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

Protection de la vie privée et des données:

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

Protection de la vie privée et des données:

Modèles de lignes directrices politiques et de textes législatifs

HIPCAR

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

Commission européenne

CARICOM

CTU

ITU

Avis de non-responsabilité

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

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

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

Avant-propos

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

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

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

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

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

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

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

Brahima Sanou
Directeur du BDT

Remerciements

Le présent document représente l'achèvement des activités régionales réalisées dans le cadre du projet HIPCAR « *Enhancing 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 Mme. Karen Stephen-Dalton et M. Kwesi Prescod. 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 Saint-Kitts-et-Nevis du 19 au 22 juillet 2010 (voir Annexes). Les notes explicatives du modèle de texte législatif incluses dans ce document ont été préparées par M. Kwesi Prescod 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.

Les activités ont été mises en œuvre par Mme Kerstin Ludwig, chargée de la coordination des activités dans les Caraïbes (Coordonnatrice du projet HIPCAR) et M. Sandro Bazzanella, chargé de la gestion de l'ensemble du projet couvrant l'Afrique subsaharienne, les Caraïbes et le Pacifique (Directeur du projet UIT-CE-ACP), avec l'appui de Mme Nicole Morain, Assistante du projet HIPCAR, et de Mme Silvia Villar, Assistante du projet UIT-CE-ACP. Le travail a été réalisé sous la direction générale de M. Cosmas Zavazava, Chef du Département de l'appui aux projets et de la gestion des connaissances. Les auteurs du document ont bénéficié des commentaires de la Division Applications TIC et Cybersécurité (CYB) du Bureau de développement des télécommunications (BDT) de l'UIT. Ils ont aussi bénéficié de l'appui de M. Philip Cross, Représentant de zone de l'UIT pour les Caraïbes. L'équipe du Service de composition des publications de l'UIT a été chargée de la publication.

Table des matières

Page

Introduction

1.1 Le projet HIPCAR – objectifs et bénéficiaires

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

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

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

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

1.2 Comité de pilotage du projet et groupes de travail

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

---

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

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

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

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

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

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

1.3 Mise en œuvre et contenu du projet

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

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

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

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

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

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

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

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

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

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

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

Six modèles de cadres étroitement liés

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

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

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

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

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

Élaboration des modèles de textes législatifs

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

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

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

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

Introduction

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

Interaction et chevauchement de la couverture des modèles de textes

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

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

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

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

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

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

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

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

En conclusion

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

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

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

1.5 Ce rapport

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

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

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

Le modèle de texte législatif relatif à la protection de la vie privée et des données a été élaboré en trois phases: 1) rédaction d'un rapport d'évaluation, 2) élaboration de modèles de lignes directrices politiques et 3) rédaction d'un modèle de texte législatif. Le rapport d'évaluation a été préparé en deux étapes par les consultants du projet HIPCAR: Mme Karen Stephen-Dalton pour la première et M. Kwesi Prescod pour la seconde. Les documents ont ensuite été révisés, discutés et adoptés par consensus large des participants lors de deux ateliers de consultation du Groupe de travail du projet HIPCAR sur les questions de société de l'information, qui se sont déroulés à Sainte-Lucie du 8 au 12 mars 2010 et à Saint-Christophe-et-Niévès du 19 au 22 juillet 2010 (voir Annexes). Les Notes explicatives du modèle de texte législatif proposé dans le présent document sont l'œuvre de M. Prescod à la suite, notamment, des questions soulevées lors du deuxième atelier. Ce document contient donc les données et informations valables en juillet 2010.

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

1.6 Importance de l'efficacité des politiques et des lois sur la protection de la vie privée et des données

Le respect de la vie privée fait partie intégrante des droits de l'homme: il est reconnu par plusieurs dispositions de la Déclaration universelle des droits de l'homme, du Pacte international relatif aux droits civils et politiques ou encore des Conventions américaine et européenne relatives aux droits de l'homme. Ce droit, qui protège la vie privée d'une personne contre les ingérences arbitraires, illégales ou abusives, s'applique par extension à la protection des informations à caractère personnel sur cette personne ainsi qu'à la transmission de ces informations.

[3] Cf. HIPCAR « Privacy and Data Protection: Assessment Report », disponible sur www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

Introduction

Une discussion contemporaine sur les cadres de protection de la vie privée et des données serait dépourvue de sens si elle n'évoquait pas l'ubiquité des technologies de l'information et de la communication et la capacité que celles-ci offrent en matière d'analyse, de traitement et de partage des informations. Étant donné que les entreprises cherchent à utiliser de nouveaux circuits pour améliorer leur position concurrentielle sur le marché national ou mondial, l'adoption et le succès de la révolution électronique d'Internet sont indissociables de l'assurance que les informations fournies par les utilisateurs dans le cadre d'une opération sont protégées d'une utilisation à leur insu par des tiers. Ainsi, l'application de cadres de protection de la vie privée et des données soutient les objectifs des lois sur le commerce électronique en fournissant un cadre holistique qui réaffirme l'obligation d'intégrité à l'intérieur du cadre réglementaire plus vaste et renforce sa capacité à protéger le client.

Les lois sur la protection de la vie privée et des données reposent sur le principe qu'une personne doit disposer d'un certain degré de contrôle sur la manière dont les informations à caractère personnel qu'elle confie aux pouvoirs publics ou aux entreprises sont utilisées, traitées ou divulguées. Ce contrôle s'exerce principalement au point de collecte des informations, stade auquel la partie qui les recueille doit divulguer la totalité des motifs pour lesquelles les informations sont collectées et s'engager à restreindre à ces seules fins l'usage des informations à caractère personnel après leur collecte. L'autre grande facilité de contrôle est l'obligation, pour la partie qui collecte, de donner à la personne concernée la possibilité de consulter les informations qu'elle conserve à son sujet. Cela étant, il doit exister des exceptions aux règles générales de restriction de l'utilisation des informations à caractère personnel, imposant l'application de lignes directrices spécifiques et différentes dans les domaines des services médicaux et de la sécurité nationale, lorsqu'il n'est pas commode d'obtenir le consentement de la personne concernée.

De ce fait, les cadres politiques et législatifs relatifs à la protection de la vie privée et des données sont axés uniquement sur la gestion des informations à caractère privé et personnel. Ainsi, ces cadres œuvrent de concert avec les règles relatives à l'accès accordé par l'État aux informations à caractère public et non sensible en sa possession, puisque ces cadres ne traitent pas habituellement de la gestion d'informations à caractère personnel autres que les exceptions générales à ces dispositions légales.

S'il est nécessaire d'accorder une attention particulière à la supervision par l'État, les cadres de protection de la vie privée et des données ne doivent toutefois pas se limiter au secteur public, mais englober toutes les parties qui, dans l'exercice de leurs activités, collectent, conservent et analysent des informations à caractère personnel sur des clients. Les lois en la matière sont cruciales pour mettre en place de façon utile des systèmes d'administration publique en ligne destinés à améliorer l'efficacité de la fourniture de biens et services des pouvoirs publics, mais aussi la compétitivité économique du secteur commercial.

Les administrations et autres organismes chargés de fournir des services publics utilisent traditionnellement, dans le cadre de leur mandat, des informations à caractère personnel concernant les clients du secteur public. Cependant, le mouvement en faveur d'une transparence et d'une équité accrues dans la gestion des affaires publiques entraîne un certain nombre de préoccupations concernant la manière dont il convient d'utiliser ces informations: moyens de limiter l'influence de préjudices injustes fondés sur la race, la religion, l'origine ethnique, le sexe ou l'orientation sexuelle lors de l'attribution de ressources, de biens ou de services publics qui ne sont pas directement liés à ces caractéristiques, ou encore préoccupations concernant les systèmes mis en place pour protéger les informations conservées de l'accès non autorisé de tiers, etc. Par conséquent, tout comme il a été imposé l'obligation de créer des cadres afin de réduire la prise en compte de caractéristiques privées lors de l'évaluation de l'accès aux ressources publiques (sauf lorsque celles-ci sont, de par la loi, le facteur discrétionnaire à la base de la démarche d'évaluation), des protections contre la divulgation ou l'accès non autorisés à des informations à caractère personnel doivent être mises en place en veillant au déploiement d'un niveau minimum adéquat de sécurité de l'information.

Du point de vue du secteur privé, les clients exigent toujours plus de garanties que les informations à caractère personnel recueillies au cours d'une transaction commerciale donnée ne sont pas utilisées, à bon ou à mauvais escient, par des tiers. Ces garanties doivent limiter la vente ou la divulgation d'informations à caractère personnel à des tiers à l'insu ou sans l'accord tacite de la personne concernée.

Introduction

Les lois sur la protection de la vie privée et des données doivent également reconnaître la nature émergente du commerce électronique et l'essor des transferts d'informations internationaux. Les entreprises exploitant les technologies de l'information et de la communication tendent à rechercher des opportunités de rationaliser leurs investissements de manière à réduire les coûts et à accroître les efficiences. Ces stratégies comprennent souvent la compilation en un même lieu des informations collectées lors des transactions. Dans le cas des multinationales, cette volonté se traduit habituellement par la compilation d'informations commerciales en provenance de plusieurs pays sur un même site, qui n'est pas nécessairement situé dans l'une des juridictions sous lesquelles les informations ont été collectées. Dans ce cas, si les règles relatives à la protection des informations à caractère personnel ne sont pas aussi strictes que dans le pays où l'entreprise les recueille, ce déséquilibre peut entraîner une atteinte au respect de la vie privée des personnes dans les principales juridictions d'opération. Ce point est si important que la protection réciproque des informations à caractère personnel est un élément fondamental des accords commerciaux modernes conclus entre les nations et des restrictions réglementaires imposées aux multinationales. L'application de règles pour la protection de la vie privée et des données donne ainsi aux pays la possibilité d'investir de nouveaux secteurs d'activité économique dans les échanges internationaux avec la fourniture de services distants ou à distance et d'en tirer eux aussi profit.

Enfin, l'opportunité économique présentée par le contrôle, l'utilisation et l'analyse d'informations recueillies par des agrégateurs de contenu Web ou des entreprises de marketing a récemment été débattue. Cela a conduit à discuter de la « chaîne de valeur des informations à caractère personnel » et de la reconnaissance du potentiel économique associé aux différents acteurs de cette chaîne. Le cœur de ce cadre de la nouvelle économie de l'information repose sur la reconnaissance des droits d'une personne à exercer un contrôle sur la manière dont des informations à caractère personnel données doivent être utilisées. Par conséquent, la révolution économique générée par Internet prenant de l'ampleur, la mise en œuvre et l'application (et donc la crédibilité) des règles de protection de la vie privée et des données d'une juridiction sont appelées à devenir un avantage concurrentiel majeur pour cette dernière, en tant que priorité d'investissement dans ce secteur d'activité économique florissant, qui implique en grande partie la gestion d'informations à caractère personnel.

L'application de politiques, de législations et de systèmes efficaces pour garantir la protection de la vie privée et des données assure donc des avantages variés substantiels aux pays qui profitent de l'amélioration de la gouvernance et de la démocratie, mais elle les prépare également, avec les entreprises qui y sont implantées, à saisir les nouvelles opportunités de l'ère de l'information. L'application de ces politiques, législations et systèmes doit refléter des cadres administratifs qui limitent les possibilités d'ingérences injustifiées de la part du pouvoir exécutif ou d'une entreprise commerciale, afin de réaffirmer l'importance de la protection de la vie privée et des données pour les règles et les principes d'une bonne gouvernance.

Partie I:
Modèles de lignes directrices politiques:
Protection de la vie privée et des données

Voici des modèles de lignes directrices politiques qu'un pays pourrait prendre en considération en matière de protection de la vie privée et des données.

1. LES PAYS DE LA CARICOM / DU CARIFORUM VISERONT À INTRODUIRE DES CADRES JURIDIQUES ET INSTITUTIONNELS CLAIRS POUR GARANTIR LA PROTECTION DES INFORMATIONS À CARACTÈRE PERSONNEL ET PRIVÉ.

- La loi prévoit un mandat statutaire clair visant à soutenir la mise en place d'un régime qui garantit la protection des informations à caractère personnel et/ou privé.
- Le régime de protection des données ne doit pas être spécifique à une technologie et doit donc être de pertinence égale pour les environnements papier ou TIC.
- Le mandat juridique/statutaire doit affirmer clairement que la loi engage l'État.
- Le mandat juridique/statutaire doit veiller à ce que l'obligation de protection de la vie privée s'applique aux secteurs aussi bien public que privé.
- Le mandat juridique/statutaire identifie clairement un organisme désigné pour l'application du cadre de protection de la vie privée et des données.
- Le mandat juridique/statutaire prévoit clairement l'indépendance de l'organisme désigné.
- Le mandat juridique/statutaire prévoit clairement que les informations à caractère personnel doivent être collectées et traitées avec le consentement de la personne concernée par ces informations.
- Le mandat juridique/statutaire prévoit clairement les circonstances dans lesquelles les informations à caractère personnel peuvent être collectées et traitées sans le consentement ou la notification de la personne concernée par ces informations.
- Le mandat juridique/statutaire doit identifier une catégorie d'informations à caractère personnel dites « sensibles » qui nécessitent un suivi et un contrôle plus stricts.

2. LES PAYS DE LA CARICOM / DU CARIFORUM S'ASSURERONT QUE LES GRANDS PRINCIPES DE LA PROTECTION DES DONNÉES SONT CLAIREMENT DÉFINIS DANS LES LOIS PERTINENTES.

- Les grands principes du cadre de la protection des données sont clairement définis dans les lois.
- Les grands principes de la protection des données doivent comporter des dispositions garantissant qu'au moment de la collecte, la personne concernée est informée de l'usage ou de la finalité de ces données et qu'elle consent clairement à cet usage ou à cette finalité.
- Les grands principes de la protection des données doivent comporter des dispositions conférant à la personne et/ou entité collectant et/ou traitant les informations à caractère personnel la responsabilité de la sécurité, de l'exactitude et de l'utilisation appropriée de ces informations.
- Les grands principes de la protection des données doivent comporter des dispositions instaurant la confiance du public en autorisant la personne concernée à consulter et à vérifier l'exactitude des informations la concernant conservées par quelque personne que ce soit.

- Les grands principes de la protection des données doivent comporter des dispositions limitant le transfert international d'informations à caractère personnel dans des juridictions n'offrant pas de garanties comparables en matière de protection de la vie privée et des données.

3. LES PAYS DE LA CARICOM / DU CARIFORUM VISERONT À METTRE EN PLACE DES CADRES DE GOUVERNANCE APPROPRIÉS CONFÉRANT AUX INSTITUTIONS LES POUVOIRS REQUIS POUR FACILITER LE SUIVI.

- Le mandat juridique/statutaire doit stipuler clairement l'existence de dispositions pour désigner sans ambiguïté les personnes et/ou entités chargées de la collecte, de l'utilisation et du traitement des informations à caractère personnel; ces dispositions peuvent inclure la notification de la personne désignée ou l'enregistrement auprès de cette dernière.
- L'organisme désigné pour garantir la conformité au mandat juridique/statutaire doit être une personne morale distincte ayant le droit de posséder ou de disposer d'actifs, la capacité de conclure des contrats et le pouvoir d'agir en toute indépendance dans l'exercice de ses fonctions.
- Le responsable de l'organisme désigné sera nommé d'une manière garantissant l'indépendance et l'impartialité de ses fonctions.
- Le responsable de l'organisme désigné bénéficiera de conditions d'emploi, notamment en matière d'ancrage de sa position et de conditions de reconduction, qui seront prévues dans le mandat juridique/statutaire et suffiront à limiter les possibilités d'incitation ou de contrainte.
- Le responsable de l'organisme désigné recevra dans le mandat juridique/statutaire les pouvoirs d'investigation nécessaires pour faciliter l'exercice des fonctions relevant du cadre de protection des données.
- Le responsable de l'organisme désigné recevra dans le mandat juridique/statutaire le pouvoir de déléguer une certaine autorité à des agents habilités afin de faciliter l'exercice de ses fonctions.
- L'organisme désigné pourra entreprendre des audits ou des enquêtes sur les opérations des personnes auxquelles s'applique le cadre, que ce soit de son propre chef ou en réponse à des plaintes du public. La personne qui supportera les coûts de ces audits ou enquêtes sera déterminée par la réglementation.
- Les personnes auxquelles la loi s'applique coopéreront avec l'organisme désigné dans l'exercice de ses fonctions, sous peine de sanctions civiles et/ou pénales.
- L'organisme désigné pourra demander certains documents destinés à faciliter ses investigations, demande à laquelle devront obtempérer les personnes concernées. L'organisme pourra bénéficier d'un mandat du tribunal à cette fin si cela se justifie.
- Le mandat juridique/statutaire prévoit que l'organisme désigné pourra bénéficier d'une protection légale pour les actes effectués de bonne foi dans l'exercice de ses fonctions.
- L'organisme désigné présentera chaque année au Parlement/Conseil législatif un compte rendu de ses activités au cours de l'année précédente.
- Le mandat juridique/statutaire précisera la période d'entrée en vigueur de l'organisme désigné lors de la promulgation de la loi.

4. LES PAYS DE LA CARICOM / DU CARIFORUM DÉFINIRONT LES CONDITIONS ET OBLIGATIONS PARTICULIÈRES RELATIVES À LA COLLECTE D'INFORMATIONS À CARACTÈRE PERSONNEL.

