aux fins du paragraphe (4).

Attribution des communications électroniques

19. (1) Une communication électronique est celle de la personne qui l'envoie, si elle est envoyée directement par la personne concernée ou par un agent électronique en son nom. Entre l'expéditeur et le destinataire, un enregistrement électronique est attribuable à l'expéditeur s'il a été envoyé
- a. par une personne ou son agent électronique, ou par une autre personne autorisée par l'expéditeur à envoyer l'enregistrement électronique en son nom; ou
 - b. par l'agent électronique de l'expéditeur.
- (2) Entre l'expéditeur et le destinataire, un destinataire est en droit d'attribuer un enregistrement électronique à l'expéditeur et d'agir en se fondant sur cette hypothèse si:
- a. afin de s'assurer que l'enregistrement électronique est celui de l'expéditeur, le destinataire applique convenablement une procédure préalablement convenue par l'expéditeur à cette fin; ou
 - b. l'enregistrement électronique tel que reçu par le destinataire est la conséquence d'actions d'une personne dont les relations avec l'expéditeur, ou avec un agent de l'expéditeur, ont permis à cette personne d'avoir accès à une méthode que l'expéditeur utilise pour identifier ses enregistrements électroniques comme les siens.
- (3) Le paragraphe (2) ne s'applique pas
- a. à partir du moment où le destinataire a reçu un avis de l'expéditeur indiquant que l'enregistrement électronique n'est pas le sien et a bénéficié d'un délai raisonnable pour agir en conséquence; ou
 - b. dans un cas relevant du paragraphe (2)(b), à tout moment lorsque le destinataire sait ou devrait savoir s'il avait pris des dispositions raisonnables ou utilisé une procédure convenue, que l'enregistrement électronique n'est pas celui de l'expéditeur.
- 4) Le destinataire a le droit de considérer chaque enregistrement électronique reçu comme un enregistrement électronique distinct et d'agir en se fondant sur cette hypothèse, sauf dans la mesure où un enregistrement électronique en reproduit un autre et où le destinataire sait ou devrait savoir s'il avait pris des dispositions raisonnables ou utilisé une procédure convenue, que l'enregistrement électronique est un doublon.

Autres règles de droit non modifiées

20. (1) Rien dans la présente Loi ne limite l'application d'une autre loi qui autorise, interdit ou régleme expressément l'utilisation d'enregistrements de transactions, y compris une méthode de signature électronique ou de signature électronique avancée.
- (2) Rien dans la présente Loi ne limite l'application d'une autre loi qui exige qu'un enregistrement de transaction soit posté ou affiché de manière spécifique, ou qu'un enregistrement de transaction soit transmis selon une méthode précise.

Consentement

21. (1) Rien dans la présente Loi n'exige d'une personne qu'elle utilise, fournisse ou accepte des enregistrements de transactions sans consentement.

(2) Rien dans la présente Loi:

- a. n'exige d'une personne qu'elle utilise ou accepte les communications, signatures ou contrats électroniques; ou
- b. n'interdit à une personne qui s'engage dans une transaction en utilisant des moyens électroniques:
 - i. de modifier par convention toute disposition relative à la reconnaissance juridique et l'équivalence fonctionnelle des communications, signatures et contrats électroniques; ou
 - ii. d'établir des exigences raisonnables sur la manière d'accepter les communications, signatures ou formes de documents électroniques.

(3) La présente Loi s'applique à toute transaction entre des parties ayant chacune accepté de conduire la transaction par voie électronique.

(4) Pour déterminer si une partie accepte ou non de conduire une transaction par des moyens électroniques, il convient:

- a. lorsque la partie est un organisme public, que celui-ci fasse une déclaration expresse, rendue accessible au public ou aux personnes les plus susceptibles de communiquer avec cet organisme à des fins particulières;
- b. dans le cas d'une autre partie, de s'appuyer sur le contexte et les circonstances, y compris la conduite de la partie en question.

(5) Une partie qui accepte de conduire une transaction particulière par voie électronique peut refuser de conduire d'autres transactions par cette même voie.

(6) Les parties à une transaction commerciale électronique peuvent préciser les certifications et/ou fournisseurs de services d'authentification particuliers ou les catégories de certificats à utiliser en rapport avec les enregistrements ou les signatures électroniques qui leur sont soumis.

TITRE III – PROTECTION DES CONSOMMATEURS

Données obligatoires

22. (1) Un fournisseur qui offre des biens ou des services en vue de leur vente, de leur location ou de leur échange au moyen d'une transaction électronique doit mettre les données suivantes à la disposition des consommateurs, de façon claire et compréhensible:
- a. son nom complet et son statut juridique;
 - b. son adresse physique et son numéro de téléphone;
 - c. l'adresse de son site Internet et son adresse électronique;
 - d. l'adresse physique où le fournisseur recevra la transmission légale des documents;

- e. une description suffisante des principales caractéristiques des biens ou services offerts par le fournisseur afin de permettre au consommateur de prendre une décision éclairée à propos de la transaction électronique proposée;
- f. le prix total des biens ou services, incluant les frais de transport, les taxes et tout autre droit ou frais;
- g. la méthode de paiement;
- h. les termes de l'accord, notamment les garanties, qui s'appliqueront à la transaction et les moyens dont disposent les consommateurs pour accéder à ces termes, les stocker et les reproduire par voie électronique;
- i. le délai d'attente avant l'envoi ou la livraison des biens ou jusqu'à la date de réalisation des services;
- j. la manière selon laquelle et la période pendant laquelle les consommateurs peuvent accéder à l'enregistrement intégral de la transaction et le conserver;
- k. la politique de réexpédition, d'échange, d'assurance et de remboursement du fournisseur;
- l. les procédures de sécurité et la politique de confidentialité du fournisseur concernant le paiement, les informations sur le paiement et les informations à caractère personnel;
- m. un canal permettant de recevoir les avis des consommateurs, dans la même zone que la communication électronique initialement utilisée par le fournisseur pour présenter l'offre et/ou pour promouvoir la transaction.

(2) Le fournisseur donne au consommateur la possibilité de:

- a. revoir l'intégralité de la transaction électronique;
- b. corriger les éventuelles erreurs; et de
- c. se retirer de la transaction juste avant de passer commande.

(3) Si le fournisseur ne respecte pas les dispositions des paragraphes (1) ou (2), le consommateur peut annuler la transaction dans les quatorze (14) jours suivant la réception des biens ou des services visés par la transaction.

(4) En cas d'annulation d'une transaction conformément aux dispositions du paragraphe (3):

- a. le consommateur renvoie les biens du fournisseur ou, le cas échéant, cesse de recourir aux services effectués; et
- b. le fournisseur rembourse tous les paiements effectués par le consommateur, y compris les frais de réexpédition des biens.

(5) Le fournisseur doit utiliser un système de paiement suffisamment sécurisé et faisant référence aux normes technologiques acceptées au moment de la transaction et le type de transaction concernée.

(6) Le fournisseur est responsable de tout dommage encouru par un consommateur en raison du non-respect du fournisseur du paragraphe (5).

Délai de réflexion

- (7) Le fournisseur s'assure de la disponibilité d'un système de réponse automatisé destiné à accuser réception des communications électroniques envoyées par le consommateur.
- (8) Une transaction électronique d'un consommateur est considérée comme conclue dès la réception par le consommateur de la communication électronique du fournisseur confirmant la réception de l'acceptation de l'offre par le consommateur.
23. (1) Un consommateur a le droit d'annuler, sans raison et sans pénalité, toute transaction et tout accord de crédit y afférent pour la fourniture:
- a. de biens dans les sept (7) jours qui suivent la date de réception des biens; ou
 - b. de services dans les sept (7) jours qui suivent la date de conclusion de l'accord.
- (2) Les seuls frais susceptibles d'être prélevés au consommateur sont les coûts directs de la réexpédition des biens.
- (3) Si le paiement pour les biens ou services a été effectué avant que le consommateur n'exerce un droit mentionné au paragraphe (1), le consommateur a le droit à un remboursement intégral de ce paiement, remboursement qui doit être fait dans les 30 jours suivant la date d'annulation.
- (4) Le présent article ne s'applique pas à une transaction électronique:
- a. pour des services financiers, y compris des services d'investissement, des opérations d'assurance et de réassurance et des services bancaires;
 - b. conduite comme une vente aux enchères;
 - c. pour des services ayant débuté, avec le consentement du consommateur, avant le délai de réflexion applicable indiqué au paragraphe (1);
 - d. dans laquelle le prix pour la fourniture des biens, des services ou des équipements en question dépend des fluctuations des marchés financiers et ne peut pas être contrôlé par le fournisseur;
 - e. dans laquelle les biens en question:
 - i. sont fabriqués selon les spécifications du consommateur;
 - ii. sont clairement personnalisés;
 - iii. du fait de leur nature, ne peuvent pas être réexpédiés; ou
 - iv. sont susceptibles de se détériorer ou de se périmier rapidement;
 - f. dans laquelle des enregistrements audio ou vidéo ou des logiciels grand public ont été descellés par le consommateur;
 - g. pour la vente de journaux, de périodiques, de magazines ou de livres;
 - h. pour la fourniture de services de jeux ou de loterie; ou

Messages commerciaux non sollicités

- i. pour la fourniture de services ou d'équipements d'hébergement, de transport, de restauration ou de loisirs, que le fournisseur s'engage à fournir (lorsque la transaction est conclue) à une date ou au cours d'une période spécifique.]
24. (1) Une personne qui envoie des communications commerciales non sollicitées aux consommateurs doit limiter le nombre des destinataires à ceux qui ont fait preuve d'un intérêt potentiel envers le sujet de la communication, qui doit être clairement indiqué dans le titre de la communication, et donner au consommateur auquel des communications sont envoyées:
- a. la possibilité de refuser de recevoir d'autres communications de ce type de cette personne et fournir une adresse électronique valable à cette fin; et
 - b. sur demande du consommateur, les détails permettant l'identification de la source auprès de laquelle cette personne a obtenu ses informations sur le consommateur ou d'autres informations à caractère personnel.
- (2) Une personne qui ne respecte pas le paragraphe (1) est coupable d'une infraction et passible, sur déclaration de culpabilité par procédure sommaire, d'une amende minimale de (dollars) pour la première condamnation et d'un minimum de (dollars), pour chacune des condamnations ultérieures.