- Le mandat juridique/statutaire doit réaffirmer que les pouvoirs publics ne peuvent pas collecter d'informations à caractère personnel autres que celles expressément autorisées par une loi écrite.
- Le mandat juridique/statutaire doit prévoir que la personne concernée sera expressément informée de la finalité de la collecte des informations à caractère personnel et de la pertinence des informations collectées par rapport à cette finalité.
- Le mandat juridique/statutaire doit prévoir que la personne concernée donnera son consentement explicite à la collecte des informations.
- Le mandat juridique/statutaire prévoit la collecte d'informations à caractère personnel uniquement auprès de la personne concernée, sous réserve d'exemptions spécifiques liées à des questions relevant de la sécurité nationale ou de la gestion de la santé.
- Le mandat juridique/statutaire doit prévoir des exemptions claires, précises et limitées de manière à ce qu'il subsiste pour la personne concernée des protections suffisantes contre la collecte de données non justifiées.
- Les lois et réglementations associées doivent inclure des considérations spécifiques afin de garantir un équilibre des pouvoirs adéquat concernant l'accès et l'utilisation d'informations à caractère personnel eu égard aux exemptions identifiées dans les lois générales sur la protection de la vie privée et des données.
- Le mandat juridique/statutaire prévoit que la personne concernée sera informée au moment de la collecte des données de la personne chargée de contrôler les données, de la durée prévue de conservation de ces données et de la manière dont elles seront éliminées à l'expiration de la durée de conservation, sauf dans les circonstances relevant de la gestion de la santé et de la sécurité nationale.
- Le mandat juridique/statutaire limite la collecte d'informations à caractère personnel sensibles, sauf dans des cas et à des fins spécifiés. Ces exceptions peuvent concerner:
  - l'élaboration de statistiques,
  - la gestion de la santé,
  - les conditions d'application de la loi,
  - les prescriptions d'une règle de droit,
  - les prescriptions d'un jugement de tribunal.
- Le mandat juridique/statutaire prévoit des sanctions civiles et pénales en cas de violation des dispositions définies relatives à la collecte d'informations à caractère personnel. Ces sanctions peuvent s'appliquer à la partie chargée de la collecte ou à tout agent ou administrateur dont il peut être prouvé qu'il a enfreint le mandat juridique/statutaire en connaissance de cause.

5. LES PAYS DE LA CARICOM / DU CARIFORUM DÉFINIRONT LES CONDITIONS ET OBLIGATIONS PARTICULIÈRES RELATIVES AU TRAITEMENT D'INFORMATIONS À CARACTÈRE PERSONNEL.

- Le mandat juridique/statutaire restreint l'utilisation ou le traitement des informations par la partie qui les collecte aux finalités spécifiées et consenties par la personne concernée au moment de la collecte.
- Le mandat juridique/statutaire restreint la conservation des informations collectées à la durée nécessaire pour la finalité spécifiée.
- Le mandat juridique/statutaire oblige la partie utilisant les informations (« la partie chargée du traitement ») à s'assurer de la fidélité de l'enregistrement et du traitement de ces informations.
- Le mandat juridique/statutaire oblige la partie chargée du traitement à sauvegarder les informations stockées en mettant en place des systèmes appropriés pour assurer une sécurité adéquate.
- Le mandat juridique/statutaire impose à la partie chargée du traitement de demander la vérification et l'aval de l'organisme désigné avant d'entreprendre certains types de traitement.
- Le mandat juridique/statutaire prévoit que la personne concernée aura accès, à sa demande, aux informations à caractère personnel conservées à son sujet par la partie chargée du traitement.
- Le mandat juridique/statutaire confère au responsable de la partie chargée du traitement le pouvoir discrétionnaire de refuser une demande d'accès aux informations stockées relatives à la personne concernée si:
  - la publication de ces informations compromet l'anonymat d'une autre personne,
  - ou la demande est de nature vexatoire et perturbe de façon excessive le bon déroulement des opérations.
- Le mandat juridique/statutaire prévoit la possibilité de faire appel des décisions du responsable de la partie chargée du traitement auprès de l'organisme désigné.
- Le mandat juridique/statutaire interdit le traitement d'informations à caractère personnel sensibles, sauf dans des cas et à des fins spécifiés. Ces exceptions peuvent concerner:
  - les statistiques,
  - la gestion de la santé,
  - les conditions d'application de la loi,
  - les prescriptions d'une règle de droit,
  - les prescriptions d'un jugement de tribunal.
- Le mandat juridique/statutaire prévoit des sanctions civiles et pénales en cas de violation des dispositions définies relatives à la collecte d'informations à caractère personnel. Ces sanctions pourront s'appliquer à la partie chargée de la collecte ou à tout agent ou administrateur dont il peut être prouvé qu'il a enfreint le mandat juridique/statutaire en connaissance de cause.

6. LES PAYS DE LA CARICOM / DU CARIFORUM DÉFINIRONT LES CONDITIONS ET OBLIGATIONS PARTICULIÈRES RELATIVES À LA DIVULGATION D'INFORMATIONS À CARACTÈRE PERSONNEL.

- Le mandat juridique/statutaire impose à la partie chargée de la collecte, du traitement ou de l'utilisation des informations à caractère personnel de ne pas divulguer ces informations à caractère personnel sans avoir obtenu au préalable le consentement de la personne concernée.
- Le mandat juridique/statutaire prévoit une exception à l'obligation de consentement de la personne concernée dans les conditions prévues par une règle de droit et dans les circonstances relevant de la sécurité nationale, de l'exercice de la justice et de la gestion de la santé.
- Le mandat juridique/statutaire limite le transfert international d'informations à caractère personnel dans des juridictions ne disposant pas de lois et de mécanismes comparables en matière de protection de la vie privée et des données. Dans ce cas, la loi autorise le transfert d'informations uniquement dans la mesure où il n'entraîne pas une altération de la protection des informations de la personne concernée.
- Le mandat juridique/statutaire, nonobstant d'éventuelles restrictions normatives, prévoit qu'un transfert d'informations à caractère personnel pourra être organisé avec le consentement explicite de la personne concernée concernant le transfert des informations dans ladite juridiction, sous réserve que la personne concernée ait été informée des risques qui en découlaient.
- Le mandat juridique/statutaire autorise la divulgation d'informations à caractère personnel en réponse à une demande de la personne concernée. Lorsque cette divulgation peut entraîner celle d'autres informations à diffusion restreinte, le mandat juridique/statutaire prescrit des recommandations appropriées au responsable de la partie chargée du traitement.
- Le mandat juridique/statutaire prévoit des sanctions civiles et pénales en cas de violation des dispositions définies relatives à la divulgation d'informations à caractère personnel. Ces sanctions pourront s'appliquer à la partie chargée du traitement ou à tout agent ou administrateur dont il peut être prouvé qu'il a enfreint les obligations du mandat juridique/statutaire.

Partie II:
Modèle de texte législatif:
Protection de la vie privée et des données

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

Organisation des articles

Partie II

Partie II

TITRE I: PRÉAMBULE

Titre abrégé et entrée en vigueur

1. La présente loi peut être citée sous la dénomination suivante: « loi relative à la protection de la vie privée et des données ». Elle entrera en vigueur [le xxx suivant sa publication au *Journal officiel*].

Objectif

2. La présente loi a pour objet de fournir un cadre législatif favorable pour soutenir le développement d'une culture et de pratiques de protection de la vie privée par différents moyens:

   a. la définition des principes généraux selon lesquels les informations à caractère personnel d'une personne doivent être traitées,

   b. la définition de lignes directrices de gestion (y compris les systèmes et la technologie) auxquelles les personnes chargées de la gestion d'informations à caractère personnel devront souscrire, et

   c. la mise en place d'un cadre administratif garantissant un suivi transparent et une résolution impartiale des litiges, qui renforcera la protection des informations à caractère personnel dans les secteurs aussi bien public que privé.

Définitions

3. 1) Aux fins de la présente loi, les mots et expressions suivants s'entendent au sens qui leur est attribué ci-après:

   a. Les « données » ou « informations » désignent tout enregistrement, document, correspondance, note de service, livre, plan, carte, dessin, illustration, graphique, photographie, film, microfilm ou enregistrement sonore, vidéo ou informatisé et tout autre matériel documentaire, quelles que soient sa forme physique ou ses caractéristiques et toute copie de ceux-ci.

   b. Le « Commissaire chargé des données » désigne le commissaire chargé des données nommé en vertu de l'Article 49 du Titre VII de la présente loi.

   c. Le « Contrôleur des données » désigne une personne qui détermine, seule ou en collaboration ou de concert avec d'autres, à quelles fins et de quelle manière des données à caractère personnel sont ou doivent être collectées, traitées ou divulguées.

   d. La « personne concernée » désigne la personne concernée par des données à caractère personnel.

   e. Le « Ministre » désigne le ministre à qui incombe la responsabilité [des informations/de l'administration publique].

   f. « L'établissement de santé » désigne les institutions inscrites en tant qu'établissement fournissant des soins de santé conformément à [la loi de santé publique pertinente]; cela englobe les hôpitaux, les centres de soins, les dispensaires [et les cabinets médicaux].

   g. Le « professionnel de la santé » désigne un professionnel habilité à exercer la médecine conformément à [la loi de santé publique pertinente].

h. Les « informations à caractère personnel » désignent les informations relatives à un individu identifiable qui sont enregistrées sous quelque forme que ce soit, et notamment:

i. les informations relatives à la nationalité, l'adresse, l'âge ou l'état civil de l'individu,

ii. les informations relatives aux origines raciales ou ethniques de l'individu,

iii. les informations relatives aux opinions ou allégeances politiques de l'individu,

iv. les informations relatives aux convictions religieuses ou autres de nature similaire de l'individu,

v. les informations relatives à la santé physique ou mentale ou à l'état de santé physique ou mental de l'individu,

vi. les informations relatives aux éléments biométriques de l'individu,

vii. les informations relatives à l'orientation sexuelle ou à la vie sexuelle de l'individu,

viii. les informations relatives au casier judiciaire ou à la situation financière de l'individu,

ix. les informations relatives à l'éducation ou aux antécédents professionnels de l'individu,

x. tout numéro ou symbole, ou toute autre indication identificatrice, propre à l'individu,

xi. les points de vue et opinions d'autres personnes sur l'individu.

i. Les « pouvoirs publics » désignent notamment:

i. une chambre du Parlement ou un comité d'une chambre du Parlement,

ii. le Conseil des Ministres institué par la Constitution,

iii. un Ministère, un service ou un département d'un ministère,

iv. des autorités locales,

v. une entreprise ou une entité publique créée par la loi,

vi. une société ou une personne morale créée à des fins publiques, possédée ou contrôlée par l'État,

vii. toute autre entité désignée par le Ministre dans un règlement promulgué dans le cadre de la présente loi pour faire partie des pouvoirs publics aux fins de la présente loi.

j. Le « traitement » et le verbe « traiter » sous ses formes conjuguées, en rapport avec des données, désignent l'obtention, l'enregistrement ou la détention de données ou l'exécution d'une opération ou d'une série d'opérations sur les données, telles que:

i. l'organisation, l'adaptation ou l'altération des données,

ii. la récupération, la consultation ou l'utilisation des données, ou

iii. l'alignement, la combinaison, le blocage, l'effacement ou la destruction des données.

k. Un « fichier pertinent » désigne tout ensemble d'informations concernant des personnes dans la mesure où, bien que ces informations ne fassent pas l'objet d'un traitement automatisé conformément aux instructions données à cette fin, l'ensemble est structuré, soit par référence aux personnes, soit par référence à des critères concernant les personnes, de telle sorte qu'une information spécifique relative à une personne précise soit facilement accessible.

2) Lorsqu'un État membre l'estime justifié, il peut définir comme suit un ensemble particulier d'informations à caractère personnel sensibles:

a. les « informations à caractère personnel sensibles » désignent les informations relatives:

i. aux origines raciales ou ethniques,

ii. aux opinions politiques,

iii. aux convictions religieuses ou autres de nature similaire,

iv. à la santé physique ou mentale ou à l'état de santé physique ou mental,

v. à l'orientation sexuelle ou à la vie sexuelle, ou

vi. au casier judiciaire ou à la situation financière d'une personne.

Engagement de l'État

4. La présente loi engage l'État.

Applicabilité de la loi

5. La présente loi s'applique aux Contrôleurs des données concernant toutes les données:

a. si le Contrôleur des données est établi (par sa résidence habituelle, son siège ou sa succursale) au/en [Nom de l'État membre] et si les données font l'objet d'un traitement dans le cadre des activités de cet établissement ou

b. si le Contrôleur des données n'est pas établi au/en [Nom de l'État membre], mais utilise du matériel au/en [Nom de l'État membre] afin de traiter des données à des finalités autres que le transit par le/la [Nom de l'État membre].

Non-applicabilité de la loi

6. La présente loi:

a. ne limite pas les informations qui, en vertu de la loi, sont normalement mises à la disposition des parties à une action judiciaire,

b. ne porte pas atteinte aux pouvoirs des tribunaux judiciaires ou administratifs de contraindre des témoins à déposer ou de contraindre à la production de pièces ou autres preuves,

c. ne s'applique pas aux notes préparées par ou pour une personne présidant un tribunal de [pays] ou dans un tribunal si ces notes sont préparées pour l'usage personnel de cette personne, dans le cadre d'une action judiciaire.

Principes généraux de protection de la vie privée

7. En vertu de la présente loi, il incombe à toute personne traitant des données à caractère personnel dans le cadre de la conduite de ses affaires d'observer les principes généraux suivants:

a. Les données à caractère personnel feront l'objet d'un traitement juste et légal et, en particulier, leur traitement devra respecter des conditions particulières.

b. Les données à caractère personnel ne pourront être obtenues qu'à des fins légales et spécifiées et ne pourront faire l'objet d'aucun traitement supplémentaire incompatible avec lesdites fins.

c. Les données à caractère personnel devront être appropriées, pertinentes et sans excès en rapport aux fins pour lesquelles elles sont traitées.

d. Les données à caractère personnel seront exactes et, le cas échéant, tenues à jour.

e. Les données à caractère personnel traitées à toute autre fin ne seront pas conservées plus que nécessaire pour ladite fin.

f. Les données à caractère personnel seront traitées dans le respect des droits des personnes concernées conférés par la présente loi.

g. Des mesures techniques et institutionnelles appropriées seront prises afin d'éviter le traitement illégal de données à caractère personnel et la perte, la destruction ou l'endommagement accidentels de ces données.

h. Les données à caractère personnel ne pourront pas être transférées dans un pays ou un territoire extérieur à [*nom de la juridiction*], à moins que ledit pays ou territoire garantisse un niveau suffisant de protection des droits et des libertés des personnes concernées par les données en matière de traitement des données à caractère personnel.

TITRE II: OBLIGATIONS DES CONTRÔLEURS DES DONNÉES

Restriction de la collecte et du traitement des informations à caractère personnel

8. 1) Nul ne peut autoriser la collecte et/ou le traitement de données à caractère personnel à moins d'être enregistré comme Contrôleur des données dans le registre maintenu par le Commissaire chargé des données.

2) Il est interdit de collecter des informations à caractère personnel par ou pour le Contrôleur des données à moins que:

a. la collecte de ces informations ne soit jugée juste et nécessaire dans le cadre d'un accord conclu entre le Contrôleur des données et la personne concernée,

b. la collecte ne soit expressément autorisée par une loi écrite.

Collecte directe des informations à caractère personnel

9. 1) Lorsque le Contrôleur des données requiert des informations à caractère personnel concernant un individu, lesdites informations seront recueillies directement auprès de la personne concernée et avec son consentement explicite.

2) Hormis dans les cas prévus par d'autres lois, la personne concernée a le droit de s'opposer à tout moment au traitement de ces données, pour des motifs impératifs et légitimes, auprès du Contrôleur des données.

3) Nonobstant les dispositions du paragraphe 1, les informations à caractère personnel pourront être collectées auprès de sources autres que la personne concernée lorsque:

a. une autre méthode de collecte est autorisée par l'intéressé, par le Commissaire chargé des données ou par une loi écrite, et que

b. les informations sont recueillies aux fins:

i. de détermination des candidats possibles à une distinction honorifique ou à un prix, notamment un diplôme, une bourse ou un prix honorifique,

ii. d'une procédure devant un tribunal ou une instance judiciaire ou quasi-judiciaire,

iii. de recouvrement d'une dette ou d'une amende ou de versement d'un paiement, ou

iv. d'exécution de la loi.

Information de la personne concernée de la finalité

10. Au moment de la collecte des données à caractère personnel, ou préalablement à celle-ci, le Contrôleur des données est tenu de veiller à ce que la personne concernée soit informée:

a. des finalités de la collecte,

b. des destinataires prévus,

c. du caractère facultatif ou obligatoire des questions posées et des conséquences éventuelles d'un défaut de réponse,

d. le cas échéant, du pouvoir légal autorisant la collecte, et

e. des titre, adresse du bureau, numéro de téléphone et autres coordonnées d'un agent du Contrôleur des données qui pourra renseigner la personne concernée au sujet de la collecte.

Conservation d'informations à caractère personnel

11. Les informations à caractère personnel utilisées par le Contrôleur des données à des fins administratives ne seront conservées par celui-ci, à l'issue de leur utilisation, que pour la durée prévue par la réglementation, de sorte que la personne concernée bénéficie d'une opportunité raisonnable d'accéder à ces informations.

Élimination des informations à caractère personnel

12. Le Contrôleur des données est tenu d'éliminer toutes les informations à caractère personnel dont il a la garde ou le contrôle conformément aux règlements publiés par le Ministre en vertu de la présente loi.

Exactitude des informations à caractère personnel

13. Le Contrôleur des données s'efforce de garantir que les informations à caractère personnel dont il a la garde concernant une personne donnée sont exactes et complètes.

Protection des informations à caractère personnel

14. 1) Le Contrôleur des données est tenu de protéger les informations à caractère personnel dont il a la garde ou le contrôle en prenant des dispositions de sécurité technique et institutionnelle raisonnables pour se prémunir de risques tels que l'accès, la collecte, l'utilisation, l'altération ou la divulgation non autorisés ou l'élimination accidentelle des données.

2) Lorsqu'une autre personne traite des informations à caractère personnel pour le compte du Contrôleur des données, celui-ci veille à ce que cette personne:

a. puisse appliquer les mesures de sécurité qui s'imposent,

b. prenne effectivement les mesures déterminées par le Contrôleur des données.

Compatibilité du traitement des informations à caractère personnel avec leur finalité

15. 1) Il est interdit de traiter les informations à caractère personnel qui sont sous la garde ou le contrôle du Contrôleur des données à des fins autres que celles pour lesquelles ces informations ont été obtenues ou compilées par le Contrôleur des données ou pour un usage incompatible avec ces fins, sans le consentement de la personne concernée.

2) Le traitement des informations à caractère personnel est conforme aux fins auxquelles elles ont été obtenues si le traitement a un lien direct et suffisant avec leur finalité et si cette finalité est compatible avec les critères définis au paragraphe 3.

3) Les informations à caractère personnel ne peuvent être traitées que si:

a. la personne concernée a donné son consentement sans équivoque, ou

b. celui-ci a été donné par un professionnel de la santé exerçant les attributions nécessaires dans un établissement de santé,

c. lorsqu'elles ont été rendues publiques par la personne concernée,

d. à des fins de recherche ou de statistique, conformément à l'Article 17,

e. dans l'intérêt de l'application de la loi et de la sécurité nationale, ou

f. aux fins de déterminer l'accès aux services sociaux,

g. le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou afin de prendre des mesures à la demande de la personne concernée avant la conclusion d'un contrat, ou

h. le traitement est nécessaire à l'observation d'une obligation légale qui incombe au Contrôleur des données, ou

i. le traitement est nécessaire à la protection des intérêts vitaux de la personne concernée, ou

j. le traitement est nécessaire à l'exécution d'une activité menée dans l'intérêt public ou dans l'exercice d'une autorité officielle conférée au Contrôleur des données ou à un tiers auquel les données sont communiquées, ou

k. le traitement est nécessaire à des fins relevant de l'intérêt légitime du Contrôleur des données ou d'un tiers auquel les données à caractère personnel sont communiquées, hormis dans les cas où la protection du droit au respect de la vie privée de la personne concernée prévaut sur cet intérêt.

4) Lorsque la juridiction estime nécessaire de distinguer les « informations à caractère personnel sensibles », elle peut restreindre la collecte et le traitement de ces informations, sous réserve des exceptions associées aux alinéas b à f ci-dessus.

Divulgation des informations à caractère personnel

16. Sauf dans les cas prévus par une autre loi écrite, les informations à caractère personnel qui sont sous le contrôle du Contrôleur des données ne peuvent être divulguées que:

a. aux fins auxquelles les informations ont été collectées par le Contrôleur des données ou pour un usage compatible avec cette fin,

b. à toute autre fin conforme à une loi écrite ou à une ordonnance signée en vertu de cette loi écrite autorisant cette divulgation,

c. aux fins de l'observation d'une assignation à témoin, d'un mandat ou d'une ordonnance émanant d'un tribunal, d'une personne ou d'un organisme ayant compétence pour contraindre à la production d'informations ou aux fins d'observer des règles de procédure en matière de production d'informations,

d. au Procureur général de [nom de la juridiction] pour être utilisées dans une procédure judiciaire impliquant l'État,

e. à un organisme d'enquête précisé par le Ministre dans une ordonnance, à la demande écrite de l'organisme d'enquête, afin d'enquêter sur le respect d'une loi écrite ou de procéder à une enquête légale, si la demande spécifie la finalité et décrit les informations à fournir,

f. par un organisme d'exécution de la loi de [nom de la juridiction] à un autre organisme d'exécution de la loi de [nom de la juridiction] aux fins de l'application d'une loi écrite,

g. à une autorité de police étrangère, en vertu d'un accord écrit, d'un traité ou sous l'autorité du Gouvernement de [nom de la juridiction],

h. si le responsable du Contrôleur des données reconnaît l'existence de circonstances déterminantes ayant une incidence sur la santé ou la sécurité d'une personne et si, sous réserve des dispositions de l'Article 23, paragraphe d, un avis de divulgation est expédié à la dernière adresse connue de la personne concernée par les données,

i. de manière à ce qu'un proche ou un ami d'une personne blessée, malade ou décédée puisse être contacté,

j. aux fins de la collecte des sommes dues par la personne concernée au Gouvernement de [nom de la juridiction] ou au Contrôleur des données,

k. à des fins statistiques lorsque la divulgation est conforme aux prescriptions de l'Article 17, ou

l. à des fins d'archivage lorsque la divulgation est conforme aux prescriptions de l'Article 18.

Divulgation à des fins de recherche ou de statistique

17. Le Contrôleur des données ne peut autoriser la divulgation d'informations à caractère personnel dont il a la garde ou le contrôle à des fins de recherche, y compris de recherche statistique, que dans les cas suivants:

a. l'objectif de la recherche ne peut être raisonnablement atteint sans que ces informations soient fournies sous une forme permettant d'identifier l'individu,

b. les informations sont divulguées à la condition qu'elles ne soient pas utilisées afin de contacter une personne pour participer à une étude,

c. le lien enregistré ne porte pas préjudice à la personne concernée et les avantages découlant du lien enregistré relèvent clairement de l'intérêt public,

d. le responsable du Contrôleur des données concerné a approuvé les conditions relatives aux points suivants:

i. sécurité et confidentialité,

ii. retrait ou destruction des identifiants individuels le plus tôt possible,

iii. interdiction de toute utilisation ou divulgation ultérieure de ces informations sous une forme permettant d'identifier les individus sans l'autorisation expresse du Contrôleur des données, et

e. la personne à laquelle ces informations sont communiquées a signé un contrat l'engageant à respecter les conditions approuvées, la présente loi et les politiques et procédures du Contrôleur des données relatives à la confidentialité des informations à caractère personnel.

Divulgation à des fins d'archivage

18. Les Archives nationales du Gouvernement de [nom de la juridiction] ou les archives du Contrôleur des données peuvent divulguer des informations à caractère personnel ou autoriser la divulgation d'informations de caractère personnel dont elles ont la garde ou le contrôle à des fins d'archivage ou de recherches historiques si:

a. la divulgation ne constitue pas une atteinte injustifiée à la vie professionnelle ou privée,

b. la divulgation est destinée à des recherches historiques et conforme à l'Article 18,

c. les informations concernent une personne décédée depuis au moins […] ans, ou

d. les informations se trouvent dans un dossier existant depuis au moins […] ans.

Limitation concernant les transferts vers des juridictions tierces

19. 1) Sans préjudice des dispositions suivantes, les transferts vers des juridictions tierces de données à caractère personnel destinées à être traitées ne sont autorisés que sous réserve des dispositions de la présente loi, et sous réserve que la juridiction tierce vers laquelle sont transférées les données garantisse des niveaux de protection comparables.

2) L'adéquation du niveau de protection d'une juridiction tierce doit être évaluée au regard de l'ensemble des circonstances entourant l'opération de transfert des données ou une série d'opérations de transfert de données. Une attention particulière doit être accordée à la nature des données, à la finalité et à la durée des opérations de traitement projetées, au pays d'origine et au pays de destination finale, aux règles de droit aussi bien générales que sectorielles en vigueur dans le pays tiers, ainsi qu'aux règles professionnelles et aux mesures de sécurité qui sont observées dans ce pays.

3) Il appartient au Commissaire chargé des données de déterminer si un pays tiers garantit un niveau de protection suffisant. Lors de cette procédure de détermination, le Commissaire chargé des données rendra publics:

a. les pouvoirs publics compétents pour la protection des données dans l'autre juridiction,

b. sa détermination des niveaux comparables de protection fournis, et

c. lorsque les protections sont jugées incompatibles, les aspects des informations à caractère personnel [et des informations à caractère personnel sensibles] qui ne bénéficieraient pas d'une protection suffisante.

4) Lorsque, malgré des niveaux de protection non comparables, le Commissaire chargé des données détermine qu'une forme restreinte de transfert peut être organisée en limitant les atteintes aux droits de la personne concernée conférés par la présente loi, le Commissaire chargé des données peut autoriser ce transfert à la condition que:

a. la personne concernée consente au transfert des informations vers la juridiction tierce, et

b. des censures ou des retraits appropriés sont mis en place concernant les aspects des informations que le Commissaire chargé des données juge opportuns.

5) [Lorsqu'il existe un accord concernant le traitement de données ou d'informations dans une juridiction tierce, une période de transition raisonnable peut être accordée par le Commissaire chargé des données afin de permettre au Contrôleur des données de transférer, le cas échéant, le traitement dans une autre juridiction.]

6) Sous réserve des dispositions des paragraphes 4 et 5, il est interdit de transférer des données à caractère personnel vers une juridiction tierce n'offrant pas de garanties de protection suffisantes.

Codes de pratique

20. Le Commissaire chargé des données est tenu de consulter l'industrie pour promouvoir l'application des Principes généraux de protection de la vie privée par l'élaboration de codes de pratique et en fournissant des moyens tels que:

a. des conseils sur l'élaboration des codes de pratique,

b. des conseils sur les mécanismes conformes de résolution des litiges,

c. l'encouragement d'une formation aux Principes généraux de protection de la vie privée,

d. la collaboration avec des organismes du secteur public et privé en vue de faire connaître les codes de conduite aux consommateurs, et

e. toute action que le Commissaire chargé des données jugera appropriée.

Codes de pratique obligatoires

21. 1) Lorsque, de l'avis du Commissaire chargé des données, l'intérêt général justifie l'élaboration de codes de conduite obligatoires ayant trait à l'application des Principes généraux de protection de la vie privée dans une industrie, un secteur économique ou une activité donnés, le Commissaire chargé des données peut exiger, par ordonnance, l'élaboration d'un code de conduite dont il fixera la date limite d'élaboration.

2) Sous réserve des dispositions du paragraphe 1, lorsqu'il existe un organisme public de réglementation compétent dans une industrie, un secteur économique ou une activité donnés, le Commissaire chargé des données peut demander à celui-ci de superviser l'élaboration du code de conduite de l'industrie, du secteur économique ou de l'activité en question.

Partie II

TITRE III: DROITS DES PERSONNES CONCERNÉES

Droit d'accès aux informations à caractère personnel

22. 1) Tout citoyen et tout résident du/de la [nom de la juridiction] a le droit d'accéder, à sa demande et moyennant le règlement des frais prévus:

a. aux informations à caractère personnel le concernant et versées dans un fichier à cette fin sous la garde et le contrôle du Contrôleur des données,

b. aux autres informations à caractère personnel le concernant placées sous la garde et le contrôle du Contrôleur des données, dans la mesure où il peut fournir des indications suffisamment précises pour que le Contrôleur des données puisse les retrouver aisément.

2) La demande d'accès aux informations à caractère personnel doit être adressée au Contrôleur des données chargé du contrôle du fichier d'informations à caractère personnel ou des informations proprement dites, selon le cas, sous une forme approuvée par le Commissaire chargé des données.

Possibilité de refus du Contrôleur des données

23. 1) Le Contrôleur des données peut refuser de communiquer des informations à caractère personnel à la personne concernée lorsque:

a. leur divulgation constituerait une atteinte injustifiée à la vie privée d'une autre personne,

b. il s'agit d'un dossier des services correctionnels dont la communication pourrait raisonnablement entraîner la divulgation d'informations fournies à titre confidentiel,

c. il s'agit d'informations couvertes par le secret professionnel ou obtenu dans le cadre d'une enquête ou d'une procédure judiciaire,

d. il s'agit d'informations médicales ou de santé pour lesquelles le responsable du Contrôleur des données a des motifs raisonnables de croire que leur divulgation pourrait nuire à la santé ou à la sécurité d'une personne,

e. il s'agit d'informations pour évaluation ou avis recueillies dans le seul but de déterminer la qualification ou l'adéquation à un emploi, l'attribution d'un contrat public ou d'autres avantages, dont la communication entraînerait la divulgation de l'identité d'une source ayant fourni des informations dans des circonstances laissant raisonnablement supposer que cette identité doit demeurer confidentielle.

2) Le responsable du Contrôleur des données peut ignorer les demandes d'une personne à accéder aux informations à caractère personnel la concernant lorsque cela perturberait exagérément les opérations du Contrôleur des données en raison du caractère répétitif ou systématique ou de la nature futile ou vexatoire des demandes.

Censure des informations visées par une exception

24. 1) Le Contrôleur des données s'efforcera de retirer des informations susceptibles d'être mises à la disposition d'une personne demandant l'accès aux informations à caractère personnel la concernant toute information visée par une exception, conformément à l'Article 24, afin de mettre à sa disposition les informations non visées par une exception.

2) Le responsable du Contrôleur des données peut refuser de divulguer l'existence d'informations lorsque la reconnaissance de cette existence révélerait des aspects essentiels du caractère d'exception des informations.

Délégation des droits d'une personne concernée

25. Tout droit ou pouvoir conféré à une personne par la présente loi peut être exercé:

a. en cas de décès de la personne, par son représentant personnel si l'exercice du droit ou du pouvoir est lié à l'administration de son patrimoine,

b. par l'avocat de la personne en vertu d'une procuration,

c. par le tuteur de la personne ou

d. lorsque la personne est âgée de moins de 18 ans, par une personne ayant sa garde légitime.

Délais de réponse à une demande

26. 1) Le responsable du Contrôleur des données à qui il est fait une demande d'accès à des informations à caractère personnel en vertu de l'Article 23 est tenu, dans les […] jours qui suivent la réception de cette demande:

a. d'accorder l'accès total ou partiel, en communiquant les informations à la personne qui en a fait la demande ou

b. de refuser l'accès total ou partiel, en donnant à la personne qui en a fait la demande, par écrit, une réponse précisant:

i. le fait que les informations demandées n'existent pas,

ii. ou la disposition précise de la loi sur laquelle le refus pourrait raisonnablement se fonder si les informations existaient.

iii. dans les deux cas, il informera l'auteur de la demande de son droit de recours auprès du Commissaire chargé des données.

2) Dans le cas où un accès total ou partiel aux informations est accordé, le responsable du Contrôleur des données veille à ce que les informations soient disponibles de manière détaillée et, dans les limites du raisonnable, compréhensibles aux personnes atteintes d'une déficience sensorielle.

Correction d'erreurs dans les informations à caractère personnel conservées

27. 1) Lorsqu'une personne estime que les informations à caractère personnel la concernant sont erronées ou incomplètes, elle peut demander au responsable du Contrôleur des données sous la garde et le contrôle duquel sont placées les données de corriger lesdites informations.

2) Si aucune correction n'est apportée à la suite d'une demande déposée en vertu du paragraphe 1, le responsable du Contrôleur des données doit joindre aux informations les corrections qui ont été demandées, mais non effectuées et aviser la personne qui en a fait la demande qu'aucune correction n'a été effectuée.

3) En cas de correction ou d'annotation des informations à caractère personnel en vertu du présent article, le responsable du Contrôleur des données doit aviser desdites corrections ou annotations toute autre partie ou Contrôleur des données auxquels les informations ont été communiquées au cours de l'année écoulée.

4) Lors de la notification, en vertu du paragraphe 3, d'une correction ou d'une annotation des informations à caractère personnel, le Contrôleur des données doit porter la correction ou l'annotation sur tous les dossiers sous sa garde ou son contrôle dans lesquels elles apparaissent.

TITRE IV: OBLIGATIONS PARTICULIÈRES DES POUVOIRS PUBLICS

Évaluations de l'impact sur la vie privée

28. 1) Chaque Ministère est tenu de préparer, sous la forme prescrite par le Commissaire chargé des données, une évaluation de l'impact sur la vie privée de tout projet d'application, de système, de projet, de programme ou d'activité.

2) Lors de la préparation d'une évaluation de l'impact sur la vie privée, le Ministère concerné est tenu de présenter ladite évaluation au Commissaire chargé des données pour approbation.

3) Lorsqu'il a été déposé une évaluation de l'impact sur la vie privée conformément aux dispositions du paragraphe 2, le Commissaire chargé des données évalue ladite évaluation au regard des Principes généraux de protection de la vie privée et, le cas échéant, soumet au Ministère des recommandations d'amendements afin de garantir sa conformité.

4) Lorsque le Commissaire chargé des données émet des recommandations conformément aux dispositions du paragraphe 3, le Ministère est tenu de procéder aux amendements nécessaires du projet d'application, de système, de projet, de programme ou d'activité.

5) Tout Ministère est tenu d'appliquer, dans la mesure du possible, les mesures découlant de son évaluation de l'impact sur la vie privée afin d'éviter toute atteinte inutile à la vie privée des personnes lors de la conception, de la mise en œuvre ou de l'exécution des applications, systèmes, projets, programmes ou activités.

Fichiers d'informations à caractère personnel

29. Le responsable d'un pouvoir public enregistré en tant que Contrôleur des données veille à ce que soient versées dans un fichier d'informations à caractère personnel toutes les informations à caractère personnel dont le Contrôleur des données a la garde et le contrôle et qui:

a. ont été, sont ou peuvent être utilisées à des fins administratives,

b. sont organisées ou prévues de façon à pouvoir être retrouvées par référence au nom d'un individu ou à un numéro, un symbole ou une indication identificatrice propre à cette personne.

Exemption des Archives nationales

30. Nonobstant les dispositions de l'Article 31, les informations à caractère personnel relevant des Archives du Gouvernement de [nom de la juridiction] qui lui ont été transmises par un pouvoir public à des fins historiques ou d'archives sont exclues des fichiers d'informations à caractère personnel.

Représentant des données à caractère personnel

31. 1) Le Contrôleur des données est tenu d'informer le Commissaire chargé des données de la désignation ou de la relève d'un Représentant des données à caractère personnel.

2) Le Représentant des données à caractère personnel a pour fonctions de veiller en toute indépendance à ce que le Contrôleur des données assure le traitement des données à caractère personnel de manière légale et régulière et conformément aux bonnes pratiques. Dans le cas où le Représentant des données à caractère personnel identifie des irrégularités, il est tenu de les porter à la connaissance du Contrôleur des données.

3) Si le Représentant des données à caractère personnel a lieu de soupçonner que le Contrôleur des données a enfreint les dispositions relatives au traitement des données à caractère personnel, et si aucune rectification n'est apportée au plus tôt après que cette infraction a été soulignée, le Représentant des données à caractère personnel est tenu d'aviser le Commissaire chargé des données de cette situation.