TITRE IV – INTERMÉDIAIRES ET FOURNISSEURS DE SERVICES DE TÉLÉCOMMUNICATION

Responsabilité

25. (1) Un intermédiaire ou un fournisseur de services de télécommunication qui fournit un simple canal pour la transmission de communications électroniques n'est pas responsable de leur contenu si cet intermédiaire ou fournisseur de services de télécommunication n'a pas effectivement connaissance ou n'est pas au courant de faits qui, pour une personne raisonnable, indiquerait une probabilité de responsabilité pénale ou de responsabilité civile délictuelle relativement à du matériel sur Internet ou qui, dès qu'il a connaissance ou est au courant de ces faits, ne continue pas conformément à l'article 26 des présentes, tant qu'il:
- a. n'est pas à l'origine de la transmission;
 - b. ne sélectionne pas le destinataire;
 - c. réalise les fonctions de manière technique et automatique, sans sélectionner l'enregistrement électronique; et
 - d. ne modifie pas l'enregistrement électronique contenu dans la transmission.
- (2) Les actes de transmission, d'acheminement et de fourniture d'accès mentionnés au paragraphe (1) incluent le stockage automatique, intermédiaire et transitoire des informations transmises tant que ce stockage a lieu:

- a. dans le seul but d'effectuer la transmission dans le système d'information;
- b. de manière à les rendre d'ordinaire inaccessibles à quiconque ne fait pas partie des destinataires prévus; et
- c. pendant une période ne devant pas être supérieure à ce qui est raisonnablement nécessaire pour la transmission.

(3) Un intermédiaire ou un fournisseur de services de télécommunication n'est pas tenu de surveiller les informations contenues dans un enregistrement électronique pour lequel l'intermédiaire ou le fournisseur de services de télécommunication fournit des services afin d'établir sa connaissance ou de devenir informé de faits ou de circonstances pour déterminer si les informations donnent lieu ou non à une responsabilité civile ou pénale.

(4) Rien dans le présent article n'exempte un intermédiaire ou un fournisseur de services de télécommunication de l'observance d'une ordonnance judiciaire, d'une injonction, d'un acte de procédure, d'une orientation du ministère, d'une exigence réglementaire ou d'une obligation contractuelle relatif à un enregistrement électronique ou à une communication ou une transaction électronique.

Procédure de traitement des avis d'actes illégaux

26. (1) Si un intermédiaire ou un fournisseur de services de télécommunication a effectivement connaissance du fait que les données d'un enregistrement ou d'une communication électronique donnent lieu à une responsabilité pénale ou une responsabilité civile délictuelle, ou peuvent raisonnablement donner à penser qu'elles donnent lieu à une responsabilité pénale ou une responsabilité civile délictuelle, et a obtenu de l'utilisateur de ses services des informations qui ne peuvent pas raisonnablement indiquer autre chose, l'intermédiaire ou le fournisseur de services de télécommunication doit dès que possible:

- a. avertir les autorités chargées de l'application de la loi appropriées des informations pertinentes, lorsque les lois pénales en vigueur l'exigent;
- b. divulguer l'identité de la personne pour laquelle l'intermédiaire ou le fournisseur de services de télécommunication fournissait les services relativement aux informations, si l'identité de cette personne est connue de l'intermédiaire, lorsque la loi écrite l'autorise; et
- c. supprimer les informations ou le message de données de tout système de traitement de l'information contrôlé par l'intermédiaire ou le fournisseur de services de télécommunication et cesser de fournir ou d'offrir de fournir des services relativement à ces informations ou prendre toute autre mesure autorisée par la loi, lorsque la loi écrite l'autorise

(2) La non-divulgateion de la connaissance d'un contenu illégal conformément au paragraphe (1) ci-dessus constitue une infraction.

Partie II

Offre de biens et de services dans un environnement sûr

27. (1) Le fournisseur de l'offre électronique de biens et de services s'assure que ces services sont réalisés dans un environnement électronique raisonnablement sûr et que ces conditions de sûreté sont rendues publiques.
- (2) Le fournisseur doit informer le consommateur de tout manquement à la sécurité susceptible d'avoir une incidence sur la confidentialité des données privées du consommateur, à l'adresse électronique fournie par le consommateur pour être contacté.

Partie III:

Notes explicatives relatives au modèle de texte législatif sur les transactions électroniques

INTRODUCTION

1. Le présent texte législatif élabore un cadre juridique pour les transactions électroniques. Les principaux objectifs de ce modèle de texte législatif sont d'éliminer les obstacles juridiques au commerce électronique, d'harmoniser les règles juridiques relatives aux transactions électroniques nationales ou internationales, de promouvoir la confiance dans le commerce électronique et de faciliter le remplissage électronique de documents avec le gouvernement et la fourniture électronique de services gouvernementaux («cybergouvernance»).
2. Ces Notes explicatives sont destinées à expliquer le contenu du présent modèle de texte législatif et doivent être lues simultanément à ce texte. Elles expliquent l'importance des principales dispositions de ce modèle et, le cas échéant, attirent l'attention sur des discussions particulières⁸, en qui ont eu lieu au sein du Groupe de travail⁹ pour le projet HIPCAR décrivant les différentes options de réglementation qui ont été abordées. Elles ne sont pas une description détaillée du présent texte législatif et ne sont pas destinées à en être une. Aussi, lorsqu'un article ou une partie d'un article ne semble pas nécessiter de clarification, de commentaires ou de références exhaustifs, ou lorsqu'une disposition particulière n'a donné lieu à aucune discussion au sein du Groupe de travail, aucune explication détaillée n'est fournie.
3. Le présent modèle de texte législatif (Loi) est constitué de quatre titres:
 - **Le Titre I** décrit les objectifs de la présente Loi, fournit les définitions de la terminologie applicable et exclut certains sujets de l'application de ce texte législatif;
 - **Le Titre II** envisage le principe de non-discrimination envers les informations et les transactions électroniques, établit des exigences formelles applicables aux transactions électroniques, fournit des critères permettant de déterminer l'intégrité des informations électroniques ou des enregistrements de transactions et de reconnaître les documents et signatures électroniques de sources étrangères, traite des contrats électroniques automatisés et des agents électroniques, définit l'heure et le lieu de réception des communications électroniques, énonce des règles pour l'attribution des communications électroniques et reconnaît la nécessité d'un consentement des parties intéressées;

⁸ Le titre complet du projet HIPCAR est «*Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures*» (Amélioration de la compétitivité dans les Caraïbes au travers de l'harmonisation des politiques, législations et procédures réglementaires en matière de TIC). Ce projet de 3 ans a été lancé en septembre 2008, dans le contexte d'un projet-cadre englobant les pays ACP financé par l'Union européenne et l'Union internationale des télécommunications. Le projet est mis en œuvre par l'Union internationale des télécommunications (UIT) en collaboration avec le Secrétariat de la Communauté des Caraïbes (CARICOM) et l'Union des télécommunications des Caraïbes (CTU).

⁹ Les membres des Groupes de travail pour le projet HIPCAR incluent les représentants du ministère et du régulateur nommés par leurs gouvernements nationaux, les organismes régionaux et observateurs concernés, tels que les opérateurs et d'autres parties prenantes intéressées. Les mandats des Groupes de travail sont disponibles à l'adresse: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.

Le second atelier de consultation (stade B) du Groupe de travail 1 pour le projet HIPCAR sur le cadre législatif applicable aux TIC – questions relatives à la société de l'information s'est déroulé à la Barbade, du 23 au 26 août 2010. Les participants ont examiné le projet de modèle de texte législatif sur le domaine de travail respectif, en ont discuté et l'ont adopté par un large consensus. Lorsque l'expression «Groupe de travail» apparaît dans le présent document, elle fait référence à l'atelier susmentionné. Dans ce document, l'expression «pays bénéficiaire» fait référence aux 15 pays ACP de la région des Caraïbes identifiés dans le cadre du projet HIPCAR financé par l'ITU/UE.