Procédure d'autorisation du partage d'informations

32. Tout pouvoir public envisageant de partager des informations avec d'autres pouvoirs publics est tenu pour cela d'observer un accord présenté sous la forme requise au Commissaire chargé des données, qui donnera son aval.

Commissaire chargé de la publication d'un rapport sur les fichiers d'informations à caractère personnel

33. Le Commissaire chargé des données est tenu de publier périodiquement, et au minimum une fois par an, un index des informations à caractère personnel détenues par les pouvoirs publics et incluant un résumé des renseignements suivants:

a. les fichiers d'informations à caractère personnel sous la garde et le contrôle de chaque pouvoir public,

b. les accords de partage d'informations conclus par un pouvoir public avec d'autres pouvoirs publics ou individus,

c. les activités de concordance des données approuvées par le Commissaire chargé des données,

d. les coordonnées du fonctionnaire auquel doivent être adressées les demandes relatives aux informations à caractère personnel contenues dans le fichier,

e. une déclaration indiquant à quelles fins les informations à caractère personnel contenues dans le fichier de données ont été obtenues ou compilées et une déclaration de leur usage, qui doit être compatible avec les finalités de l'utilisation ou de la divulgation des informations,

f. une déclaration des normes et pratiques en matière de conservation et d'élimination qui sont applicables aux informations à caractère personnel du fichier de données et

g. les évaluations d'impact sur la vie privée préparées par les Ministères concernés.

TITRE V: EXEMPTIONS SPÉCIALES

Fins domestiques

34. Les dispositions des Titres III, IV et V ne s'appliquent pas aux données traitées par une personne à des fins strictement personnelles, familiales ou domestiques ou à des fins récréatives.

Sécurité nationale, crime et fiscalité

35. 1) Le Ministre peut, sur ordonnance publiée au Journal officiel, exempter le Contrôleur des données du respect de certaines dispositions de la présente loi dans l'intérêt de la sécurité nationale.

2) Tout Contrôleur des données au sein des pouvoirs publics est exempté du respect des dispositions des [Titres II et III] si le traitement des données est requis à des fins:

a. de prévention ou de détection des crimes,

b. d'arrestation ou de poursuite de délinquants ou

c. d'estimation ou de recouvrement d'un impôt, d'une taxe, d'un droit ou de toute imposition de nature similaire.

Exemptions de l'applicabilité pour les activités réglementaires

36. 1) Les données à caractère personnel traitées dans l'exercice de fonctions relevant des activités réglementaires requises par une loi écrite sont exemptes des dispositions des Titres II et III de la présente loi dans tous les cas, dans la mesure où l'application de ces dispositions pourrait nuire au bon exercice desdites fonctions.

2) Le paragraphe 1 est applicable à toutes les fonctions pertinentes destinées:

a. à protéger les citoyens contre:

i. les pertes financières occasionnées par la malhonnêteté, la faute professionnelle ou toute autre conduite abusive ou par l'inaptitude ou l'incompétence des personnes concernées par la fourniture de services de banque, d'assurance et d'investissement ou d'autres services financiers ou par la gestion d'entreprise,

ii. les pertes financières occasionnées par les faillites libérées ou non ou

iii. la malhonnêteté, la faute professionnelle ou toute autre conduite abusive, ou l'inaptitude ou l'incompétence des personnes habilitées à exercer une profession ou une activité,

b. à protéger les œuvres caritatives de fautes ou d'une mauvaise gestion (d'un administrateur ou de toute autre personne) dans leur administration,

c. à protéger le patrimoine des œuvres caritatives contre les pertes et les détournements,

d. au recouvrement du patrimoine des œuvres caritatives,

e. à assurer l'hygiène, la sécurité et le bien-être des travailleurs ou

f. à protéger les personnes autres que des travailleurs contre les risques pour l'hygiène ou la sécurité découlant de l'action de travailleurs ou liée à l'action de travailleurs.

Exemptions de l'applicabilité pour le journalisme, les lettres et les arts

37. 1) Les informations à caractère personnel sont exemptes des dispositions des Titres II et III de la présente loi dans les cas particuliers où:

a. Le traitement est entrepris en vue de la publication d'un matériau journalistique, littéraire ou artistique par un individu,

b. Le Contrôleur des données a lieu de croire que, compte tenu notamment de l'importance particulière de l'intérêt public pour la liberté d'expression, la publication présenterait un intérêt public, et

c. Le Contrôleur des données a lieu de croire que, compte tenu des circonstances, le respect des dispositions pertinentes du Titre II serait incompatible avec la finalité journalistique, littéraire ou artistique projetée.

2) En application du paragraphe 1, le Commissaire chargé des données peut instituer des codes de conduite conformes aux dispositions des Articles 21 et 22, susceptibles, le cas échéant, de modifier les dispositions des Titres II et III de manière à trouver un équilibre approprié entre l'objet de la présente loi et le droit à la liberté d'expression en vigueur.

TITRE VI: RECOURS ET APPELS

Droit d'appel d'une décision du Contrôleur des données

38. Toute personne ayant demandé la communication des informations à caractère personnel la concernant en vertu de l'Article 23 ou la correction d'informations à caractère personnel en vertu de l'Article 28 peut faire appel de la décision du responsable du Contrôleur des données auprès du Commissaire chargé des données.

Délai du pourvoi en appel

39. Tout appel auprès du Commissaire chargé des données en vertu de l'Article 39 doit être interjeté dans un délai de […] semaines à compter de la date à laquelle a été reçu l'avis de la décision dont il est fait appel, en déposant auprès du Commissaire chargé des données, par écrit, un avis d'appel.

Possibilité de rejet de l'appel par le Commissaire

40. Le Commissaire chargé des données peut rejeter un appel si l'avis d'appel ne présente pas un motif raisonnable de conclure à l'existence des informations à caractère personnel concernées par l'avis.

Contrôleur des données avisé de l'appel par le Commissaire

41. À réception de l'avis d'appel, le Commissaire chargé des données informe le responsable du Contrôleur des données et toute autre personne concernée de cet avis d'appel.

Autorisation d'un médiateur

42. Le Commissaire chargé des données peut autoriser un médiateur à enquêter sur les circonstances de l'appel et à essayer de trouver un accord sur la question visée par l'appel.

Enquête du Commissaire

43. 1) Le Commissaire chargé des données peut mener une enquête afin d'examiner la décision du responsable du Contrôleur des données, lorsque le Commissaire chargé des données:

a. n'a autorisé aucun médiateur à mener une enquête en vertu de l'Article 43 ou

b. a autorisé un médiateur à mener une enquête en vertu de l'Article 43, sans qu'aucun accord n'ait été trouvé.

2) Lorsque le Commissaire chargé des données mène une enquête en vertu du présent article, il peut, lors de la conclusion de cette enquête:

a. soit confirmer la décision du responsable du Contrôleur des données,

b. soit ordonner au responsable du Contrôleur des données de communiquer les informations à caractère personnel ou d'effectuer les corrections demandées.

Réunions à huis clos

44. L'enquête menée par le Commissaire chargé des données ou par un médiateur et toutes les réunions organisées par le médiateur avec les parties à l'appel peuvent se dérouler à huis clos.

Représentation lors de l'enquête

45. Les personnes faisant appel d'un refus d'accès à des informations à caractère personnel, le responsable du Contrôleur des données concerné et toute partie concernée peuvent être représentés par un avocat ou un agent.

Charge de la preuve au Contrôleur des données

46. Lorsque le Contrôleur des données refuse l'accès à des informations à caractère personnel, la charge de prouver que les informations relèvent de l'une des exceptions visées dans la présente loi selon la prépondérance des probabilités incombe au Contrôleur des données.

Recours devant les tribunaux

47. Chacune des parties peut faire appel de la décision du Commissaire chargé des données devant les tribunaux, conformément à l'Article 80 de la présente loi.

TITRE VII: BUREAU DU COMMISSAIRE CHARGÉ DES DONNÉES

Création du Bureau du Commissaire chargé des données

48. 1) Sous réserve des dispositions du paragraphe 2, il est institué un Commissaire chargé des données, nommé par le [Chef de l'État] après consultation du Premier ministre et du chef de l'opposition.

2) Les fonctions de Commissaire ne peuvent pas être exercées par:

a. un ministre, un secrétaire d'État ou un membre du Parlement,
b. un juge ou un magistrat,
c. un officier ministériel,
d. un membre des autorités locales,
e. une personne ayant un intérêt financier ou autre dans une entreprise ou une activité susceptible d'affecter l'exercice de ses fonctions de Commissaire,
f. un failli non libéré,
g. une personne ayant été condamnée pour des méfaits impliquant la malhonnêteté.

3) Le Commissaire chargé des données emploie du personnel en tant que de besoin, lequel relève de son autorité.

4) Le Commissaire chargé des données n'occupera aucune autre charge rétribuée, que ce soit dans le service public ou autre et n'exercera aucune autre fonction rémunérée.

5) [Le Chef de l'État], après consultation du [Premier ministre et du chef de l'opposition], nomme une personne qualifiée aux fonctions de Commissaire par intérim si:

h. le Commissaire chargé des données démissionne de ses fonctions ou laisse son poste vacant,
i. le Commissaire chargé des données se trouve dans l'incapacité, pour quelque raison que ce soit, d'exercer les fonctions de sa charge,
j. le Commissaire chargé des données estime nécessaire d'être provisoirement relevé de ses fonctions du fait de circonstances qui l'obligeraient à s'abstenir s'il était juge de la Haute Cour.

Les fonctions de Commissaire par intérim sont dissoutes dès lors qu'un Commissaire est nommé pour exercer cette charge à titre permanent ou, le cas échéant, lorsque le Commissaire chargé des données qui se trouvait dans l'incapacité d'exercer les fonctions de sa charge reprend ses fonctions ou, dans le cas d'une charge provisoire, lorsque le Commissaire par intérim a exercé la fonction qui lui a été attribuée.

6) La désignation d'un Commissaire par intérim à titre provisoire, conformément aux alinéas b et c du paragraphe 3, n'est possible que sur présentation d'un certificat signé du Commissaire chargé des données indiquant que, selon lui, le bon exercice des fonctions dévolues par la présente loi au Commissaire chargé des données impose la désignation d'un Commissaire par intérim.

Personnalité juridique et représentation du Commissaire chargé des données

49. 1) Le Commissaire chargé des données bénéficiera d'une personnalité juridique à part entière et aura la capacité, sous réserve des dispositions de la présente loi, de conclure des contrats, d'acquérir, de détenir et de céder tout type de bien nécessaire à l'exercice de ses fonctions, d'engager des poursuites ou d'être poursuivi en justice et de prendre toute mesure et de conclure toute opération relevant de l'exercice de ses fonctions ou favorisant leur exercice en vertu de la présente loi.

2) Tout document censé servir d'instrument produit ou publié par le Commissaire chargé des données et portant sa signature pourra servir de preuve et, à charge de la preuve du contraire, sera considéré comme produit ou publié par le Commissaire chargé des données.

Durée du mandat

50. 1) Le Commissaire chargé des données est nommé pour un mandat renouvelable ne pouvant excéder cinq ans.

2) Sous réserve des dispositions du paragraphe 3, le Commissaire chargé des données quitte ses fonctions:

a. à l'expiration du mandat pour lequel il a été nommé,

b. s'il vient à remplir les conditions énoncées au paragraphe 2 de l'Article 49, ou

c. s'il est nommé à toute autre charge rétribuée ou vient à exercer une autre fonction rémunérée.

3) Le Commissaire chargé des données ne peut être démis de ses fonctions que par le Chef de l'État après [consultation du Premier ministre et du chef de l'opposition] aux motifs de son incapacité à exercer les fonctions de sa charge, incapacité découlant d'une infirmité du corps ou de l'esprit ou de toute autre cause ou en cas de faute.

Rémunération du Commissaire chargé des données et du personnel

51. Le Commissaire chargé des données et son personnel recevront leur rémunération et leurs indemnités sur les sommes fournies par le Fonds consolidé.

Protection du Commissaire chargé des données

52. Aucune action ni procédure en dommages et intérêts ne pourra être instruite à l'encontre d'un Commissaire chargé des données qui aura agi de bonne foi dans l'exercice de l'une de ses fonctions ou d'un pouvoir conféré par la présente loi.

Délégation des pouvoirs du Commissaire

53. Le Commissaire chargé des données pourra déléguer tout ou partie des pouvoirs d'investigation et d'exécution qui lui ont été conférés par la présente loi à un fonctionnaire habilité ou à un agent de police désigné à cet effet par le Commissaire chargé des données.

Indépendance de la charge

54. Dans l'exercice de ses fonctions en vertu de la présente loi, le Commissaire chargé des données agit en toute indépendance. Il ne doit pas être soumis à

l'autorité ou au contrôle de quelque personne ou organisme que ce soit.

Fonctions du Commissaire chargé des données

55. Le Commissaire chargé des données est tenu de:

a. veiller au respect de la présente loi et de la règlementation,

b. créer et maintenir un registre des Contrôleurs des données,

c. exercer un contrôle sur toutes les activités de traitement des données et vérifier, de son propre chef ou à la demande d'une personne concernée, que le traitement des données s'effectue conformément aux dispositions de la présente loi ou de la règlementation,

d. instruire le Contrôleur des données de prendre toutes les mesures nécessaires pour s'assurer que le traitement des données est conforme à la présente loi ou à la règlementation

e. enquêter sur les signalements et réclamations de personnes concernées ou d'associations représentant des personnes concernées relatifs à des infractions à la présente loi ou à la règlementation; prendre toutes les mesures correctives jugées nécessaires par le Commissaire chargé des données ou prescrites par la présente loi; et informer les personnes concernées ou les associations de leurs résultats,

f. publier les indications ou déclarations publiques relevant de la charge du Commissaire chargé des données en vertu de la présente loi,

g. prendre toutes mesures nécessaires pour porter les dispositions de la présente loi à la connaissance du grand public,

h. promouvoir, par l'éducation et la publicité, la compréhension et l'acceptation des principes de la protection des données et des objets de ces principes,

i. conseiller le Gouvernement concernant les mesures législatives requises en matière de protection de la vie privée et des données,

j. de son propre chef ou sur demande, établir un rapport à l'intention du Ministre, en tant que de besoin, sur toute question affectant le respect de la vie privée d'une personne, comportant des recommandations relatives au caractère nécessaire ou souhaitable de mesures législatives, administratives ou autres destinées à assurer ou renforcer la protection de la vie privée de la personne concernée,

k. collaborer avec les autorités de surveillance d'autres pays dans la mesure nécessaire à l'exercice de ses fonctions, en particulier par l'échange d'informations utiles, conformément aux conventions auxquelles [nom de l'État membre] est partie ou à toute autre obligation internationale de [nom de l'État membre],

l. surveiller de manière générale le respect des dispositions de la présente loi par les instances gouvernementales et non gouvernementales,

m. préparer et publier ou approuver, en concertation avec les parties prenantes de l'industrie, des codes de pratique ou des directives appropriées destinées à guider les chefs d'entreprise et les institutions manipulant des données à caractère personnel,

n. entreprendre des recherches et surveiller les progrès des technologies de l'information et du traitement des données afin d'atténuer les éventuels effets néfastes de ces progrès sur la protection des personnes concernées; inclure les résultats de ces recherches et de cette veille, le cas échéant, dans le compte rendu annuel requis par les dispositions de l'Article 72,

o. apporter ses conseils aux Ministres ou aux pouvoirs publics, qu'ils aient été ou non demandés, sur toute question relevant de l'application de la présente loi, et signaler au Ministre, le cas échéant, qu'il est souhaitable que [nom de l'État membre] accepte un instrument international donné relatif à la protection de la vie privée des personnes concernées par les données,

p. prendre toute mesure relevant de l'exercice des fonctions susmentionnées ou favorables à leur exercice et

q. exercer toute autre fonction conférée ou imposée au Commissaire chargé des données par la présente loi ou en vertu de celle-ci, ou par toute autre loi.

Confidentialité et serment

56. 1) Le Commissaire chargé des données et les fonctionnaires habilités sont tenus de prêter serment devant le Chef de l'État selon le texte indiqué dans le Programme.

2) Il est interdit aux personnes exerçant ou ayant exercé les fonctions de Commissaire chargé des données, de membre du personnel du Commissaire chargé des données ou d'agent du Commissaire chargé des données d'utiliser ou de divulguer, de façon directe ou indirecte, des données obtenues à la suite de l'exercice d'un pouvoir ou d'une fonction relevant de la présente loi, hormis:

a. dans les conditions prévues par la présente loi ou par toute autre loi, ou

b. lorsqu'elle y est autorisée par l'ordonnance d'un tribunal.

3) Toute personne qui, sans motif légitime, enfreint les dispositions du paragraphe 2, commet une infraction passible d'une amende ne pouvant excéder […] dollars et d'une peine d'emprisonnement pouvant aller jusqu'à […].

Pouvoirs du Commissaire

57. Le Commissaire chargé des données aura pouvoir, aux fins d'exercer ses fonctions, d'entreprendre toute action qui lui semblera requise, avantageuse ou utile et relative à l'exercice de ses fonctions.

Pouvoir du Commissaire d'obtenir des informations

58. 1) Le Commissaire chargé des données peut, par une note d'information écrite remise à l'intéressé, demander à ce qu'une personne lui fournisse par écrit, dans les délais indiqués:

a. un accès à des données à caractère personnel,

b. des informations et des documents concernant le traitement de données à caractère personnel,

c. des informations relatives à la sécurité du traitement des données à caractère personnel et

d. toute autre information ayant trait aux questions précisées dans la note d'information et jugée nécessaire ou utile, par le Commissaire chargé des données, à l'exercice de ses fonctions ou des pouvoirs et obligations qui lui sont conférés par la présente loi.

2) Lorsque les informations demandées par le Commissaire chargé des données sont stockées sur un ordinateur, un disque, une cassette ou un microfilm ou sous quelque autre support que ce soit ou préservées par un dispositif ou système mécanique ou électronique, la personne citée dans la note d'information est tenue de produire ou de donner accès aux informations concernées sous une forme intelligible, récupérable et transportable.

3) Une loi en vigueur au/en [nom de l'État membre] ou une règle de droit interdisant ou restreignant la divulgation d'informations ne peut dispenser une personne de fournir au Commissaire chargé des données les informations nécessaires ou utiles à l'exercice des fonctions de ce dernier.

4) Le paragraphe 3 ne s'applique pas aux informations qui, de l'avis du Ministre chargé de la sécurité nationale, sont ou ont été conservées dans le but de sauvegarder la sécurité de [nom de l'État membre], ni aux informations exemptées de l'obligation de divulgation lors des procédures d'un tribunal.

Contenu de la note d'information

59. La note d'information mentionnée à l'Article 58 doit indiquer:

a. que la personne à laquelle la note d'information est adressée a le droit, en vertu des dispositions de l'Article 81, de faire appel de l'obligation faite par la note d'information dans un délai de trente jours et

b. le délai accordé pour obtempérer à l'obligation faite par la note d'information, lequel délai ne pourra être exprimé de manière à expirer avant la fin de la période de trente jours indiquée à l'alinéa a.

Défaut ou refus d'obtempérer à la note d'information

60. 1) Nul ne peut omettre ou refuser d'obtempérer, sans motif raisonnable, à une obligation faite par note d'information.

2) Nul ne peut fournir au Commissaire chargé des données des informations que l'on sait inexactes ou trompeuses sur un point important, afin de prétendre obtempérer à une note d'information.

3) Toute personne qui enfreint les dispositions des paragraphes 1 et 2, commet une infraction passible [par déclaration sommaire de culpabilité] d'une amende ne pouvant excéder […] dollars et d'une peine d'emprisonnement pouvant aller jusqu'à […].

4) Pour sa défense, une personne accusée d'infraction en vertu des paragraphes 1 ou 2 pourra prouver qu'elle a pris toutes les mesures nécessaires pour obtempérer à la note d'information.

Insuffisance des informations fournies au titre de la note d'information

61. Si, à la suite d'une demande en vertu des dispositions du paragraphe 1 de l'Article 58, le Commissaire chargé des données n'obtient pas suffisamment d'informations pour conclure à la légalité du traitement des données à caractère personnel, il est en droit d'interdire au Contrôleur des données tout traitement autre que le stockage des données à caractère personnel.

Plaintes auprès du Commissaire et pouvoirs d'investigation

62. 1) Le Commissaire chargé des données peut, à la suite d'une plainte déposée par une personne concernée ou de sa propre initiative, enquêter ou autoriser une enquête pour savoir si des dispositions de la présente loi ou de la règlementation ont été, sont ou pourraient être enfreintes par un Contrôleur des données au sujet d'une personne concernée.

2) Lorsqu'une plainte est déposée auprès du Commissaire chargé des données en vertu du paragraphe 1, celui-ci est tenu:

a. d'enquêter sur la plainte ou d'autoriser une enquête sur celle-ci par un fonctionnaire habilité, à moins que le Commissaire chargé des données n'estime que la plainte soit futile ou vexatoire et

b. d'informer la personne concernée par écrit, dès que les circonstances le permettent, de sa décision à l'égard de la plainte et de la possibilité d'interjeter appel devant un tribunal, en cas de désaccord avec la décision du Commissaire chargé des données, conformément aux dispositions de l'Article 81.

3) Aucune disposition de la présente loi n'interdit au Commissaire chargé des données de recevoir des plaintes et d'enquêter à leur sujet lorsque les plaintes sont déposées par une personne autorisée par écrit par la personne concernée à agir en son nom et toute référence à une personne concernée dans les autres dispositions de la présente loi s'entend au sens d'une référence à la personne ainsi autorisée.

Forme de la plainte

63. 1) Toute plainte déposée en vertu de la présente loi doit être déposée par écrit auprès du Commissaire chargé des données, sauf autorisation contraire de celui-ci.

2) Le Commissaire chargé des données s'efforcera d'apporter toute l'aide possible imposée par les circonstances afin de permettre à une personne souhaitant déposer une plainte auprès du Commissaire chargé des données de déposer sa plainte par écrit.

Avis d'enquête

64. Avant d'enquêter sur une plainte conformément à la présente loi, le Commissaire chargé des données avise le Secrétaire permanent, dans le cas d'un pouvoir public et le premier dirigeant de l'institution, dans tous les autres cas, de son intention d'enquêter et lui fait connaître l'objet de la plainte.

Pouvoirs d'entrée, de recherche et de saisie

65. 1) Sous réserve des dispositions du paragraphe 2, un fonctionnaire habilité accompagné d'un agent de police peut entrer à tout moment dans les locaux afin de procéder à une recherche, d'inspecter, examiner, faire fonctionner et tester le matériel s'y trouvant qui est utilisé ou destiné au traitement des données à caractère personnel et d'inspecter et saisir tout document, équipement ou matériel qu'il y trouve.

2) Un fonctionnaire habilité ne peut entrer dans les locaux pour procéder à des recherches ou à une saisie à moins d'être accompagné par un agent de police et de présenter au propriétaire ou à l'occupant des lieux un mandat émis par [un Magistrat ou l'autorité compétente, selon la juridiction].

Sujets exemptés de l'inspection et de la saisie

66. 1) Les pouvoirs d'inspection et de saisie conférés par un mandat ne sont pas applicables aux données à caractère personnel qui, en vertu du Titre V, sont exemptées d'autres dispositions de la présente loi.

2) Les pouvoirs d'inspection et de saisie conférés par un mandat ne sont pas applicables:

a. aux communications entre un conseiller juridique professionnel et son client relatives à la fourniture de conseils juridiques audit client concernant ses obligations, responsabilités ou droits en vertu de la présente loi,

b. aux communications entre un conseiller juridique professionnel et son client ou entre ce conseiller ou son client et une autre personne, réalisées en lien ou en prévision de poursuites découlant de la présente loi.

Pouvoir du Commissaire de publier un avis d'exécution

67. Lorsque le Commissaire chargé des données estime que le Contrôleur des données enfreint ou a enfreint une disposition de la présente loi, le Commissaire chargé des données peut, en vertu de l'Article 69, remettre au Contrôleur des données un avis d'exécution imposant à ce dernier de prendre les mesures indiquées dans l'avis d'exécution dans le délai éventuellement précisé afin de respecter la disposition concernée.

Avis d'exécution

68. 1) Les avis d'exécution doivent revêtir la forme écrite et:

a. préciser la disposition de la présente loi que le Contrôleur des données enfreint ou a enfreint, selon le Commissaire chargé des données, ainsi que les raisons qui ont amené le Commissaire chargé des données à cette opinion et

b. préciser les mesures que le Commissaire chargé des données exige du Contrôleur des données,

c. sous réserve des dispositions du paragraphe 2, aviser le Contrôleur des données de son droit d'interjeter appel conformément à l'Article [81] et du délai avant lequel l'appel doit être interjeté.

2) Un avis d'exécution peut, sans préjudice de la généralité du paragraphe 1, obliger le Contrôleur des données:

a. à rectifier ou effacer tout ou partie des données concernées ou

b. à ajouter aux données à caractère personnel une déclaration relative aux matières qu'elles traitent avec l'accord du Commissaire chargé des données et relative aux données à caractère personnel qui sont inexactes ou non à jour.

3) Le délai précisé dans un avis d'exécution pour obtempérer à l'une de ses obligations ne pourra être exprimé de manière à expirer avant la fin de la période d'appel indiquée dans l'Article [81].

4) Lorsqu'il obtempère à une obligation en vertu du paragraphe 2, le Contrôleur des données est tenu d'informer le plus rapidement possible et au plus tard 30 jours après la mise en conformité:

a. la personne concernée par les données et

b. lorsque le Commissaire chargé des données l'estime raisonnable, toute personne à laquelle les données ont été communiquées peu avant leur mise en conformité,

de la rectification, de l'effacement ou de la déclaration concernée, si cette mise en conformité modifie de manière importante les données concernées.

5) Le Commissaire chargé des données peut annuler un avis d'exécution. Le cas échéant, il en informera par écrit la personne à laquelle cet avis avait été remis.

Défaut d'obtempérer à l'avis d'exécution

69. 1) Nul ne peut omettre ou refuser d'obtempérer, sans motif raisonnable, à une obligation faite par avis d'exécution.

2) Toute personne qui enfreint les dispositions du paragraphe 1 commet une infraction passible par déclaration sommaire de culpabilité d'une amende ne pouvant excéder […] dollars et d'une peine d'emprisonnement pouvant aller jusqu'à […] mois.

Enquête à huis clos

70. 1) Les enquêtes menées sur les plaintes en vertu de la présente loi sont secrètes.

2) Au cours d'une enquête du Commissaire chargé des données relatives à une plainte au titre de la présente loi, le plaignant, le responsable du Contrôleur des données ou toute autre partie concernée doivent avoir la possibilité de présenter leurs observations au Commissaire chargé des données. Toutefois, nul n'a le droit absolu d'être présent lorsqu'une autre personne présente des observations au Commissaire chargé des données, ni d'y avoir accès ou de faire des commentaires à leur sujet.

Renvoi devant le Directeur général de la police

71. À l'issue d'une enquête, le Commissaire chargé des données est tenu, si l'enquête révèle qu'une infraction pourrait avoir été commise, de renvoyer l'affaire au Directeur général de la police qui prendra les mesures nécessaires.

Rapport annuel

72. Le Commissaire chargé des données est tenu de présenter au Parlement un rapport annuel sur les activités de son bureau dans les […] mois qui précèdent la fin de chaque exercice fiscal.

TITRE VIII: VIOLATION ET APPLICATION DE LA LOI

Personne non enregistrée agissant en tant que Contrôleur des données

73. 1) Toute personne qui collecte, traite ou divulgue des informations à caractère personnel sans s'être préalablement inscrite sur le registre du Commissaire chargé des données ou en dehors d'un accord conclu pour le compte d'un Contrôleur des données enregistré commet une infraction à la présente loi passible par déclaration sommaire de culpabilité d'une amende ne pouvant excéder […] et d'une peine d'emprisonnement de […].

2) Lorsqu'une juridiction estime nécessaire de distinguer les « informations à caractère personnel sensibles », elle peut prévoir des sanctions plus répressives que celles définies dans le paragraphe 1 en cas de collecte, de traitement ou de divulgation de ces informations.

Violation des limitations de transfert vers des juridictions tierces

74. 1) Toute personne enregistrée en tant que Contrôleur des données qui omet d'observer l'une des dispositions de l'Article 19 commet une infraction à la présente loi passible:

a. par déclaration sommaire de culpabilité, d'une amende ne pouvant excéder […] et d'une peine d'emprisonnement de […] et

b. par déclaration de culpabilité par voie d'acte d'accusation, d'une amende ne pouvant excéder […] ou d'une peine d'emprisonnement ne dépassant pas […].

Entrave à un fonctionnaire habilité

75. 1) Il est interdit, dans le cadre de l'exercice des pouvoirs conférés par les Articles 66 et 67:

a. d'entraver ou de faire obstacle à un fonctionnaire habilité dans l'exercice d'une fonction relevant de ses attributions,

b. d'omettre de fournir l'aide ou les informations requises par le fonctionnaire habilité,

c. de refuser à un fonctionnaire habilité l'entrée dans des locaux dans le cadre de l'exercice de ses fonctions,

d. de donner à un fonctionnaire habilité des informations fausses et trompeuses sur un point important.

2) Toute personne qui enfreint les dispositions du paragraphe 1 commet une infraction passible par déclaration sommaire de culpabilité d'une amende ne pouvant excéder […] dollars et d'une peine d'emprisonnement ne dépassant pas […] mois.

Présentation de faux arguments

76. 1) Toute personne demandant l'accès ou la rectification d'informations à caractère personnel sous de faux prétextes commet une infraction passible, par déclaration sommaire de culpabilité, d'une amende ne pouvant excéder […] ou d'une peine d'emprisonnement de […],

2) Toute personne qui fait en connaissance de cause une fausse déclaration dans le but de tromper ou d'essayer de tromper le Commissaire chargé des données dans l'exercice de ses fonctions commet une infraction passible, par déclaration sommaire de culpabilité, d'une amende ne pouvant excéder […] ou d'une peine d'emprisonnement de […].

Violation de la confidentialité

77. Toute personne qui enfreint les obligations de confidentialité définies par l'Article 57 commet une infraction passible, par déclaration sommaire de culpabilité, d'une amende ne pouvant excéder […] ou d'une peine d'emprisonnement de […].

TITRE IX: DIVERS

Protection des dénonciateurs

78. Il est interdit à un employeur d'un pouvoir public ou autre de congédier, de mettre à pied, de rétrograder, d'appliquer des mesures disciplinaires, de harceler ou de désavantager de toute autre manière un employé, au motif que:

a. l'employé agissant de bonne foi et sur la base d'une conviction raisonnable

i. a informé le Commissaire chargé des données que l'employeur ou une autre personne a enfreint ou s'apprête à enfreindre la présente loi,

ii. est intervenu ou a émis l'intention d'intervenir afin d'empêcher quelqu'un d'enfreindre la présente loi, ou

iii. a refusé ou a émis l'intention de refuser d'agir en infraction à la présente loi;

b. l'employeur a lieu de croire que l'employé effectuera l'une des actions décrites à l'alinéa a.

Redevance

79. 1) Le Ministre peut réglementer, en consultation avec l'Autorité désignée:

a. la redevance exigible par un Contrôleur des données ou une catégorie de Contrôleurs des données pour le dépôt d'une demande d'informations à caractère personnel par une personne concernée,

b. la manière dont une redevance exigible en vertu de la présente loi sera calculée, ainsi que son montant maximum.

Règlementation

80. 1) Le Ministre peut réglementer, en concertation avec le Commissaire chargé des données, l'entrée en vigueur des objectifs de la présente loi et toute prescription requise ou autorisée par la présente loi.

2) Nonobstant les dispositions générales du paragraphe 1, la réglementation découlant du présent article peut:

a. prescrire le montant de la redevance à régler au Contrôleur des données,

b. fournir des directives de procédure pour interjeter appel de la décision d'un Contrôleur des données,

c. prescrire tout élément prévu par la présente loi et

d. mettre en œuvre les dispositions de la présente loi.

3) La réglementation adoptée en vertu du présent article sera soumise à la ratification du Parlement.

Rôle des tribunaux

81. 1) Sous réserve des dispositions du paragraphe 2, il peut être interjeté appel devant un tribunal:

a. d'une obligation faite par avis d'exécution ou par note d'information,

b. d'une décision du Commissaire chargé des données relative à une plainte ou

c. d'une décision du Commissaire chargé des données en vertu de l'exercice de ses responsabilités.

2) L'appel doit être interjeté dans un délai de […] jours à compter de la remise de la note concernée à l'intéressé ou, le cas échéant, de la réception par l'intéressé de la notification de refus ou de décision.

3) Le tribunal aura compétence pour traiter, sur demande du Commissaire chargé des données, des affaires impliquant une infraction aux dispositions de la présente loi et rendre les ordonnances appropriées à cet égard.

Partie III:
Notes explicatives
relatives au modèle de texte législatif
sur la protection de la vie privée et des données

INTRODUCTION

1. Ce modèle de texte législatif sur la protection de la vie privée et des données a été préparé dans le cadre d'une série de modèles de textes législatifs afin de rendre possible une « société de l'information » grâce à un projet régional englobant les pays de la CARICOM et la République Dominicaine.

2. La société de l'information est fondée sur le principe de l'utilisation de systèmes de traitement automatisés afin d'améliorer la fourniture des services sur les marchés et aux personnes du monde entier. Avec ce nouveau paradigme, compte tenu de la puissance de traitement des systèmes d'information, les possibilités d'utilisation abusive des informations recueillies sur quelqu'un lors d'une opération augmentent de manière exponentielle. Le fait d'encourager l'utilisation de ces systèmes par le grand public impose de mettre en place des systèmes qui inspirent confiance à l'utilisateur et qui donnent l'assurance que les informations recueillies ne seront pas impunément utilisées de façon injustifiée.

3. Le cadre de protection de la vie privée et des données est un aspect essentiel de ce système élargi d'instauration de la confiance.

4. Le modèle de texte législatif sur la protection de la vie privée et des données du projet HIPCAR se fonde sur des principes politiques élaborés lors des phases précédentes du projet HIPCAR[4]. Ces principes ont examiné les bonnes pratiques internationales en matière d'objectifs, les principaux outils communs et les précédents. Ils ont identifié les positions politiques et les systèmes majeurs qu'il fallait inscrire dans les cadres législatifs de la région[5]. Le modèle de texte législatif cherche à codifier les lignes directrices politiques dans un outil législatif destiné à concilier la démarche contradictoire de clarté des intentions, des structures et des fonctions et l'abstraction nécessaire pour faciliter son adaptation, le cas échéant, dans le cadre législatif de chaque État bénéficiaire du projet HIPCAR.

5. Le modèle de texte législatif sur la protection de la vie privée et des données se décompose en neuf titres et quatre-vingt-un articles.

---

[4] Le titre complet du projet HIPCAR est: « *Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures* » (Renforcer la compétitivité dans les Caraïbes par l'harmonisation des politiques, de la législation et des procédures réglementaires dans le domaine des TIC). Ce projet a démarré en septembre 2008, pour une durée de trois ans, dans le contexte d'un projet cadre englobant les pays ACP qui est financé par l'Union européenne et l'Union internationale des télécommunications (UIT). Ce projet est mis en œuvre par l'UIT, avec le concours du Secrétariat de la Communauté des Caraïbes (CARICOM) et de l'Union des télécommunications des Caraïbes (CTU).

[5] Voir également le chapitre 1.5 du présent document expliquant la méthodologie. Les membres des Groupes de travail du projet HIPCAR comprennent des représentants des ministères et des organismes de réglementation nommés par leurs gouvernements nationaux, les instances régionales compétentes et des observateurs, tels que des opérateurs ou d'autres parties intéressées. Le mandat des Groupes de travail est disponible en anglais à l'adresse www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.