- **Le Titre III** établit l'obligation faite aux fournisseurs de fournir certaines données aux consommateurs d'offres électroniques de biens ou de services, garantit un délai de réflexion pour l'annulation par le consommateur des transactions électroniques et des accords de crédit qui y sont liés et définit les exigences pour l'envoi des messages commerciaux non sollicités;
- **Le Titre IV** régleme la responsabilité des intermédiaires et des fournisseurs de services de télécommunication, établit une procédure de traitement des avis d'actes illégaux et exige que les approvisionnements garantissent un environnement sûr pour l'offre électronique des biens et des services.

COMMENTAIRE DES ARTICLES

TITRE I – PRÉAMBULE

4. Le Titre I fournit le titre abrégé et la clause d'entrée en vigueur à l'Article 1, les objectifs à l'Article 2 et les définitions à l'Article 3.

Le Titre I a motivé une discussion au sein du Groupe de travail pour le projet HIPCAR en ce qui concerne le style de la rédaction dans différents pays. La question de savoir si un Article devait inclure les objectifs de ce modèle de texte législatif a fait l'objet de discussions. Il a été convenu par consensus de laisser chaque État bénéficiaire trancher cette question.

Article 2. Objectifs

5. L'Article 2 répertorie les objectifs de ce modèle de texte législatif (Loi), principalement destinés à favoriser le commerce électronique, mais qui peuvent s'étendre (au moins en termes généraux) aux autres catégories de transactions électroniques et aux services d'administration publique électronique.

Article 3. Définitions

6. La définition d'**ordinateur** fournie au paragraphe (9) permet d'englober tout dispositif électronique susceptible d'exécuter les fonctions typiques d'un ordinateur.
7. Le Groupe de travail pour le projet HIPCAR a débattu du fait de savoir s'il devait être fait une référence explicite aux appareils de télécommunications tels que les téléphones mobiles. Il a été convenu qu'il était préférable, du fait du rythme rapide du développement technologique et du principe de neutralité technologique, de conserver un intitulé général mentionnant des «dispositifs électroniques d'information ou de communication» en plus des références à «ordinateur» et à «dispositifs informatiques».
8. Les **données** sont définies au paragraphe (11) comme représentant des faits, des informations, ou des concepts sous une forme qui se prête au traitement dans un système d'information.
9. «Données» a été choisie pour être l'expression définie plutôt qu'«information», qui est une expression présente dans la législation de certains pays relative aux transactions générales et non particulièrement aux transactions électroniques. Le champ d'application de la présente Loi comprenant uniquement les transactions électroniques, l'intention était ici de désigner uniquement les faits, les informations et les concepts représentés sous forme de chiffres binaires électroniques.
10. Le Groupe de travail pour le projet HIPCAR a débattu de la commodité d'inclure la mention d'«état» dans la définition de «données», ce qui semble souligner que les données pourraient ne pas être uniquement conçues logiquement comme des séquences de «0» et de «1» (lesquelles représentent des lettres ou des chiffres), mais qui désigne également le changement tangible de

l'état électromagnétique ou optique dans un ordinateur que le système d'information «lit» comme correspondant aux chiffres binaires. Bien que l'expression «état» puisse aider les non-spécialistes (y compris les magistrats) à également prendre en compte l'aspect tangible des données et contribuer ainsi à qualifier juridiquement les données de «choses» (impliquant, par exemple, qu'elles pourraient faire l'objet d'une possession ou d'un détournement), la dernière partie de cette définition, qui précise «... y compris un programme de nature à faire en sorte qu'un système d'information exécute une fonction...» pourrait indirectement atteindre, dans une certaine mesure, l'objectif de désigner également le caractère tangible (dans la mesure où l'on s'attend à ce que l'exécution d'une fonction dans un système d'information produise un certain changement tangible). Par conséquent, la préférence pour l'un ou l'autre niveau d'insistance sur l'aspect tangible des données a été laissée à la libre appréciation des États bénéficiaires.

11. Enfin, cette définition indique clairement que «données» est un synonyme de «données informatiques» et de «données électroniques», dont les expressions sont présentes dans les législations qui y sont liées aux niveaux national et international. Leur équivalence est donc établie par souci de cohérence, en particulier pour ce qui concerne la législation d'autres pays, où la diversité de la terminologie employée est plus importante, renforçant la nécessité de jeter des ponts afin de faciliter une interprétation commune et une application efficace.
12. La réponse électronique automatisée utilisée comme interface pour l'interaction entre des êtres humains et des ordinateurs caractérise l'**agent électronique** tel que défini au paragraphe (13). Cette définition est celle d'éléments qui intègrent les concepts d'expéditeur et de destinataire d'une communication électronique, capables de déterminer si un envoi ou une réception effectifs ont bien eu lieu, ainsi que la manière de le prouver et l'emplacement des preuves.
13. La définition de **communication électronique**, contenue au paragraphe (15), est axée sur le transfert d'enregistrements, y compris les envois et réceptions respectifs (tandis que les définitions d'«ordinateur» et de «système d'information» sont limitées et s'attachent aux activités internes exécutées par l'ordinateur ou par le système d'information).
14. Le Groupe de travail pour le projet HIPCAR a discuté de l'utilité d'inclure ou non des références aux passages «les communications par fil ou verbale» et «les communications émises par un dispositif de repérage». Certains se sont dits préoccupés par le fait que ces expressions pourraient chevaucher des expressions déjà en vigueur dans les lois sur les télécommunications de certains pays, en particulier en ce qui concerne les dispositifs de téléphonie, de radiomessagerie et de repérage. Le Groupe de travail a décidé de laisser chacun des États bénéficiaires trancher sur l'opportunité de conserver ou non ces formulations.
15. Le paragraphe (16) définit l'**enregistrement électronique** comme un ensemble de données qui peut être lu ou perçu par une personne au moyen d'un système d'information ou d'un autre dispositif similaire.
16. Tandis que les données sont représentées sous forme binaire et sont supposées être «lues» par un ordinateur ou «traduites» par un programme informatique, un «enregistrement électronique» est l'apparence ou le résultat d'un système d'information qui peut être perçu par un être humain.
17. La distinction entre ces expressions complémentaires («données» et «enregistrement électronique») est nécessaire pour légiférer sur les transactions électroniques, dans la mesure où la manifestation du consentement ou la preuve de certains faits, informations ou concepts peut reposer sur la perception d'une personne (ou sur la capacité à être perçu par ladite personne).

18. La définition d'«enregistrement électronique» est également intéressante pour déterminer le sens de «dispositif d'information électronique» (auquel il est fait référence dans certaines dispositions du présent texte législatif par la formulation «dispositifs électroniques d'information ou de communication»), ce dernier étant clairement destiné à désigner un dispositif utilisé par les hommes pour accéder à des enregistrements électroniques ou les percevoir.
19. En outre, la définition d'«enregistrement électronique» a intégré l'expression «quel que soit le support physique», ce qui devrait contribuer à étendre la portée des supports associés aux transactions électroniques, en l'étendant au-delà des supports traditionnels de façon à inclure, par exemple, les supports biométriques (tels qu'une image numérisée des doigts, du visage ou de l'iris), qui pourraient connaître des applications croissantes dans le contexte des transactions électroniques (comme cela a déjà commencé à se produire avec les guichets automatiques bancaires dans certains pays).
20. De la même façon, la référence aux impressions précise que les enregistrements électroniques ne sont pas nécessairement destinés à être perçus dans un système informatique et qu'ils peuvent, plutôt être perçus à l'extérieur de ce système.
21. Enfin, ce paragraphe précise que le concept d'«enregistrement électronique» a été utilisé tout au long du présent texte législatif pour désigner les informations en général, tandis que les concepts d'«enregistrements de transactions» (ou d'«enregistrement d'une transaction») ont été utilisés plus particulièrement en ce qui concerne les transactions (que celles-ci soient commerciales ou non).
22. La **signature électronique** est définie au paragraphe (17) comme une méthode d'authentification. Avec la définition pertinente d'autres expressions apparentées (comme **autorité d'accréditation, certificat accrédité, fournisseur de services de certification accrédité, signature électronique avancée, produits et services d'authentification, fournisseur de services d'authentification, fournisseur de services de certification, fournisseur de services cryptographiques, certificat électronique et signature**) présentées aux autres paragraphes de l'Article 3, elle fournit une signification cohérente à un système de validation essentiel des transactions électroniques (le système d'authentification, la certification et l'accréditation des signatures numériques) capable d'identifier l'auteur, l'origine, l'heure et d'autres éléments des enregistrements électroniques.
23. Les définitions adoptées pour cet ensemble d'expressions tiennent compte du fait que l'État bénéficiaire peut avoir ou non mis en œuvre un système de services de certification pour les signatures électroniques, établi au niveau local ou loué à l'étranger. Voilà pourquoi ces définitions se concentrent sur les aspects de base, laissant aux réglementations ultérieures la possibilité d'ajouter des options plus spécifiques (telles que les différentes structures des rôles et des pouvoirs, la répartition des ressources régionales et/ou nationales, l'offre de services de certification par horodatage, etc.).
24. En adoptant cette approche, la définition des signatures électroniques facilite l'intégration avec d'autres dispositions du présent texte législatif (telles que les dispositions en rapport avec les exigences relatives à la signature et la production d'un document original), la formulation générique adoptée fournissant la souplesse nécessaire pour adapter différentes manières d'utiliser les signatures électroniques pour signer un document et garantir son intégrité.
25. La définition de **système d'information**, contenue au paragraphe (19) est tout aussi importante pour comprendre les phénomènes qui entourent les transactions électroniques. Tandis qu'un «ordinateur» désigne un équipement électronique unique, un «système d'information» est composé de groupes de dispositifs interconnectés, typiques des réseaux électroniques.
26. La définition de «système d'information» au sens large comprend des réseaux à divers niveaux, y compris Internet, considéré au niveau technique comme un «réseau de réseaux». Compte tenu de l'importance d'Internet en tant que plate-forme technologique pour les transactions électroniques, une référence spécifique y est faite. Le concept de groupe de dispositifs interconnectés est suffisamment complet pour inclure tout équipement relié à Internet.

27. Le Groupe de travail pour le projet HIPCAR s'est aussi demandé si ce modèle de texte législatif devait utiliser l'expression «système d'information» plutôt que celle de «système informatique». Le fait que l'expression «système d'information» (et «système de traitement de l'information») soit utilisée dans la législation de la plupart des pays a fait pencher la balance en sa faveur. Bien qu'il existe quelques différences techniques de signification entre «système d'information» et «système informatique», celles-ci n'ont pas été considérées comme essentielles dans le contexte des transactions électroniques. Le Groupe de travail a donc choisi d'utiliser «système d'information», tout en ajoutant «système informatique» en tant qu'expression équivalente. Le niveau de précision technique souhaité pour aborder ces concepts dans le présent texte législatif a été laissé à la libre appréciation des États bénéficiaires.
28. La définition d'**intermédiaire**, fournie au paragraphe (20), est suffisamment large pour comprendre l'accès, le contenu et l'hébergement de fournisseurs de services Internet, ainsi que d'autres fournisseurs de services possibles.
29. Le concept d'**expéditeur**, tel qu'il est défini au paragraphe (21), comprend non seulement la personne qui envoie effectivement une communication électronique, mais également la personne qui en charge une autre de faire l'envoi en son nom et la personne qui utilise un agent électronique pour faire ses envois.
30. L'exhaustivité de ce concept revêt une importance croissante à mesure que le volume des communications électroniques «envoyées» par l'intermédiaire de tiers (tels que les «centres d'appels électroniques» ou les fournisseurs de services de «marketing par e-mail») ou par le biais d'agents électroniques (comme dans les contrats dits «contrats d'achat en ligne») se développe à un rythme rapide.
31. Le Groupe de travail pour le projet HIPCAR a décidé d'inclure une remarque visant à préciser que l'«agent électronique» ne comprend pas les personnes qui agissent en tant qu'«intermédiaires» (expression définie au paragraphe (20)) en ce qui concerne l'enregistrement électronique.
32. **Organisme public** est défini au paragraphe (22) comme incluant un ministère ou un département, les entreprises détenues en tout ou en partie par l'État, les organismes exerçant une autorité légale, de nature législative, exécutive ou judiciaire et les pouvoirs publics territoriaux ou locaux, y compris les municipalités.
33. Cette définition est conforme à l'observation du point 23 ci-dessus, qui mentionne la possibilité pour une réglementation ultérieure d'établir un système d'authentification et/ou de certification des signatures numériques. La question ici, est que les transactions électroniques présentent un vaste éventail d'implications pour les organismes d'État et pour chaque citoyen, ce qui signifie que la législation susceptible de les réglementer est aussi diverse que le nombre d'autorités ou d'entreprises détenues par l'État qui peuvent les utiliser est important, d'où la nécessité d'une définition aussi complète.
34. La définition d'«organisme public» est utilisée dans un grand nombre de dispositions du présent texte législatif (par exemple, dans les Articles 8.(1).c, 10.(1).c et .d, 13.(2) et 21.(4).a). En outre, elle préétablit la large portée des «organismes publics» susceptible de publier des réglementations supplémentaires ou d'en être le bénéficiaire, en fournissant la cohérence nécessaire pour la publication d'une législation subordonnée.
35. Le paragraphe (26) traite des **données relatives au trafic** en visant à inclure les données qui qualifient le flux d'une communication électronique donnée. Les détails tels que l'origine, l'itinéraire, la destination, la date, l'heure, la taille et la durée sont extrêmement importants pour déterminer l'auteur, le lieu et l'heure de certaines transactions (en particulier lorsque le flux des communications électroniques est divisé en «paquets» qui peuvent suivre différents trajets jusqu'à ce qu'ils atteignent la destination prévue, comme sur Internet).

Article 4. Exclusions

36. Bien que ce modèle de texte législatif soit censé s'appliquer à une large gamme de transactions (commerciales ou non, conclues entre des parties privées et/ou publiques), certaines situations ne peuvent pas ou ne doivent pas être soumises à ses dispositions. L'Article 4 présente une liste de ces situations, qui comprennent: i) la création ou le transfert d'intérêts dans des biens immobiliers, ii) les instruments négociables, iii) les titres, iv) les testaments, fiducies créées par testament ou autres instruments testamentaires, v) les procurations, vi) les passeports et documents d'immigration, vii) toute procédure régie par les règles de procédure civile ou par les règles des tribunaux, viii) toute catégorie de documents, ix) les transactions ou lois exclues par la réglementation en vertu de la présente loi et x) tout autre instrument susceptible d'être désigné par le ministre par ordonnance. L'objet de cet Article est principalement d'éviter tout conflit avec d'autres Lois.

TITRE II – TRANSACTIONS ÉLECTRONIQUES**Article 5. Principe de non-discrimination**

37. Le présent Article établit le principe de non-discrimination envers les informations ou les transactions électroniques. Toute information ou transaction peut être ou ne pas être fiable, qu'elle soit électronique ou non. Par conséquent, il n'y a aucune raison d'exercer une discrimination *a priori* envers les informations ou les transactions électroniques. On peut même dire que certaines informations ou transactions électroniques (comme dans le cas de signatures numériques certifiées) peuvent être plus dignes de confiance que d'autres qui ne sont pas électroniques.
38. Cet Article est important en ceci qu'il énonce la recevabilité des informations ou des transactions électroniques en tant que règle générale, sous réserve des exigences répertoriées dans les Articles suivants.

Article 6. Prescription d'une forme non électronique

39. La philosophie qui sous-tend la prescription de forme des informations ou des transactions est de s'assurer des degrés convenables de fiabilité. Cette philosophie peut également être appliquée aux informations ou aux transactions sous forme électronique. Cet Article dresse la liste des critères qui déterminent cette équivalence: i) organisation de la même manière ou essentiellement de la même manière que la forme non électronique prescrite, ii) accessibilité à d'autres personnes de façon à pouvoir être consultée ultérieurement et iii) possibilité d'être conservée par d'autres personnes.
40. Cet Article est conforme au principe accepté au niveau international de l'équivalence fonctionnelle, qui stipule qu'aucune restriction ne doit être imposée sur l'environnement en ligne qui n'est pas également imposée à l'univers hors ligne. L'équivalence établie par cet Article s'inscrit dans l'objectif visant à jeter des ponts entre les exigences des formes électronique et non électronique, facilitant la migration vers l'environnement numérique.
41. Le Groupe de travail pour le projet HIPCAR a discuté des possibles implications du critère exigeant des capacités de conservation, qui peut présenter des chevauchements avec les lois sur la conservation des données et le respect de la vie privée ou avec les dispositions contractuelles de services d'hébergement ou d'entreposage. Bien que la formulation utilisée pour cette exigence soit relativement générale (par exemple, elle ne précise pas la durée de la conservation et autorise la conservation par des tiers), les États bénéficiaires doivent vérifier si cette exigence entre en conflit avec une autre disposition légale et établir une règle de préséance, le cas échéant.

42. Le paragraphe (2) établit une liste d'exemples de situations dans lesquelles la fourniture d'informations électroniques doit être considérée comme équivalente à la fourniture d'informations non électroniques. L'une de ces situations fait référence au fait de faire, modifier ou annuler un «vote électronique», qui est destiné à répondre aux élections générales électroniques (le vote aux élections politiques ou à certaines autres élections étant progressivement devenu un processus électronique, jusqu'à un certain point, malgré le fait que la législation la plus pertinente n'y fasse pas référence). Le Groupe de travail pour le projet HIPCAR a noté que certains pays de la région des Caraïbes peuvent souhaiter supprimer ce point, lorsqu'il empiète sur la Loi sur la représentation du peuple ou sur une législation similaire.