- Le **Titre I** aborde des considérations préliminaires telles que le titre abrégé et l'interprétation de termes particuliers du texte; il traite des questions de champ d'application du texte et définit également les principes généraux de protection de la vie privée inscrits dans le texte.
- Le **Titre II** porte sur l'établissement des obligations générales des pouvoirs publics et des organismes privés pouvant être considérés comme des Contrôleurs des données, qui doivent endosser des responsabilités particulières en ce qui concerne la gestion des informations à caractère personnel sous leur contrôle.
- Le **Titre III** institue le droit général des individus ou des personnes concernées par les données à accéder aux informations à caractère personnel les concernant et à s'assurer de leur exactitude, lorsque ces informations sont détenues par des organismes publics ou privés. Il crée par ailleurs le mécanisme et les procédures permettant de faciliter l'octroi de cet accès.
- Le **Titre IV** identifie les obligations particulières des pouvoirs publics en vertu du texte. Ces obligations concernent les circonstances d'opération particulières des organismes publics.
- Le **Titre V** traite des conditions spéciales dans lesquelles le Contrôleur des données n'est pas tenu de s'assurer préalablement du consentement des personnes concernées avant une divulgation.
- Le **Titre VI** aborde les procédures par lesquelles une personne concernée peut demander la révision d'une décision de refus d'accès d'un Contrôleur des données et, le cas échéant, faire appel de la décision auprès d'un organisme de supervision indépendant.
- Le **Titre VII** fournit le cadre général et les pouvoirs de l'organisme désigné par l'autorité de supervision pour surveiller l'application de la protection de la vie privée et des données et fournit les conditions de réponse aux appels interjetés en vertu des dispositions du Titre VI.
- Le **Titre VIII** définit les infractions particulières aux dispositions du texte, ainsi que les peines qui y sont associées.
- Le **Titre IX** prévoit des considérations diverses, notamment la clarification du rôle des tribunaux, l'établissement d'une approche réglementaire conjointe pour l'application du cadre de supervision. Il établit les pouvoirs nécessaires pour réglementer en vertu du texte.

Partie III

APERÇU GÉNÉRAL DES DISPOSITIONS

TITRE I: PRÉAMBULE

6. Le **Titre I du modèle de texte législatif** (loi) est composé de sept articles. Les premiers articles donnent les dispositions préliminaires, notamment le titre abrégé et l'entrée en vigueur de la loi[6], ainsi que l'objectif général de la loi, afin de servir de cadre interprétatif aux articles présentés ensuite.

Article 3: Interprétations et définitions

7. L'Article 3 donne l'interprétation des termes particuliers en usage dans la loi[7]. Les interprétations des termes décrits ci-dessous revêtent un intérêt particulier.

8. « Données » et « informations » (termes rendus équivalents) soulignent l'interprétation large des formulaires, formats et technologies (électroniques ou autres) applicables, sur lesquels les données peuvent être présentées ou stockées. Ceci est impératif, car, nonobstant la raison d'être dominante associée à l'ubiquité des technologies de l'information et de la communication (TIC), cela assure l'applicabilité de la loi et son intention dans des contextes n'utilisant pas nécessairement des systèmes de TIC[8].

9. La définition du « Contrôleur des données » prévoit de prendre le terme « personnes » au sens large, y compris les parties des secteurs public et privé. On remarquera que la définition ne suggère pas que tous les organismes publics ou privés sont des Contrôleurs des données, limitant l'applicabilité de la loi aux personnes ayant un besoin légitime de traiter des informations à caractère personnel dans la conduite de leurs activités principales[9].

10. Bien que les principes politiques et certains précédents internationaux suggèrent la nécessité de distinguer les « informations à caractère personnel » et les « informations à caractère personnel sensibles », il est souvent apparu que les dispositions concernées étaient largement équivalentes sur le plan du traitement de ces deux types d'information. De ce fait, le modèle de texte législatif propose d'inclure la définition de ces dernières dans les premières. Les informations à caractère personnel sensibles sont essentiellement intégrées aux cadres de protection des données en tant que moyen supplémentaire de traiter des questions de discrimination sexuelle, raciale ou autre de mauvais goût. On y parvient habituellement en limitant davantage le traitement de ces caractéristiques (sexe, orientation sexuelle, opinions politiques, appartenance ethnique ou raciale) en plus des limitations générales prévues par ailleurs dans le cadre législatif et en énonçant des sanctions plus lourdes en cas d'infractions liées à ce sous-ensemble d'informations par rapport à celles applicables pour des informations « non sensibles ». Cela étant, il semble y avoir un consensus général sur le fait que la protection des données n'est peut-être pas le lieu le plus approprié pour ce genre de dispositions. Des indications sont toutefois fournies tout au long du texte législatif dans les domaines pouvant nécessiter une distinction supplémentaire si la juridiction compétente décide d'établir la distinction entre les informations à caractère personnel et les informations à caractère personnel sensibles[10].

---

6 L'auteur des Notes explicatives utilise principalement la notion de « Loi » pour désigner le modèle de texte législatif sur la protection de la vie privée et des données.

7 Principe politique 1.1: « La loi prévoit un mandat statutaire clair visant à soutenir la mise en place d'un régime qui garantit la protection des informations à caractère personnel et/ou privé. »

8 Principe politique 1.2: « Le régime de protection des données ne doit pas être spécifique à une technologie et doit donc être de pertinence égale pour les environnements papier ou TIC. »

9 Principe politique 1.4: « Le mandat juridique/statutaire doit veiller à ce que l'obligation de protection de la vie privée s'applique aux secteurs aussi bien public que privé.»

10 Principe politique 1.9: « Le mandat juridique/statutaire doit identifier une catégorie d'informations à caractère personnel dites « sensibles » qui nécessitent un suivi et un contrôle plus stricts. »

11. « Professionnel de la santé » et « établissement de santé » sont des termes qui exigent une définition appropriée, car ils constituent une base récurrente de la non-applicabilité de la loi pour ce qui touche au consentement des personnes concernées en termes de collecte, de traitement et de divulgation des informations à caractère personnel. Cette exception, comme celle relative aux forces de l'ordre, a pour but de veiller à ce que le cadre de la protection des données ne perturbe pas le déroulement normal de ces services. En règle générale, lors de la fourniture de soins de santé, compte tenu de la nature spécialisée de la profession, il serait absurde de s'attendre à ce que le praticien qui officie soit capable d'identifier toutes les parties auxquelles les informations médicales seront communiquées pour déterminer un diagnostic ou, de façon plus importante, dans le cas d'une situation d'urgence marquée par l'incapacité de la personne concernée. Par conséquent, il est nécessaire de prévoir une exception générale au cadre de la protection des données pour les personnes opérant dans ces milieux spécifiques; ce secteur devra faire l'objet d'un traitement spécifique dans des législations les concernant plus directement. On notera que certaines fonctions administratives n'ayant pas de lien direct avec la fourniture de services de santé doivent tout de même entrer dans le cadre de cette exception.

Article 4: Loi engageant l'État

12. L'Article 4 stipule que la loi engage l'État. Cette disposition est nécessaire, car les lois d'interprétation des États membres expriment une règle bien établie, prononcée dans l'affaire ***Procureur général c. Hancock [1940] 1 KB 427***, selon laquelle un texte de loi n'engage pas l'État ou n'a pas d'incidence sur son droit à moins que cela ne soit expressément spécifié dans la loi[11].

Article 5: Juridiction compétente de la loi

13. Reconnaissant la nature multinationale de certaines entreprises et le contexte mondialisé du commerce que favorise l'utilisation des TIC, l'Article 5 tente de clarifier les frontières juridictionnelles de la loi, concernant les Contrôleurs des données qui peuvent être établis dans une juridiction donnée (où l'applicabilité est certaine) et les Contrôleurs des données qui peuvent ne pas être établis ou résider dans la juridiction, mais qui utilisent néanmoins des ressources qui y sont situées. Cet article est particulièrement important au regard des dispositions de l'Article 22.

Article 6: Limitation de l'applicabilité de la loi

14. L'Article 6 limite ensuite l'applicabilité de la loi pour ce qui touche à la limitation des informations mises à la disposition des tribunaux en vertu du droit.

Article 7: Aperçu général des Principes de protection de la vie privée

15. Ce Titre présente également, dans l'Article 7, les principes de protection de la vie privée que la loi entend incarner dans l'exécution d'entreprises du secteur public et privé[12]. Ces principes se fondent sur différents précédents de l'OCDE et de l'UE:

Principe de la responsabilité

Tout Contrôleur des données doit être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

11 Principe politique 1.5: « Le mandat juridique/statutaire doit affirmer clairement que la loi engage l'État. »

12 Principe politique 2.1: « Les grands principes du cadre de la protection des données sont clairement définis dans [la loi]. »

Principe de la limitation en matière de collecte

Il convient d'assigner des limites à la collecte des données à caractère personnel. Toute donnée de ce type doit être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement[13].

Principe de la qualité des données

Les données à caractère personnel doivent être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles doivent être exactes, complètes et tenues à jour.

Principe de la spécification des finalités

Les finalités en vue desquelles les données à caractère personnel sont collectées doivent être déterminées au plus tard au moment de la collecte des données et lesdites données ne doivent être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui soient déterminées dès leur modification[14].

Principe de la limitation de l'utilisation

Les données à caractère personnel ne doivent pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au principe de la spécification des finalités, si ce n'est:

a) avec le consentement de la personne concernée ou
b) lorsqu'une règle de droit le permet.

Principe des garanties de sécurité

Il convient de protéger les données à caractère personnel, grâce à des garanties de sécurité raisonnable, contre des risques tels que la perte des données ou leur accès, destruction, utilisation ou divulgation non autorisés.

Principe de la transparence

Il convient d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques ayant trait aux données à caractère personnel. Il doit être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données à caractère personnel et les finalités principales de leur utilisation, de même que l'identité du Contrôleur des données et le siège habituel de ses activités.

Principe de la participation individuelle

Toute personne physique doit avoir le droit:

a) d'obtenir du Contrôleur des données ou par d'autres voies la confirmation du fait que le Contrôleur des données détient ou non des données la concernant,
b) de se faire communiquer les données la concernant:
   • dans un délai raisonnable,
   • moyennant, éventuellement, une redevance modérée,
   • selon des modalités raisonnables et
   • sous une forme qui lui soit aisément intelligible;
c) d'être informée des raisons pour lesquelles une demande présentée conformément aux paragraphes a et b est rejetée et de pouvoir contester un tel rejet;

[13] Principe politique 1.7: « Le mandat juridique/statutaire prévoit clairement que les informations à caractère personnel doivent être collectées et traitées avec le consentement de la personne concernée par ces informations. »

[14] Principe politique 2.2: « Les grands principes de la protection des données doivent comporter des dispositions garantissant qu'au moment de la collecte, la personne concernée est informée de l'usage ou de la finalité de ces données et consent clairement à cet usage ou à cette finalité. »

d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger[15].

TITRE II: OBLIGATIONS GÉNÉRALES DES CONTRÔLEURS DES DONNÉES

16. Le **Titre II du modèle de loi** définit les règles que doivent observer tous les Contrôleurs des données lors de l'application des principes de protection de la vie privée énoncés au Titre I.

Article 8: Enregistrement des Contrôleurs des données

17. L'Article 8 prévoit l'inscription des Contrôleurs des données sur un registre et la maintenance de ce registre par le Commissaire chargé des données. Dans le cas où il serait préféré un processus de notification moins contraignant, celui-ci peut être organisé ici[16]. Dans les deux cas, cela permettrait de respecter les ***Principes de responsabilité et de transparence de l'OCDE*****,** en vertu desquels il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques ayant trait aux données à caractère personnel et aux ressources permettant de déterminer l'existence et la nature des données à caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du Contrôleur des données et le siège habituel de ses activités. De même, l'Article 8, paragraphe 2, garantit le respect du ***Principe de la limitation de la collecte de l'OCDE*****,** en vertu duquel il convient d'assigner des limites à la collecte des données à caractère personnel et toute donnée de ce type doit être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement[17,18]. Il est nécessaire de répéter que la personne concernée doit obligatoirement connaître la finalité de la collecte, de l'utilisation, de la divulgation et savoir qu'elle peut donner ou refuser son consentement. Le consentement explicite (communiqué oralement ou par écrit) est normalement obligatoire, mais le consentement peut être implicite dans certains cas limités. Le consentement doit également être volontaire, porter sur les informations en question et ne pas avoir été obtenu par tromperie ou sous la contrainte. Il peut également être retiré ou limité par la personne qui l'accorde, chaque fois que le consentement (implicite ou explicite) est requis.

Article 9: Limitation des informations à caractère personnel à collecter

18. Ces dernières obligations, associées au présent principe, sont énoncées par l'Article 9, en même temps que l'injonction selon laquelle, lorsque c'est possible, les informations doivent toujours être obtenues directement auprès de la personne concernée. Conformément à cet article, les Contrôleurs des données doivent s'assurer qu'ils peuvent présenter la finalité de la collecte des données à caractère personnel et les noms des destinataires prévus de celles-ci. En dépit de ces droits d'ordre général, l'Article 9, paragraphe 2, décrit les cas particuliers dans lesquels il ne serait pas pratique pour l'organisme collectant les informations à caractère personnel de se renseigner directement auprès des personnes concernées[19].

---

15 Principe politique 2.3: « Les grands principes de la protection des données doivent comporter des dispositions conférant à la personne et/ou entité collectant et/ou traitant les informations à caractère personnel la responsabilité de la sécurité, de l'exactitude et de l'utilisation appropriée de ces informations.. »

16 Principe politique 3.1: « Le mandat juridique/statutaire doit stipuler clairement l'existence de dispositions pour désigner sans ambiguïté les personnes et/ou entités chargées de la collecte, de l'utilisation et du traitement des informations à caractère personnel; ces dispositions peuvent inclure la notification de la personne désignée ou l'enregistrement auprès de cette dernière. »

17 Principe politique 4.1: « Le mandat juridique/statutaire doit réaffirmer que les pouvoirs publics ne peuvent collecter d'informations à caractère personnel autres que celles expressément autorisées par [la loi]. »

18 Principe politique 4.3: « Le mandat juridique/statutaire doit prévoir que la personne concernée donnera son consentement explicite à la collecte des informations. »

19 Principe politique 1.8: « Le mandat juridique/statutaire prévoit clairement les circonstances dans lesquelles les informations à caractère personnel peuvent être collectées et traitées sans le consentement ou la notification de la personne concernée par ces informations. »

Article 10: La finalité de la collecte des informations doit être précisée

19. L'Article 10 établit un cadre garantissant le respect du ***Principe de la spécification des finalités de l'OCDE***, en vertu duquel les finalités en vue desquelles les données à caractère personnel sont collectées doivent être déterminées au plus tard au moment de la collecte des données. De ce fait, la personne concernée peut déterminer si elle consent ou non à la collecte de ces informations en tant que de besoin pour atteindre cette finalité. En outre, le Contrôleur des données est donc obligé de détruire les données à caractère personnel lorsqu'elles ne sont plus nécessaires. Pour cela, il doit appliquer les pratiques correspondantes en matière de gestion des fichiers, notamment les méthodes de stockage et d'élimination sécurisés.

Article 11: Limitation de la conservation des informations à caractère personnel

20. L'Article 11 établit par conséquent des limitations à la conservation de ces informations, qui ne seront conservées que pour la durée nécessaire aux finalités auxquelles elles ont été collectées et aux autres obligations (conformément à l'Article 13 de la présente loi et à d'autres textes) pour lesquelles la personne concernée a le droit d'accéder aux informations.

Article 12: Élimination appropriée des informations à caractère personnel

21. Conformément à cette définition des considérations de conservation, l'Article 12 fournit de même la définition d'une élimination appropriée des informations conformes aux bonnes pratiques en matière de gestion des dossiers. Afin de permettre la consultation (et la flexibilité) nécessaire concernant la durée de conservation appropriée qui serait applicable en concertation avec des parties prenantes plus nombreuses (y compris, dans le cas de dossiers publics, les Archives nationales d'une juridiction), la détermination finale de cette durée est renvoyée à la règlementation qui viendra appuyer la loi principale.

Article 13: Exactitude des informations à caractère personnel

22. L'Article 13 du modèle de loi assure le respect du ***Principe de la qualité des données de l'OCDE***. En conjonction avec l'Article 28 du Titre III, cet article définit un cadre selon lequel les Contrôleurs des données sont responsables de l'exactitude des informations conservées ou destinées à être utilisées à des fins de traitement.

Article 14: Sécurité des informations à caractère personnel

23. L'Article 14 du modèle de loi assure le respect du ***Principe des garanties de sécurité de l'OCDE***, en vertu duquel les données à caractère personnel doivent être protégées par des garanties de sécurité raisonnable, contre des risques tels que:

    a) la perte des données ou

    b) leur accès,
       i. destruction,
       ii. utilisation,
       iii. modification ou
       iv. divulgation non autorisés.

Les garanties de sécurité doivent être adaptées au niveau de sensibilité des informations à caractère personnel. La disposition elle-même n'entend pas prescrire un type particulier de sécurité de l'information au Contrôleur des données. Une supervision appropriée du respect des lignes directrices, codes et, dans le cas des pouvoirs publics, des évaluations de risque approuvées, apportera la flexibilité nécessaire à l'organisme désigné.