Article 7. Exigences écrites

43. De la même façon que pour la prescription de la forme, les exigences écrites peuvent faire référence à des informations ou des transactions électroniques ou non électroniques.
44. La conformité avec le principe de l'équivalence fonctionnelle suppose d'établir des critères qui jettent des ponts entre les exigences électroniques et non électroniques pour les informations ou les transactions écrites.
45. Par souci de cohérence, le présent Article renvoie aux critères établis à l'Article 6 (plus précisément, à ceux envisagés aux points 1.(b) et 1.(c)).
46. Le présent Article prévoit également la renonciation à ces exigences si les parties intéressées y consentent.

Article 8. Exigences relatives à la signature

47. Le principe de l'équivalence fonctionnelle s'applique également aux exigences relatives à la signature.
48. L'Article 8 établit des critères qui jettent un pont entre les exigences pour les signatures électroniques et les signatures non électroniques. Ces critères cumulatifs comprennent: i) une méthode pour identifier la personne et montrer son approbation de la transaction; ii) le fait que la méthode ait été fiable et appropriée aux fins de la transaction et iii) la conformité avec les exigences technologiques imposées par les organismes publics, le cas échéant.
49. Le paragraphe (2) traite spécifiquement des signatures numériques, établissant la présomption selon laquelle elles satisfont aux exigences d'une méthode fiable et appropriée pour identifier une personne et montrer son approbation de la transaction lorsque la signature numérique est: i) liée de façon unique au signataire; ii) capable d'identifier le signataire; iii) maintenue sous le contrôle du signataire et iv) liée à la transaction de façon à en révéler une quelconque modification.
50. Ces critères génériques sont importants dans la mesure où les signatures numériques sont associées à différents niveaux de sécurité, alors que ce modèle de texte législatif vise à ne pas imposer de restrictions qui pourraient nuire à la conformité avec le principe de neutralité technologique accepté au niveau international selon lequel il ne doit y avoir aucune préférence déraisonnable pour des technologies particulières.
51. Le paragraphe (3) fait référence aux signatures électroniques avancées, permettant à toute personne d'établir leur fiabilité ou d'apporter des preuves de leur manque de fiabilité d'une façon différente de celles énoncées aux paragraphes (1) et (2).
52. Ce paragraphe est important dans la mesure où les signatures électroniques avancées jouissent d'une présomption de fiabilité en propre, indépendamment des autres facteurs, et où l'on s'attend à ce que cette présomption soit appliquée (ou contestée, si nécessaire).

53. Le paragraphe (5) envisage les certificats ou les signatures électroniques émis au sein de la juridiction soumise au présent texte législatif, établissant qu'il ne doit pas être tenu compte de l'emplacement géographique, à condition que l'autorité nationale et/ou régionale chargée d'administrer le système de signature électronique avancée accrédite le fournisseur de services de certification.
54. Ce paragraphe est important dans la mesure où il crée la possibilité que les certificats accrédités par une éventuelle autorité régionale soient juridiquement valables dans l'État bénéficiaire.
55. Bien évidemment, ce texte législatif ne prétend pas créer une autorité régionale, mais il prévoit cette hypothèse, qui pourrait être pratique dans la mesure où elle est possible et souhaitée.
56. Le paragraphe (6) déclare que cet Article ne fait pas obstacle à l'application d'un autre principe de légalité qui exige qu'une transaction contienne une signature électronique, une identification unique ou une méthode particulière afin d'identifier l'expéditeur et de montrer son approbation de la transaction.
57. Ce paragraphe est important puisqu'il évite ou réduit la possibilité d'un conflit avec une loi apparentée, telle qu'une loi qui impose une identification par d'autres moyens (p. ex., biométriques) ou qui stipule que chaque transaction doit recevoir un numéro unique (comme dans le cas des factures de redevance électroniques).

Article 9. Exigences de reconnaissance, d'authentification, de certification notariée et de vérification

58. Suivant la voie de la construction d'une équivalence juridique entre les enregistrements ou les signatures électroniques et non électroniques, l'Article 9 établit les critères aux termes desquels les exigences de reconnaissance, d'authentification, de certification notariée ou de vérification sont satisfaites en matière d'enregistrements et de signatures électroniques.
59. Ces critères incluent: i) la signature électronique avancée; ii) une déclaration du signataire attestant son identité; iii) une déclaration du signataire certifiant la réalisation de toutes les obligations relatives à la validité de l'enregistrement électronique; et iv) toutes les autres informations nécessitant d'être incluses en vertu d'une autre loi.
60. Cet Article est important dans la mesure où il fournit un certain nombre d'options pour satisfaire lesdites exigences, y compris des solutions de remplacement non électronique, qui peuvent être particulièrement pratiques lorsque des signatures électroniques avancées ne sont pas disponibles, sont trop onéreuses ou bureaucratiques au vu des circonstances, ou lorsque l'inclusion numérique sociale n'a pas encore atteint les parties intéressées.

Article 10. Exigence de production d'un document original

61. Bien qu'il soit notoire que les enregistrements électroniques présentent certaines difficultés techniques liées à la détermination de l'original d'un enregistrement par rapport à une copie, il existe des moyens susceptibles de confirmer l'équivalence de la production d'originaux de documents non électroniques.
62. L'Article 10, dans son paragraphe (1), établit une liste des critères d'équivalence avec les enregistrements électroniques d'une transaction. Ces critères incluent: i) l'existence d'un moyen fiable d'assurer l'intégrité de l'enregistrement; ii) l'accessibilité immédiate des enregistrements envoyés de façon à pouvoir être consultés ultérieurement; iii) la satisfaction des exigences particulières imposées par les organismes publics et iv) le consentement de la personne intéressée par l'enregistrement est produit par voie électronique.

63. Cette disposition est importante dans la mesure où elle est conforme au principe de l'équivalence fonctionnelle et où elle fournit des options raisonnablement disponibles pour établir des enregistrements électroniques originaux d'une transaction.
64. Le paragraphe (2) précise les façons de procéder à l'évaluation de l'intégrité d'un enregistrement. À cet effet, il établit les critères suivants: i) l'enregistrement reste complet et sans altération (exception faite des changements qui se produisent dans le cours normal de la communication, du stockage et de l'affichage); ii) les fins de la production de l'enregistrement et iii) tout autre facteur pertinent.
65. Ce paragraphe est important en ceci qu'il assure une évaluation souple de l'intégrité d'un enregistrement en tenant compte des fins de la production de l'enregistrement et de tout autre facteur pertinent.
66. Enfin, et ce n'est pas le moins important, il ne tient pas compte des changements négligeables (qui se produisent sur l'enregistrement) dus à des causes normales; les environnements numériques étant souvent soumis à des changements (en vue d'une mise à jour technologique ou pour d'autres raisons), les changements négligeables normaux ne modifient pas l'état «complet» et «sans altération» d'un enregistrement.

Article 11. Conservation de documents écrits

67. L'Article 11, au paragraphe (1), décrit les critères qui répondent aux exigences de conservation de documents écrits, lorsque des enregistrements électroniques d'une transaction sont concernés. Ces critères comprennent: i) il était raisonnable de penser que les informations ou l'enregistrement seraient immédiatement accessibles de façon à pouvoir être consultés ultérieurement; ii) la méthode de conservation des informations ou de l'enregistrement a fourni un moyen fiable d'assurer l'intégrité; iii) les données relatives au trafic sont également conservées, iv) les données relatives au trafic devaient être immédiatement accessibles de façon à pouvoir être consultées ultérieurement et v) conformité avec une éventuelle exigence de conservation des informations ou de l'enregistrement sur un type particulier de support de stockage. Le paragraphe (2) permet de satisfaire à toutes les exigences susmentionnées au moyen des services d'une autre personne.
68. Cet Article est important, car il envisage les moyens pratiques de satisfaire aux exigences de conservation des informations ou des enregistrements électroniques.
69. Il est intéressant de noter la présence des données relatives au trafic parmi les critères sélectionnés, ce qui souligne l'utilité de conserver non seulement le «contenu» d'une information ou d'un enregistrement, mais également les données associées à son envoi ou à sa réception. Les données relatives au trafic peuvent être un élément essentiel de la reconnaissance des informations ou des enregistrements électroniques.

Article 12. Intégrité des informations ou de l'enregistrement de la transaction

70. L'Article 12 complète les dispositions de l'Article 10 en étendant aux informations électroniques les critères qu'il prévoit pour évaluer l'intégrité dans le contexte de la production de documents originaux.
71. Il complète également l'Article 11, en étendant ces critères d'évaluation de l'intégrité au contexte de la conservation de documents écrits.
72. L'importance de cet Article réside dans le fait qu'il garantit la cohérence lors de l'évaluation de l'intégrité des informations et des enregistrements électroniques dans les deux contextes.

Article 13. Reconnaissance des documents et des signatures étrangers

73. De la même façon que les dispositions de l'Article 8.(5) concernent les effets juridiques des certificats ou des signatures électroniques émis au sein de la juridiction soumise à la présente Loi (voir le point 48 ci-dessus), l'Article 13 traite de la reconnaissance des documents et des signatures étrangers, établissant, au paragraphe (1), qu'il n'est pas tenu compte du lieu dans lequel les informations ou l'enregistrement des transactions ont été créés ou utilisés ou du lieu d'établissement de leur créateur.
74. Cet Article est particulièrement important, le paragraphe (2) autorisant l'autorité d'accréditation ou un organisme public habilité à réglementer les signatures électroniques dans la juridiction soumise au présent texte législatif, pour reconnaître les certificats électroniques et les services d'authentification étrangers lorsqu'il considère que le pays étranger en question est doté de politiques et de pratiques aussi fiables que celles requises dans la juridiction du premier.
75. Cette disposition peut présenter un intérêt en supposant qu'un État bénéficiaire a défini ou prévoit de définir ses propres politiques et pratiques en matière de services d'authentification, de certification et d'accréditation et qu'il souhaite établir une équivalence avec celles en vigueur dans d'autres pays, en se fondant sur ces comparaisons.
76. Il est également important de mentionner qu'une telle disposition n'est pas exclusivement applicable aux pays qui ont déjà créé une autorité d'accréditation, puisqu'elle mentionne la possibilité que ce jugement relatif à l'équivalence avec les politiques et pratiques d'autres pays soit également réalisé par un organisme public habilité à réglementer les signatures électroniques.
77. Le Groupe de travail pour le projet HIPCAR a attiré l'attention sur l'aspect pratique que pourrait représenter, pour les États bénéficiaires, l'établissement de politiques ou de réglementations relatives à l'accréditation de la certification de base des entités étrangères. Cela pourrait représenter un autre point de comparaison avec les autres pays pour juger de l'équivalence des politiques et des pratiques concernées.

Article 14. Contrats électroniques

78. L'Article 14 établit les principes généraux relatifs à l'admissibilité des contrats électroniques.
79. Le paragraphe (1) permet que la formation ou l'exécution d'une transaction électronique soit exprimée: i) au moyen d'un enregistrement de transaction au format électronique; ou ii) par une action destinée à entraîner une communication électronique.
80. Le point ii) ci-dessus fournit des exemples d'actions destinées à entraîner des communications électroniques, citant notamment «le fait de toucher l'icône appropriée ou tout autre endroit de l'écran d'un ordinateur ou de cliquer dessus ou de parler (...)».
81. Cette formulation est importante, car elle indique clairement que la plupart des formes récentes d'établissement de contrats électroniques (tels que les «contrats d'achat en ligne») sont également admissibles.
82. Le point ii) fait en outre référence à ce qu'il convient d'appeler les conclusions de contrats en ligne («ou, le cas échéant, en parcourant des pages électroniques dont l'accès n'est autorisé qu'à des conditions expresses préalablement indiquées»).
83. Particulièrement à cet égard, le Groupe de travail pour le projet HIPCAR a considéré que les conclusions de contrats en ligne peuvent ne pas être applicables dans certaines circonstances et a donc décidé de laisser le maintien de ce point à la libre appréciation des États bénéficiaires.
84. Le paragraphe (2) stipule qu'une transaction électronique n'est ni invalide ni non exécutoire pour la seule raison qu'elle est sous forme électronique. Cette affirmation renforce le principe général portant sur l'admissibilité des contrats électroniques.

Article 15. Contrats électroniques automatisés

85. L'Article 15, au paragraphe (2), établit que les contrats électroniques automatisés sont valables et contraignants, à condition que: i) la partie contractante sache ou ait des raisons de savoir que le dispositif achèvera la transaction; et que ii) la partie contractante ait pu revoir les termes du contrat avant sa formation.
86. Dans la mesure où les contrats électroniques automatisés impliquent une interaction du consommateur avec un dispositif électronique qui n'est pas nécessairement capable de répondre aux questions que le consommateur pourrait poser, le consentement du consommateur est un sujet de préoccupation et doit être protégé, conformément aux dispositions du présent Article.

Article 16. Effets d'une erreur lors des transactions avec un agent électronique

87. Les interactions avec les agents électroniques sont sujettes aux erreurs qui peuvent nuire à la validité d'une transaction électronique. L'Article 16 stipule qu'en un tel cas, la transaction électronique n'a aucun effet juridique si: i) la personne fait une erreur importante; ii) la personne concernée n'a pas l'occasion d'empêcher ou de corriger l'erreur; iii) la personne concernée informe rapidement de l'erreur dès qu'elle s'en aperçoit et iv) la personne concernée renvoie la contrepartie reçue en conséquence de l'erreur.
88. Cet Article est important, car il protège les personnes contre les manquements de l'établissement des contrats électroniques par l'intermédiaire des agents électroniques. Cette disposition est la bienvenue, un grand nombre de sites Internet ne semblant pas préparés à traiter les réclamations des consommateurs ayant connu des problèmes pour conclure leur contrat avec des agents électroniques.

Article 17. Manifestations de volonté

89. L'Article 17 établit l'admissibilité générale des déclarations de volonté ou autres déclarations effectuées par des moyens électroniques.
90. Il limite ses effets aux relations entre l'expéditeur et le destinataire de cette communication.
91. Cette portée limitée ne nuit pas à la disposition de l'Article 4.(d) qui exclut les testaments de l'application de ce modèle de texte législatif.

Article 18. Heure et lieu de réception des communications électroniques

92. L'heure et le lieu font partie des éléments essentiels des transactions, y compris lorsque la transaction est conclue sous forme électronique. Par conséquent, une attention particulière devra être accordée à la détermination du moment et du lieu de l'envoi ou de la réception d'une communication électronique pertinente.
93. Le paragraphe (1) établit qu'une communication électronique est envoyée lorsque: i) elle pénètre dans un système d'information hors de contrôle de l'expéditeur ou, si l'expéditeur et le destinataire utilisent le même système d'information, ii) lorsque le destinataire peut la récupérer et la traiter.
94. Le Groupe de travail pour le projet HIPCAR a décidé de laisser le point ii) à la libre appréciation des États bénéficiaires, chaque pays disposant de ses propres politiques juridiques relatives à la conclusion de contrats en général, susceptibles de s'étendre à la conclusion des contrats électroniques.

95. La justification pour conserver le point ii) est qu'il accorde la priorité aux intérêts du destinataire, tandis que la justification pour l'éliminer est qu'il accorde la priorité aux intérêts de l'expéditeur. Par conséquent, il s'agit typiquement d'une question de politique législative que les États bénéficiaires devront résoudre.
96. Le paragraphe (2) reprend les dispositions du paragraphe (1) en établissant le moment de réception d'une communication électronique et en mentionnant les critères permettant de récupérer et de traiter la communication électronique. Par conséquent, les observations concernant les sujets 94 et 95 ci-dessus s'appliquent également au paragraphe (2).
97. Le paragraphe (3) permet aux parties de se mettre d'accord sans tenir compte des dispositions des paragraphes (1) et (2).
98. Ce paragraphe est important dans la mesure où la négociation libre entre les parties peut l'emporter sur les différentes politiques législatives sur le sujet, en particulier lorsque la transaction électronique est conclue entre des parties qui relèvent de juridictions différentes.
99. Le paragraphe (4) détermine le lieu d'envoi et de réception des communications électroniques, en accordant la priorité aux critères d'établissement des parties.
100. Les paragraphes (5) et (6) établissent les critères suivants applicables dans l'éventualité où un expéditeur ou un destinataire dispose de plusieurs établissements commerciaux ou n'en a aucun. Dans ces situations, le lieu envisagé doit être, dans l'ordre i) celui présentant le rapport le plus étroit avec la transaction sous-jacente ou ii) l'établissement principal de la personne concernée, ou iii) le lieu de résidence habituel de la personne concernée.
101. Cette disposition est importante, car, dans de nombreuses transactions électroniques, en particulier pour les transactions conclues sur des sites Internet, il est difficile de trouver l'adresse d'un expéditeur ou d'un destinataire; les paragraphes (4) à (6) fournissent des moyens pratiques de surmonter cette difficulté.

Article 19. Attribution des communications électroniques

102. Compte tenu du fait que les communications électroniques facilitent l'envoi et la réception par l'intermédiaire de tiers et compte tenu de l'existence de communications anonymes, le sujet de l'attribution nécessite une réglementation rigoureuse.
103. Le paragraphe (1) établit que, en règle générale, une communication électronique est celle de la personne qui l'envoie, lorsqu'elle est envoyée directement par la personne concernée ou par un agent électronique en son nom.
104. Il établit également qu'un enregistrement électronique est, dans la relation entre l'expéditeur et le destinataire, attribuable à l'expéditeur lorsqu'il a été envoyé: i) par une personne autorisée par l'expéditeur ou par l'agent électronique de cette personne, ou ii) par l'agent électronique de l'expéditeur.
105. Ce paragraphe est important dans la mesure où il attribue à l'expéditeur la quasi-totalité ou presque toutes les situations possibles dans lesquelles une communication électronique a été envoyée, directement ou indirectement, par l'expéditeur ou en son nom.
106. Le paragraphe (2) traite de situations dans lesquelles le destinataire peut attribuer une certaine communication électronique à l'expéditeur. Cette attribution est possible lorsque: i) le destinataire applique convenablement une procédure préalablement convenue par l'expéditeur à cette fin; ou ii) l'enregistrement électronique reçu par le destinataire est la conséquence d'une action d'une personne dont les relations avec l'expéditeur ou avec son agent ont permis à cette personne d'avoir accès à une méthode que l'expéditeur utilise pour identifier ses enregistrements électroniques comme les siens.