Article 15: Limitation de l'utilisation des informations à caractère personnel

24. L'Article 15 garantit le respect du ***Principe de la limitation de l'utilisation de l'OCDE***, en vertu duquel les données à caractère personnel ne doivent pas être traitées à des fins autres que celles spécifiées conformément au ***Principe de la spécification des finalités*** évoqué plus haut, dans la mesure où le consentement est habituellement requis pour toute collecte, utilisation et divulgation de données à caractère personnel[20]. On notera que, bien que le projet prévoie qu'un Contrôleur des données puisse obtenir l'autorisation de la personne concernée après une collecte, cette pratique doit être découragée. Les Contrôleurs des données sont tenus d'accorder aux personnes concernées des informations et un contrôle sur les données à caractère personnel les concernant, sans interférer avec les échanges d'informations licites et appropriés destinés à permettre et à soutenir le commerce électronique. Nonobstant ce principe général, il existe des cas dans lesquels les informations collectées devront être traitées à d'autres fins ou divulguées à d'autres parties spécifiées pour le bien public. Pour que cette disposition ne soit pas modifiée en profondeur, les exceptions seront déterminées par la Loi. Les situations dans lesquelles le traitement des informations à caractère personnel relève des exceptions au ***Principe général de la limitation de l'utilisation*** sont énoncées au **Titre V**.

25. On notera que le paragraphe 4 prévoit l'identification d'un traitement différent pour les « informations à caractère personnel sensibles » à distinguer des « informations à caractère personnel ». Il est possible de glaner des exemples d'applications potentielles dans les juridictions de l'UE, dans lesquelles il est expressément interdit aux Contrôleurs des données de traiter des informations à caractère personnel sensibles sauf dans certaines exceptions[21], alors que les informations à caractère personnel peuvent être traitées dès lors que le traitement est compatible avec la finalité de la collecte initiale, conformément aux dispositions de l'Article 15. Par conséquent, en vertu du ***Principe de la limitation de la collecte***, il va de soi que les informations à caractère personnel sensibles ne doivent pas être collectées, hormis dans les cas visés par des exceptions identifiées. Il existe des exceptions notables à cette restriction (de la collecte et) du traitement, qui sont encore plus limitées que dans le cas d'informations à caractère personnel:

    a) l'utilisation par un professionnel de la santé dans les circonstances particulières de l'exercice de ses obligations médicales et soignantes dans un établissement de santé,

    b) l'utilisation par les forces de l'ordre et le personnel de sécurité dans le cadre express de la prévention, de la répression ou de la détection des crimes ou d'autres cas relevant de la sécurité nationale,

    c) l'utilisation pour déterminer la qualification à un service social spécifié pour lequel ces informations sont nécessaires.

[20] Principe politique 5.1: « Le mandat juridique/statutaire restreint l'utilisation ou le traitement des informations par la partie qui les collecte aux finalités spécifiées et consenties par la personne concernée au moment de la collecte. »

[21] Principe politique 5.9: « Le mandat juridique/statutaire interdit le traitement d'informations à caractère personnel sensibles, sauf dans des cas et à des fins spécifiés. »

26. Les Articles 16, 17 et 18 décrivent dans quels cas les informations à caractère personnel peuvent être divulguées sans le consentement préalable de la personne concernée. Ces situations sont notamment les suivantes.

Article 16: Divulgation d'informations à caractère personnel conformément à la finalité de leur collecte

27. L'Article 16 autorise la divulgation d'informations à caractère personnel à des fins compatibles avec la finalité à laquelle la collecte et le traitement ont été consentis par la personne concernée, à l'exception des informations recueillies en vertu d'une loi écrite, des actions d'application de la loi, d'une procédure judiciaire ou au profit de la santé publique[22].

Article 17: Divulgation d'informations à caractère personnel aux fins de recherche et de statistique

28. L'Article 17 autorise la divulgation d'informations à caractère personnel afin d'entreprendre des travaux de recherche et d'analyse statistique, sous réserve que le Contrôleur des données soit assuré que les conditions de sécurité sont préservées et que la partie destinataire prévoie d'observer les dispositions de la loi.

Article 18: Divulgation d'informations à caractère personnel aux fins d'archivage

29. L'Article 18 autorise la divulgation d'informations à caractère personnel aux fins d'archivage, sous réserve que les informations répondent à des critères particuliers, ou que la personne concernée soit décédée depuis une période spécifiée. Sur le fond, cette clause permet aux informations à caractère personnel remises aux institutions et aux instances d'archives concernant un défunt dont on estime qu'il présente un intérêt national ou culturel autre d'échapper au champ d'application des obligations de ce modèle de loi. En l'absence d'une disposition de ce type, la Loi interdirait le fonctionnement d'instances telles que les Archives nationales, qui revêtent une importance considérable pour la préservation de la culture et de l'histoire nationales.

Article 19: Limitation du transfert d'informations à caractère personnel vers d'autres juridictions

30. On retiendra principalement, pour ce qui touche au stockage d'informations à caractère personnel, que l'Article 19 du Titre I limite l'activité des Contrôleurs des données dans ce domaine à la juridiction où la loi est applicable ou aux juridictions disposant de lois équivalentes sur la protection de la vie privée. Dans le premier cas, le Contrôleur des données est tenu d'obtenir l'accord préalable:

    a) du Commissaire chargé des données et

    b) de la personne concernée.

[22] Principe politique 6.2: « Le mandat juridique/statutaire prévoit une exception à l'obligation de consentement de la personne concernée dans les conditions prévues par une règle de droit et dans les circonstances relevant de la sécurité nationale, de l'exercice de la justice et de la gestion de la santé. »

Le Contrôleur des données a l'obligation de communiquer aux personnes concernées l'identité de l'administrateur des lois relatives à la protection de la vie privée dans l'autre juridiction[23]. Une disposition transitoire est prévue dans le paragraphe 5, en reconnaissance du fait que certaines entreprises multirégionales peuvent avoir organisé leurs activités en fonction de plateformes de données régionales, ainsi que du fait que l'on ne peut raisonnablement s'attendre à ce qu'une disposition telle que l'Article 19 puisse être appliquée simultanément dans la région. Le Commissaire chargé des données peut ainsi prescrire un délai raisonnable à la migration des plateformes de données vers des juridictions convenablement protégées avant la prise d'effet des sanctions.

31. Les articles 20 et 21 du Titre II autorisent le Commissaire chargé des données à recourir à une approche réglementaire concertée lorsqu'il le juge approprié, de manière à concilier au mieux les impératifs réglementaires de ses fonctions et un impact et des coûts minimaux pour l'industrie concernée.

Article 20: Création de Codes de conduite

32. L'Article 20 prévoit l'élaboration de Codes de conduite sur un plan sectoriel. Qu'ils soient volontaires ou obligatoires, ces Codes de conduite sont jugés essentiels pour permettre au secteur privé d'observer les principes généraux de protection de la vie privée définis dans le Titre I. Par ailleurs, le paragraphe 2 autorise le Commissaire chargé des données à demander aux organismes de réglementation du secteur ou de l'industrie, lorsqu'ils existent, d'élaborer ces Codes de conduite.

Article 21: Codes de conduite obligatoires

33. Le Titre II prévoit, lorsque les Codes de conduite sont jugés obligatoires, que le Ministre peut les instituer par règlementation, sous réserve de la ratification du Parlement.

TITRE III: DROITS DES PERSONNES CONCERNÉES

34. Le **Titre III du modèle de loi** traite des droits des personnes concernées pour ce qui touche à l'accès aux informations à caractère personnel détenues par un Contrôleur des données. Le ***Principe de la participation individuelle de l'OCDE*** prévoit que toute personne a le droit d'obtenir d'un Contrôleur des données confirmation du fait que le Contrôleur des données détient ou non des données la concernant, d'accéder à ces informations, de pouvoir contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

Article 22: Droit d'accès d'une personne aux informations à caractère personnel la concernant

35. La législation et la jurisprudence permettent habituellement aux personnes d'avoir pleinement accès aux informations à caractère personnel les concernant, à quelques exceptions très limitées. Il est donc normal que la législation sur la protection de la vie privée perpétue ce droit, accordé à

[23] Principe politique 6.3: « Le mandat juridique/statutaire limite le transfert international d'informations à caractère personnel dans des juridictions ne disposant pas de lois et de mécanismes comparables en matière de protection de la vie privée et des données. Dans ce cas, la loi autorise le transfert d'informations uniquement dans la mesure où il n'entraînera pas une altération de la protection des informations de la personne concernée. »
Principe politique 6.4: « Le mandat juridique/statutaire, nonobstant d'éventuelles restrictions normatives, prévoit qu'un transfert d'informations à caractère personnel pourra être organisé avec le consentement explicite de la personne concernée concernant le transfert des informations dans ladite juridiction, sous réserve que la personne concernée ait été informée des risques qui en découlaient. »

titre général par les dispositions de l'Article 22[24]. Cependant, certains détails méritent d'être approfondis. Le droit d'accès aux données à caractère personnel n'est pas absolu, car il existe certaines exceptions limitées à ce droit.

Article 23: Le Contrôleur des données peut refuser l'accès

36. L'Article 23 prévoit le cadre dans lequel un Contrôleur des données peut refuser l'accès à une personne qui en fait la demande. Le Contrôleur des données est alors tenu de justifier sa décision s'il refuse l'accès à tout ou partie d'un document. Constituent notamment des exceptions les cas dans lesquels une demande d'accès est refusée afin de protéger l'intéressé ou un tiers[25] ou en raison de considérations établies ayant trait à la protection de l'information, par exemple s'il s'agit d'informations couvertes par le secret professionnel (p.ex. entre un avocat et son client), si elles ont été recueillies dans le cadre d'une enquête ou si elles sont principalement destinées à une procédure judiciaire.

37. Par ailleurs, si la grande majorité des personnes est censée demander les informations les concernant de façon raisonnable, il convient tout aussi raisonnablement de prévoir que certaines puissent, à l'occasion, demander ces informations sans autre motif que d'entraver le travail du Contrôleur des données. Une personne pourrait ainsi déposer des demandes d'accès aux informations chaque semaine, alors que ces informations ont déjà été communiquées et qu'elles n'ont pas été actualisées depuis. Dans ce cas, il peut être approprié d'autoriser le Contrôleur des données à refuser cette demande. Comme dans la plupart des cas de refus d'un droit, c'est au Contrôleur des données qu'il revient de justifier son refus. L'Article 23, paragraphe 2 prévoit cette éventualité et donne au Contrôleur des données les bases d'un tel refus.

Article 24: Censure des informations visées par une exception

38. L'Article 24 vise à donner des indications au Contrôleur des données sur la marche à suivre lorsque le fait de répondre à une demande d'accès peut entraîner la divulgation d'informations à caractère personnel sur un tiers. Dans la mesure du possible, il est proposé que les informations qui entraîneraient cette divulgation collatérale non désirée soient retirées des informations demandées avant leur communication.

39. Le paragraphe 2 précise que l'obligation de protéger des informations à caractère personnel concernant autrui qui incombe au Contrôleur des données s'étend à la limitation de la reconnaissance de l'existence de certaines informations.

Article 25: Une personne concernée peut déléguer ses droits à un tiers

40. L'Article 25 autorise la délégation de certains droits d'une personne concernée à une autre personne. Le principal droit délégué dans le contexte de la présente loi est le droit de consentir à la collecte, au traitement ou à la divulgation d'informations à caractère personnel. Cet article prévoit que le consentement peut être accordé par la personne elle-même ou par son délégué. Dans les situations où une autre personne est amenée à agir pour le compte de l'intéressé, par exemple lorsque la personne concernée est mineure, lorsqu'elle n'est pas en mesure, pour des raisons de santé, de donner son consentement (si elle est inconsciente, par exemple) ou lorsqu'elle est décédée, la législation prévoit une hiérarchie, conforme aux lois relatives à la

[24] Principe politique 6.5: « Le mandat juridique/statutaire autorise la divulgation d'informations à caractère personnel en réponse à une demande de la personne concernée. Lorsque cette divulgation peut entraîner celle d'autres informations à diffusion restreinte, le mandat juridique/statutaire prescrit les recommandations appropriées au responsable de la partie chargée du traitement. »

[25] Principe politique 6.5, *sic*.

responsabilité parentale, des personnes à qui il sera demandé de prendre des décisions éclairées pour le compte de la personne concernée.

Article 26: Délais de réponse aux demandes

41. L'Article 26 fixe un objectif de performance large que les Contrôleurs de données devront atteindre pour ce qui a trait aux réponses aux demandes des personnes concernées. Cet indicateur de référence vise à encourager les Contrôleurs des données, entre autres, à instituer et appliquer un système de gestion de la réception et des réponses aux demandes. Ce système pourra inclure la définition de procédures standard que les personnes concernées devront suivre lorsqu'elles font la demande d'une copie des données à caractère personnel les concernant: formulaires à remplir, période de disponibilité des dossiers, montant de la redevance (le cas échéant), etc.

Article 27: Correction d'erreurs dans les informations à caractère personnel conservées

42. Conformément au Principe de l'OCDE, la législation relative à la protection de la vie privée prévoit un autre droit des personnes concernées, à savoir celui de demander la rectification des informations. C'est l'objet de l'Article 27. Il peut arriver que la rectification souhaitée par une personne concernée soit une erreur factuelle (mauvaise date de naissance, par exemple). Bien que dans ces circonstances les règles professionnelles ou institutionnelles ne permettent pas toujours la modification d'un dossier, ce cadre autorise le Contrôleur des données à mentionner sur le dossier que les informations à caractère personnel ont été vérifiées et à faire apparaître les informations exactes. Le Contrôleur des données peut également joindre un avis de désaccord, précisant le désaccord de la personne concernée avec les informations portées au dossier.

TITRE IV: OBLIGATIONS OPÉRATIONNELLES PARTICULIÈRES DES POUVOIRS PUBLICS

43. Le **Titre IV du modèle de loi** décrit les règles particulières applicables aux responsables des pouvoirs publics en application des principes de protection de la vie privée définis au Titre I et en accord avec les lignes directrices générales énoncées dans le Titre II. Ces obligations particulières visent à garantir la mise en place par la loi de systèmes appropriés de contrôle afin de faciliter le suivi de l'application des Principes de protection de la vie privée.

Article 28: Évaluations de l'impact sur la vie privée

44. Parmi les exemples notables de tels systèmes, on trouve dans l'Article 28 du Titre IV l'obligation faite aux pouvoirs publics de préparer des évaluations de l'impact sur la vie privée pour les opérations existantes ou prévues de traitement des informations, conformément aux directives du Commissaire chargé des données. Ces évaluations de l'impact peuvent servir de base à une démarche réglementaire conjointe des pouvoirs publics et du Commissaire chargé des données donnant effet à une démarche *ex ante* d'autorisation des fonctions de traitement. Bien que cela puisse occasionner des retards administratifs lors de la mise en place d'un nouveau système de traitement, ce sera globalement profitable à la flexibilité et à la réactivité des pouvoirs publics, par rapport à une démarche *ex post* ou *ad hoc* d'autorisation des fonctions de traitement.

Article 29: Fichiers d'informations à caractère personnel

45. L'Article 29 prévoit une obligation fonctionnelle des pouvoirs publics qui, encore une fois, est structurée pour aider le Commissaire chargé des données dans son travail en garantissant le respect des obligations de la loi. L'obligation réglementaire d'instituer des fichiers particuliers d'informations dans le but d'assurer le stockage principal et la gestion de toutes les informations à caractère personnel relevant des pouvoirs publics favorise l'efficacité des autres systèmes qui pourraient être appliqués. Nonobstant cette obligation d'ordre général, il convient de reconnaître que les Archives nationales peuvent gérer les informations à caractère personnel destinées, par nature, à être archivées.

Article 30: Exemption des Archives nationales

46. L'Article 30 prévoit l'exemption particulière des Archives nationales par rapport aux dispositions de l'Article 29, dans la mesure où les informations mises à la disposition du public par l'intermédiaire des Archives nationales ne relèvent habituellement pas du champ d'application envisagé par la création de fichiers d'informations à caractère personnel.

Article 31: Création d'agents de liaison au sein des Contrôleurs des données

47. Conformément à la démarche générale visant à instituer des obligations fonctionnelles particulières pour les pouvoirs publics afin de permettre la supervision de la protection de la vie privée, l'Article 31 prévoit que les pouvoirs publics pourront désigner des agents de liaison au sein de leurs organisations afin de faciliter l'évaluation interne des systèmes et des fonctions en vertu de la loi relative à la protection des données. Ainsi, les avantages opérationnels devraient s'accumuler à mesure que les pouvoirs publics structurent activement leurs systèmes et processus en vue de respecter les principes de protection de la vie privée et les dispositions de la loi à ce sujet, et grâce aux voies de communication améliorée avec le Bureau du Commissaire chargé des données. Si cela peut sembler adapté au fonctionnement d'un pouvoir public, cette disposition peut ne pas convenir à certaines entreprises privées. C'est pourquoi cette disposition est considérée comme une obligation spécifique au secteur public.

Article 32: Autorisation préalable requise pour les accords de partage d'informations

48. L'Article 32 facilite ensuite le partage d'informations entre les ministères, conformément aux directives établies par le Commissaire chargé des données et/ou à l'accord conclu avec lui. C'est une condition indispensable à la mise en place de services d'administration publique en ligne.

Article 33: Publication d'un rapport sur les fichiers d'informations par le Commissaire chargé des données

49. L'Article 33 impose au Commissaire chargé des données de publier un rapport sur l'état des différents mécanismes et instruments institués par le Titre IV afin de surveiller la gestion des informations à caractère personnel acquises par les pouvoirs publics. Cela facilitera la diffusion au public des informations détenues par un pouvoir public donné en temps voulu et donnera aux personnes concernées la visibilité nécessaire pour s'appuyer sur les dispositions du Titre III et exercer leur droit d'accès aux informations les concernant.

TITRE V: EXEMPTIONS SPÉCIALES

50. Le **Titre V du modèle de loi** prévoit les dispositions générales autorisant le Ministre compétent à apporter par ordonnance des amendements à l'applicabilité des dispositions du Titre II pour des groupes identifiés de Contrôleurs des données, à des fins ou dans des circonstances particulières. Ces clauses s'appuient en grande partie sur ce qui a été mis en place en Grande-Bretagne et à Malte, en fonction des directives pertinentes de la Commission européenne.

Article 34: Usage personnel ou familial

51. L'Article 34 explicite le fait qu'une personne peut utiliser des informations à caractère personnel lorsque celles-ci sont utilisées pour des raisons personnelles ou familiales.