107. Ce paragraphe est important dans la mesure où il permet au destinataire d'attribuer effectivement des communications électroniques à l'expéditeur, en se fondant sur des initiatives qui peuvent être disponibles pour le destinataire.
108. Le paragraphe (3) exclut les possibilités accordées au destinataire par le paragraphe (2) lorsque: i) un destinataire reçoit un avis de l'expéditeur niant que la communication soit la sienne, ou ii) lorsqu'un destinataire sait ou devrait savoir que la communication électronique n'est pas celle de l'expéditeur.
109. Ces exclusions semblent raisonnables dans la mesure où elles sont justifiées par des situations dans lesquelles la bonne foi du destinataire pourrait difficilement être prouvée.

Article 20. Autres règles de droit non modifiées

110. L'Article 20 évite ou réduit les risques de conflit de lois en établissant que rien dans le présent texte législatif ne limite l'application d'une autre loi qui: i) autorise, interdit ou régit expressément l'utilisation d'enregistrements de transactions, y compris une méthode de signature électronique ou de signature électronique avancée; ou ii) exige qu'un enregistrement de transaction soit posté ou affiché de manière spécifique, ou qu'un enregistrement de transaction soit transmis selon une méthode précise.
111. Cet article est important, car il garantit que les situations spécifiques concernant les signatures électroniques ou les enregistrements de transactions peuvent être traitées en conformité avec leur spécificité. Ce texte législatif vise à fournir des lignes directrices et des règles générales relatives aux transactions électroniques. Il assure une ouverture de façon que les situations particulières soient encadrées par d'autres lois ou réglementations.

Article 21. Consentement

112. L'Article 21 établit le principe général selon lequel personne n'est tenu d'utiliser, de fournir ou d'accepter des enregistrements de transactions (électroniques, conformément à la définition de l'Article 3.(28)), des communications électroniques, des signatures électroniques ou des contrats électroniques sans consentement. Cette disposition est conforme aux principes du libre arbitre et de la liberté de l'initiative économique.
113. Le paragraphe (2) stipule que toute personne qui s'engage dans ce type de transactions a le droit: i) de modifier par convention toute disposition relative à la reconnaissance juridique ou à l'équivalence fonctionnelle de communications, signatures ou contrats électroniques; et ii) d'établir des exigences raisonnables sur la manière d'accepter les communications, signatures, ou formes de documents électroniques.
114. Ce paragraphe est important, car il fournit la possibilité d'équilibrer la conclusion des contrats électroniques.
115. Le paragraphe (4) indique que l'accord d'une partie pour conduire une transaction par voie électronique doit être déterminé: i) lorsque la partie est un organisme public, que celui-ci fasse une stipulation expresse rendue disponible; et ii) dans le cas de toute autre partie, en s'appuyant sur le contexte et les circonstances, y compris la conduite de la partie en question.
116. Cette disposition est importante parce qu'elle reconnaît la différence d'application des exigences pour les parties publiques ou privées et parce qu'elle engage à tenir compte d'un grand nombre de facteurs lorsque la partie n'est pas un organisme public.
117. Le paragraphe (6) mentionne que dans les transactions commerciales électroniques les parties sont libres de préciser les certifications et/ou fournisseurs de services d'authentification particuliers ou les catégories de certificats à utiliser en rapport avec les enregistrements ou les signatures électroniques.

118. Cette disposition reconnaît la situation particulière des transactions commerciales, dans lesquelles l'équilibre entre les parties peut dépendre d'un accord sur l'utilisation de services particuliers visant à renforcer la sécurité du processus d'établissement des contrats.

TITRE III – PROTECTION DES CONSOMMATEURS

Article 22. Données obligatoires

119. L'Article 22 introduit, au paragraphe (1), une longue liste de données qui doivent être communiquées par les fournisseurs aux consommateurs ayant conclu une transaction électronique de vente, de location ou d'échange de biens ou de services. Ces données, qui doivent être fournies de façon claire et compréhensible, incluent, entre autres: i) le nom complet et le statut juridique; ii) l'adresse physique et le numéro de téléphone; iii) l'adresse du site Internet et l'adresse électronique; iv) l'adresse physique où le fournisseur recevra la transmission légale des documents; v) les procédures de sécurité et la politique de confidentialité du fournisseur et vi) un canal permettant de recevoir les avis des consommateurs dans la même zone que les communications électroniques initialement utilisées par le fournisseur pour présenter l'offre et/ou promouvoir la transaction.
120. Ce paragraphe est important, car il aide à combler le manque d'informations entre les fournisseurs et les consommateurs, ce qui est relativement fréquent dans l'environnement numérique, où ce manque est parfois masqué par l'apparence de confiance que les sites Internet veulent inspirer.
121. Le paragraphe (2) stipule que les fournisseurs donnent aux consommateurs la possibilité de: i) revoir l'intégralité de la transaction électronique; ii) corriger les éventuelles erreurs; et de iii) se retirer de la transaction juste avant de passer commande.
122. Ce paragraphe est important, car il donne aux consommateurs la possibilité de revoir, de corriger ou d'annuler leur consentement pour une transaction.
123. Le paragraphe (3) indique que, si un fournisseur ne respecte pas les obligations énoncées aux paragraphes (1) et (2), le consommateur peut annuler la transaction dans les quatorze jours suivant la réception des biens ou services.
124. Ce paragraphe est important, car il garantit le droit des consommateurs à mettre un terme à la transaction pour un motif valable.
125. Le paragraphe (4) complète les dispositions du paragraphe (3) en établissant les conséquences de l'annulation de la transaction conformément à ce dernier. Ces conséquences sont: i) le consommateur renvoie les biens ou cesse d'utiliser les services et ii) le fournisseur rembourse tous les paiements, y compris les frais de réexpédition des biens.
126. Le paragraphe (5) impose au fournisseur l'obligation d'utiliser un système de paiement sécurisé, en prenant en compte les normes technologiques et le type de transaction.
127. Ce paragraphe est important, car il protège les consommateurs contre les fraudes qui pourraient se produire avec les systèmes de paiement non sécurisés sélectionnés par les fournisseurs. Cette protection est renforcée par le paragraphe (6), qui confirme la responsabilité du fournisseur pour les éventuels dommages.
128. Le paragraphe (7) indique que le fournisseur doit s'assurer de la disponibilité d'un système de réponse automatisé destiné à accuser réception des communications électroniques envoyées par le consommateur.
129. Cette disposition est importante, car elle protège les consommateurs des retards ou des réfutations du fournisseur concernant la réception des communications du consommateur (y compris à propos de la réception des commandes envoyées par les consommateurs, ou de l'acceptation d'offres d'achat en ligne).

- 130. Les dispositions du présent modèle de texte législatif, qui réglementent l'envoi et la réception de communications électroniques, s'appliquent conjointement avec le présent paragraphe lorsqu'elles ne sont pas en conflit; dans le cas contraire, le présent paragraphe prévaut, car il fournit une protection plus spécifique aux parties les plus vulnérables.
- 131. Le paragraphe (8) établit qu'une transaction électronique est considérée comme conclue dès la réception par le consommateur de la communication électronique du fournisseur confirmant la réception de l'acceptation de l'offre par le consommateur.
- 132. Ce paragraphe est important, car il protège le consommateur de l'allégation du fournisseur selon laquelle le non-respect de l'offre est dû au fait que le fournisseur n'a pas reçu l'acceptation de l'offre par le consommateur, événement qu'il est difficile, voire impossible de vérifier pour les consommateurs.
- 133. La disposition du paragraphe (8) attire l'attention sur un commentaire formulé par le Groupe de travail pour le projet HIPCAR en ce sens où les États bénéficiaires doivent vérifier si les dispositions contenues dans le Titre III sont compatibles avec les lois plus générales de protection des consommateurs en vigueur dans la juridiction des États bénéficiaires.

Article 23. Délai de réflexion

- 134. L'Article 23 réglemente les événements qui autorisent le consommateur à annuler sans raison et sans pénalité toute transaction et tout accord de crédit y afférent dans les sept jours à partir de la réception des biens ou de la conclusion d'un accord de services.
- 135. Le paragraphe (2) établit que les seuls frais susceptibles d'être prélevés au consommateur sont les coûts directs de la réexpédition des biens.
- 136. Le paragraphe (3) stipule que lorsque le paiement pour les biens ou les services a été effectué avant l'annulation de la transaction, le consommateur a droit à un remboursement intégral dans les trente jours suivant la date d'annulation.
- 137. Le paragraphe (4) établit une liste des transactions électroniques exclues de l'application de cet Article, à savoir: i) les services financiers; ii) les transactions conduites comme des ventes aux enchères; iii) les services ayant débuté avant le délai de réflexion; iv) les transactions dont les prix fluctuent en fonction des marchés financiers et ne peuvent pas être contrôlés par le fournisseur; v) les biens fabriqués sur commande, clairement personnalisés, ne pouvant pas être réexpédiés, ou susceptibles de se détériorer ou de se périmérer rapidement; vi) les enregistrements audio ou vidéo ou des logiciels grand public descellés par le consommateur; vii) les journaux, périodiques, magazines ou livres; viii) les services de jeux ou de loterie et ix) les services ou équipements d'hébergement, de transport, de restauration ou de loisirs.
- 138. Ce paragraphe est important, car les biens et services susmentionnés ne justifient pas un délai de réflexion ou l'annulation de la transaction.

Article 24. Messages commerciaux non sollicités

- 139. L'Article 24 protège les consommateurs contre la réception de messages commerciaux non sollicités abusifs.
- 140. Le paragraphe (1) établit que le nombre de destinataires doit être limité à ceux qui ont fait preuve d'un intérêt potentiel envers le sujet de la communication, ce dernier devant être clairement indiqué dans le titre de la communication.
- 141. Cette disposition est importante, car elle protège les consommateurs de l'envoi de propagande non ciblée à des consommateurs potentiellement intéressés. Les messages commerciaux doivent plutôt être pertinents pour les intérêts potentiels ou effectifs des consommateurs.

142. Le paragraphe (1) stipule également que les consommateurs doivent bénéficier de la possibilité de refuser de recevoir d'autres communications et être informés de la source auprès de laquelle le fournisseur a obtenu les données du consommateur.
143. Ce paragraphe est important, car il aide à empêcher toute réception ultérieure de communications non désirées.
144. Le paragraphe (2) qualifie d'infraction le non-respect des obligations imposées par le paragraphe (1) et fait encourir au fournisseur, sur déclaration de culpabilité par procédure sommaire, une amende pour la première condamnation qui sera aggravée dans l'éventualité de condamnations ultérieures. Le montant des amendes a été laissé à la libre appréciation des États bénéficiaires.

TITRE IV – INTERMÉDIAIRES ET FOURNISSEURS DE SERVICES DE TÉLÉCOMMUNICATION

Article 25. Responsabilité

145. L'Article 25 régleme les situations dans lesquelles les intermédiaires ou les fournisseurs de services de télécommunication ne sont pas responsables de la transmission de la communication électronique.
146. Le paragraphe (1) établit que lorsque ces intermédiaires ou fournisseurs de services de télécommunication fournissent un simple canal pour ladite transmission de communications électroniques, ils ne sont pas responsables du contenu concerné s'ils n'ont pas connaissance ou ne sont pas informés des faits qui, pour une personne raisonnable, indiqueraient une probabilité de responsabilité pénale ou de responsabilité civile délictuelle relativement à du matériel sur Internet, ou s'ils ne réagissent pas comme il convient aux notifications de conduites illégales, tant qu'ils: i) ne sont pas à l'origine de la transmission; ii) ne sélectionnent pas le destinataire; iii) réalisent des fonctions de manière technique et automatique, sans sélectionner l'enregistrement électronique et iv) ne modifient pas l'enregistrement électronique contenu dans la transmission.
147. Ce paragraphe est important, car il exempte les intermédiaires ou les fournisseurs de services de télécommunication de toute responsabilité lorsqu'ils ne sont pas informés des actes illégaux ou ne sont pas censés les connaître et qu'ils ne contrôlent pas ces actes illégaux ou ne sont pas censés les contrôler.
148. Le paragraphe (2) indique clairement que la transmission, l'acheminement et la fourniture d'accès exemptés de toute responsabilité en vertu du paragraphe (1) incluent le stockage automatique, intermédiaire et transitoire des informations transmises tant que ce stockage a lieu: i) dans le seul but d'effectuer la transmission dans le système d'information; ii) de manière à les rendre d'ordinaire inaccessibles à quiconque ne fait pas partie des destinataires prévus; et iii) pendant une période ne devant pas être supérieure à ce qui est raisonnablement nécessaire pour la transmission.
149. Ce paragraphe est important, car il caractérise les situations dans lesquelles les intermédiaires ou les fournisseurs de services de télécommunication ne stockent pas les informations transmises à d'autres fins que la réalisation rapide et impersonnelle de leurs services.
150. Le paragraphe (3) établit que les intermédiaires et les fournisseurs de services de télécommunication ne sont pas tenus de surveiller les informations afin de connaître ou de devenir informés d'actes illégaux.
151. Cette disposition est importante, car les intermédiaires et les fournisseurs de services de télécommunication ne peuvent pas mettre en œuvre une surveillance ou une censure permanente des communications entre tiers.

152. Le paragraphe (4) précise que rien dans le présent article n'exempte un intermédiaire ou un fournisseur de services de télécommunication de l'observance d'une ordonnance judiciaire, d'une réglementation, ou d'une obligation contractuelle.
153. Ce paragraphe est important pour affirmer qu'il ne vise pas à remplacer un tribunal particulier, des décisions réglementaires ou contractuelles, mais qu'il vise plutôt à établir des règles générales sur le sujet.
154. Par exemple, il peut exister des situations dans lesquelles une surveillance de l'activité peut être réalisée par des intermédiaires et des fournisseurs de services de télécommunication, comme dans le cas des «espaces de bavardage» dans lesquels l'utilisation de propos offensants ou la publication d'images d'enfants (en particulier de pornographie infantile) pourrait probablement (ou, dans une certaine mesure, certainement) se produire. Dans ces cas, des lois spécifiques ou des ordonnances judiciaires peuvent décider qu'une surveillance est nécessaire.

Article 26. Procédure de traitement des avis d'actes illégaux

155. L'Article 26 établit les procédures à suivre par les intermédiaires et les fournisseurs de services de télécommunication lorsqu'ils ont connaissance d'actes illégaux et qu'ils ont obtenu des utilisateurs de leurs services des informations qui ne peuvent pas raisonnablement indiquer autre chose.
156. Le paragraphe (1) stipule que, dans un tel cas, les intermédiaires et les fournisseurs de services de télécommunication doivent: i) avertir les autorités chargées de l'application de la loi, lorsque les lois pénales en vigueur l'exigent; ii) divulguer l'identité de la personne, lorsque la loi écrite l'autorise et iii) et supprimer les informations ou le message de données du système de traitement de l'information sous leur contrôle et cesser de fournir ou d'offrir de fournir des services relativement à ces informations, lorsque la loi écrite l'autorise.
157. Ce paragraphe est important, car il exige que les avis aux autorités, la divulgation d'identité et la suppression des informations soient effectués uniquement lorsqu'une législation confirme ces procédures. Dans la mesure où ces procédures sont susceptibles de nuire aux droits de personnes qui ne sont pas encore condamnées pour des actes illégaux, il est nécessaire qu'elles soient légitimes en vertu d'une législation existante.
158. Le paragraphe (2) établit que la non-divulgation de la connaissance d'un contenu illégal conformément au paragraphe (1) ci-dessus constitue une infraction. La justification d'une telle disposition est compréhensible dans la mesure où les intermédiaires et les fournisseurs de services de télécommunication ne doivent pas ignorer les informations concernant des actes illégaux dont ils sont informés.
159. Cependant, il convient de noter que le paragraphe (1) subordonne cette obligation d'avis au respect des lois pénales en vigueur. Ces lois ne nécessitent ou n'autorisent par forcément une notification pour tous les types de situations. Par conséquent, il est essentiel d'analyser minutieusement les exigences pertinentes en vigueur dans les lois pénales.

Article 27. Offre de biens et de services dans un environnement sûr

160. L'Article 27 exige des fournisseurs d'offres électroniques de biens et de services qu'ils assurent un environnement raisonnablement sûr et publient les conditions de sûreté pertinentes. Il stipule également que le fournisseur doit informer le consommateur de tout manquement à la sécurité susceptible d'avoir une incidence sur la confidentialité de ses données privées. Cet article est important, car il protège les consommateurs en les empêchant de répondre à des offres placées dans des environnements risqués et oblige les fournisseurs à publier les niveaux de sécurité assurés.

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 Îlet, Sainte-Lucie, du 8 au 12 mars 2010

Participants et observateurs officiellement désignés

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

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 ¹⁰	J Paul
PRESCOD	Kwesi

¹⁰ 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

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 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 (OECS)	FRANCIS	Karlene

Consultants pour le projet HIPCAR participant à l'Atelier

Nom	Prénom
ALMEIDA	Gilberto Martins de
GERCKE	Marco
MORGAN ¹¹	J Paul
PRESCOD	Kwesi

¹¹ Président de l'Atelier.