Article 35: Sécurité nationale, crime et fiscalité

52. L'Article 35 prévoit des exceptions particulières aux Titres II, III et IV de la loi, conformément aux bonnes pratiques internationales en la matière. Ces exceptions sont largement formulées dans des précédents relatifs au traitement de données à caractère personnel et à la libre circulation de ces données, lorsque ces restrictions constituent une mesure nécessaire visant à sauvegarder:

    a) la sûreté et la défense nationales, ou la sécurité publique,

    b) la prévention, les investigations, la détection et les poursuites en matière pénale, ou la violation de règles déontologiques dans les professions réglementées,

    c) un intérêt économique ou financier important dans une juridiction, y compris en matière monétaire, budgétaire et fiscale.

Article 36: Exemption des affaires réglementaires

53. L'Article 36 précise les exceptions dans le cas de fonctions de surveillance, d'inspection ou de réglementation liées, y compris à titre occasionnel, à l'exercice d'une autorité officielle, à la protection de la personne concernée ou aux droits et libertés d'autrui.

Article 37: Exceptions relatives au journalisme et aux arts

54. L'Article 37 précise les exceptions à l'applicabilité relatives aux activités associées aux libertés d'expression existantes, notamment la réalisation de travaux de nature journalistique, littéraire ou artistique. Cette clause se fonde sur des clauses similaires appliquées en Europe dans des cadres relatifs à la protection des données. Des protections adéquates contre la diffamation sont habituellement déjà en place afin d'offrir un moyen de protection aux personnes concernées, sans restriction inutile des activités. En outre, l'article autorise le Commissaire chargé des données à instituer des codes sectoriels qui permettront de concilier plus facilement l'objet de la loi et le droit à la liberté d'expression en vigueur.

Partie III

TITRE VI: RECOURS ET APPEL DES DÉCISIONS DES CONTRÔLEURS DES DONNÉES

55. Le **Titre VI du modèle de loi** autorise une personne concernée par des données à faire appel et/ou à solliciter la révision d'une décision d'un Contrôleur des données auprès du Commissaire chargé des données26. Cette partie est essentielle, car elle permet à la personne concernée d'obliger un Contrôleur des données à appliquer un traitement loyal grâce au recours à une autorité indépendante.

Article 38: Droit d'une personne concernée à faire appel d'une décision

56. L'Article 38 prévoit le droit général de recours d'une personne insatisfaite du résultat d'une demande déposée conformément aux dispositions des articles 23 (droit d'accès aux informations à caractère personnel la concernant) et 28 (droit de demander la rectification des informations à caractère personnel la concernant). L'article autorise à faire appel de la décision en question auprès du Commissaire chargé des données, qui a compétence pour résoudre ce litige.

Article 39: Délai du pourvoi en appel pour la personne concernée

57. Les Articles 39 à 41 organisent le processus général permettant l'acceptation d'un recours par le Commissaire chargé des données. L'Article 39 détermine le délai maximum autorisé, à compter de la date de la décision, pour interjeter appel, afin de permettre un prompt démarrage de la procédure.

Article 40: Possibilité de rejet de l'appel par le Commissaire chargé des données

58. L'Article 40 autorise le Commissaire chargé des données à rejeter un appel avant la notification du responsable du Contrôleur des données s'il estime que l'appel n'est pas fondé.

Article 41: Notification du Contrôleur des données par le Commissaire chargé des données

59. Conformément aux procédures standard, l'Article 41 impose au Commissaire chargé des données d'aviser le responsable du Contrôleur des données de l'appel interjeté concernant une décision de ce dernier.

60. Les Articles 42 à 46 prévoient le mécanisme général par lequel le Commissaire chargé des données peut utiliser d'autres méthodes de résolution des litiges lors de la résolution de l'appel.

Article 42: Désignation d'un médiateur ou rôle d'arbitre du Commissaire chargé des données

61. En vertu de l'Article 42, le Commissaire peut nommer un médiateur afin de résoudre le litige et aller jusqu'à tenir le rôle d'arbitre en sa qualité de Commissaire.

[26] Principe politique 5.8: « Le mandat juridique/statutaire prévoit la possibilité de faire appel des décisions du responsable de la partie chargée du traitement auprès de l'organisme désigné. »

Article 43: Enquête du Commissaire

62. On notera que l'Article 43 autorise le Commissaire chargé des données à mener une enquête en réponse à un recours, à l'issue de laquelle la décision rendue aura force obligatoire pour les parties.

63. Les Articles 44 à 46 prévoient les conditions procédurales et opérationnelles dans lesquelles se déroule cette enquête.

Article 44: Enquêtes à huis clos

64. L'Article 44 établit le pouvoir discrétionnaire du Commissaire chargé des données de mener ces enquêtes à huis clos.

Article 45: Représentation des parties à une enquête

65. L'Article 45 autorise chacune des parties à être représentée par un avocat ou autre agissant en son nom lors de l'enquête.

Article 46: Charge de la preuve lors de l'enquête

66. L'Article 46 définit les principes juridiques du déroulement de l'audience de l'enquête, conférant la charge de la preuve à la partie jugée avoir plus de ressources à sa disposition, le Contrôleur des données.

Article 47: Recours devant les tribunaux en appel de la décision d'une enquête

67. L'Article 47 donne compétence aux tribunaux en cas d'appel d'une décision rendue à la suite d'une enquête.

TITRE VII: CRÉATION, FONCTIONS ET POUVOIRS DE L'AUTORITÉ DÉSIGNÉE, LE COMMISSAIRE CHARGÉ DES DONNÉES

68. Le **Titre VII du modèle de loi** institue le Bureau du Commissaire chargé des données. Il s'agit d'un élément crucial au bon fonctionnement du cadre législatif sur la protection de la vie privée. L'obligation d'une surveillance indépendante est essentielle pour s'assurer de la conformité des Contrôleurs des données du secteur public aussi bien que privé. Il est à noter que, bien que cette partie soit rédigée comme si le responsable de cet organisme est une personne (le « Commissaire chargé des données »), cet organisme peut tout aussi bien être dirigé par un groupe de personnes: la « Commission chargée des données », « l'Autorité chargée des données », etc. Les juridictions conservent un pouvoir discrétionnaire sur la forme de gouvernance privilégiée pour cet organisme de supervision. Il est toutefois indispensable que cet organisme soit indépendant du pouvoir exécutif politique, et qu'il jouisse d'une autonomie suffisante vis-à-vis de certains intérêts du secteur privé qui entreraient sous le coup de la présente loi en raison de la nature de leur activité.

Article 48: Création du Bureau du Commissaire chargé des données

69. Au regard de l'importance de cette fonction, afin de s'assurer que la surveillance du respect de la vie privée n'est entachée d'aucune impression de parti-pris à l'égard des groupes de Contrôleurs des données, l'Article 48 prévoit la désignation et le renvoi d'un Commissaire chargé de la protection des données indépendant de la même manière et avec les mêmes critères de

qualification qu'un Commissaire parlementaire ou un Médiateur27, le Commissaire ne pouvant être relevé de ses fonctions sans motif valable.

70. En cas d'absence du Commissaire chargé des données, l'article prévoit également la désignation à titre temporaire d'un Commissaire jusqu'à ce qu'un nouveau titulaire soit désigné.

71. La législation peut également prévoir des dispositions pour désigner un Commissaire adjoint chargé des données, qui agira pour le compte du Commissaire en cas de besoin. Ensuite, l'article s'assure que le Commissaire ne perçoit aucune rétribution et n'est soumis à aucune obligation expresse ou allégeance qui pourrait susciter une impression de parti-pris28. Cet aspect de la disposition peut être amendé en fonction du modèle de gouvernance proposé et des préoccupations logistiques de chaque juridiction. Il est proposé dans ce modèle de texte essentiellement en raison du fait que la fonction réglementaire traditionnelle du pouvoir exécutif sur le marché doit, dans le cas présent, s'appliquer également au secteur public. Cependant, étant donné qu'un groupe de Contrôleurs des données peut être constitué d'entreprises du secteur public ou quasi public sur lesquelles le pouvoir exécutif politique conserverait un certain pouvoir de surveillance administrative, le cadre de gouvernance générale prévoit:

   a) la réalisation de rapports destinés au ministre compétent sur l'état de la protection de la vie privée dans le secteur privé,

   b) la réalisation de rapports destinés au parlement sur l'état de la protection de la vie privée au sein des pouvoirs publics.

72. Cet article autorise également le Commissaire chargé des données, dans son paragraphe 3, à recruter du personnel en vue d'assurer l'exercice des fonctions du Bureau. Enfin, cet article définit dans quels délais, après la promulgation de la loi, le Commissaire chargé des données devra être institué[29].

Article 49: Personnalité juridique distincte du Commissaire chargé des données

73. Dans tous les cas, l'Article 49 prévoit qu'il soit conféré au Commissaire une personnalité juridique distincte, de manière à ce qu'il puisse conclure des contrats, acquérir, détenir et céder tout type de bien nécessaire à l'exercice de ses fonctions, engager des poursuites ou être poursuivi en justice, prendre toute mesure et conclure toute opération relevant de l'exercice de ses fonctions ou favorisant leur exercice en vertu de la loi[30].

Article 50: Détermination du mandat du titulaire de la charge

74. Par ailleurs, autre mécanisme visant à assurer l'intégrité de la charge et à garantir intégrité et équité, l'Article 50 instaure une durée de mandat maximum pour la charge de Commissaire. Ce mandat est plus long que le cycle électoral, compte tenu des bonnes pratiques[31].

---

27 Principe politique 3.3: « Le responsable de l'organisme désigné sera nommé d'une manière garantissant l'indépendance et l'impartialité de ses fonctions. »

28 Principe politique 3.4: « Le responsable de l'organisme désigné bénéficiera de conditions d'emploi, notamment des dispositions en matière d'ancrage de sa position et de conditions de reconduction, qui seront prévues dans le mandat juridique/statutaire et suffiront à limiter les possibilités d'incitation ou de contrainte. »

29 Principe politique 3.12: « Le mandat juridique/statutaire précisera la période d'entrée en vigueur de l'organisme désigné lors de la promulgation de la loi. »

30 Principe politique 3.2: « L'organisme désigné pour garantir la conformité au mandat juridique/statutaire doit être une personne morale distincte ayant le droit de posséder ou de disposer d'actifs, la capacité de conclure des contrats et le pouvoir d'agir en toute indépendance dans l'exercice de ses fonctions. »

31 Principe politique 3.4, *sic*.

Article 51: Rémunération du Commissaire chargé des données et du personnel

75. Par ailleurs, afin de préserver l'indépendance et l'impartialité du Commissaire, l'Article 51 prévoit la rémunération du Commissaire et de son personnel, qui sera déterminée par des moyens indépendants, de manière à ce que le titulaire de la charge ne puisse donner l'apparence d'être redevable d'une administration. Le langage adopté ici est destiné à apporter aux juridictions la flexibilité requise pour déterminer le mécanisme approprié permettant d'atteindre cette indépendance. À titre d'exemple, certaines juridictions font établir le salaire de ces charges indépendantes par une commission indépendante; il peut également être fixé par la règlementation. La clause proposée n'entend pas dicter l'adéquation de l'un ou l'autre des mécanismes, mais a uniquement pour but de s'assurer que, une fois définie, l'allocation budgétaire se présentera de façon transparente dans le cycle budgétaire annuel du gouvernement sous un poste de dépenses distinct.

Article 52: Protection du Commissaire chargé des données

76. Afin de préserver l'indépendance et l'impartialité du Commissaire chargé des données, l'Article 52 prévoit en outre l'exonération de la responsabilité du Commissaire chargé des données concernant les actes commis ou omis de bonne foi dans l'exercice ou en vue de l'exercice de ses fonctions. Cette protection ne doit pas s'étendre aux cas de dommages corporels. Par ailleurs, il est prévu dans le cadre législatif d'indemniser le Commissaire chargé des données du coût de ses frais de défense[32].

Article 53: Délégation des pouvoirs du Commissaire chargé des données

77. Dans un souci de pragmatisme opérationnel et organisationnel, l'Article 53 autorise le Commissaire à déléguer tout ou partie des pouvoirs d'investigation et d'exécution qui lui ont été conférés par la loi à un fonctionnaire habilité qu'il aura désigné à cet effet[33].

Article 54: Indépendance du Commissaire chargé des données

78. L'Article 54 réitère le fait que le Commissaire est tenu d'agir en toute indépendance dans l'exercice de ses fonctions en vertu de la loi et qu'il ne doit pas être soumis à l'autorité ni au contrôle de quelque personne ou organisme que ce soit[34].

Article 55: Fonctions du Commissaire chargé des données

79. Comme indiqué dans l'Article 55, les fonctions principales de l'organisme de supervision, une charge administrative dirigée par son responsable, le Commissaire chargé des données, consistent à s'assurer du respect de la législation sur la protection de la vie privée par les moyens suivants:

- suivi de l'administration de la législation et réalisation de contrôles,
- organisation d'enquêtes sur le respect de la protection de la vie privée,
- résolution et médiation des plaintes relatives à la protection de la vie privée,

---

32 Principe politique 3.10: « Le mandat juridique/statutaire prévoit que l'organisme désigné pourra bénéficier d'une protection légale pour les actes effectués de bonne foi dans l'exercice de ses fonctions. »

33 Principe politique 3.6: « Le responsable de l'organisme désigné recevra dans le mandat juridique/statutaire le pouvoir de déléguer une certaine autorité à des agents habilités afin de faciliter l'exercice de ses fonctions. »

34 Principe politique 1.6: « Le mandat juridique/statutaire prévoit clairement l'indépendance de l'organisme désigné. »

- fourniture d'évaluations de l'impact des contrôles et de la supervision concernant la protection de la vie privée,
- réalisation de thèmes de recherche consacrés à la législation sur la protection de la vie privée,
- élaboration de programmes d'éducation publique,
- promotion des bonnes pratiques en matière de protection de la vie privée, et
- fourniture de conseils et de commentaires aux Contrôleurs des données.

Article 56: Serment de confidentialité

80. L'Article 56 exige que les personnes qui, en vertu de l'exercice des fonctions conféré par la loi, ont accès à des informations qui peuvent être considérées comme à caractère privé ou personnel, soient tenues de prêter le serment de ne pas divulguer les données obtenues à la suite de l'exercice d'un pouvoir ou de l'exécution d'une obligation prévue par la loi, sauf dans les conditions prévues par les dispositions particulières à cet effet dans la loi sur la protection de la vie privée, dans d'autres textes législatifs ou sur l'autorisation de l'ordonnance d'un tribunal.

Article 57: Pouvoirs d'ordre général du Commissaire chargé des données

81. L'Article 57 fait du Commissaire une entité apparentée aux organismes de réglementation afin de mener à bien l'exercice de ses fonctions, avec notamment le pouvoir nécessaire d'entreprendre toute action qui lui semblera requise, avantageuse ou utile et relative à l'exercice de ses fonctions, y compris le pouvoir d'enquêter sur les opérations d'un Contrôleur des données[35], de son propre chef ou suite à une plainte, d'obtenir des informations sur la documentation, le traitement et la sécurité des données et, entre autres, de demander à ce qu'une personne lui fournisse par écrit, dans les délais indiqués, l'accès à des données à caractère personnel ou à toutes autres informations spécifiées relatives aux pratiques de gestion de l'information du Contrôleur[36].

82. Les Articles 58 à 61 instaurent un mécanisme permettant au Commissaire chargé des données de demander des informations dans le cadre d'une enquête (la note d'information), et renforcent cette obligation en qualifiant d'infraction le fait de ne pas répondre ou de ne pas obtempérer à une note d'information du Commissaire[37].

Article 58: Pouvoir du Commissaire chargé des données en vue d'obtenir des informations du Contrôleur des données

83. L'Article 58 introduit un mécanisme d'interrogation ou de recueil de données préliminaire: la note d'information. Il décrit également dans quelles circonstances la note d'information doit être utilisée et la forme qu'elle peut prendre lorsqu'elle est présentée à la partie concernée. Conformément aux considérations générales sur l'utilisation des technologies en vue de faciliter la transmission en temps voulu, le paragraphe 2 prévoit les formats autorisés pour la remise des informations demandées.

---

35 Principe politique 3.5: « Le responsable de l'organisme désigné recevra dans le mandat juridique/statutaire les pouvoirs d'investigation nécessaires pour faciliter l'exercice des fonctions relevant du cadre de protection des données. »

36 Principe politique 3.7: « L'organisme désigné pourra entreprendre des audits ou des enquêtes sur les personnes auxquelles s'applique le cadre, que ce soit de son propre chef ou en réponse à des plaintes du public. La personne qui supportera les coûts de ces enquêtes sera déterminée par la réglementation. »

37 Principe politique 3.8: « Les personnes auxquelles la loi s'applique coopéreront avec l'organisme désigné dans l'exercice de ses fonctions, sous peine de sanctions civiles et/ou pénales. »

84. Les paragraphes 3 et 4 réaffirment les thèmes visés par une exception mentionnés précédemment dans le modèle de loi. Ils sont insérés pour éviter le moindre doute dans le traitement de ces questions.

Article 59: Contenu et format de la note d'information

85. L'article 59 précise le contenu nécessaire d'une note d'information qui a pour vocation d'informer la partie desservie de son droit d'entamer une procédure afin de se protéger, conformément au cadre fourni par le modèle de texte.

Article 60: Instauration de l'infraction de non-respect d'une note d'information

86. L'Article 60 indique que le fait de ne pas obtempérer à une note d'information doit être considéré comme une infraction importante à la loi et rend la partie qui la commet passible des sanctions et des peines prévues par la loi. Par ailleurs, le paragraphe 3 définit les moyens de défense raisonnables à cette déclaration sommaire de culpabilité.

Article 61: Recours du Commissaire chargé des données en cas d'insuffisance de la réponse à une note d'information

87. L'Article 61 détermine comment le Commissaire chargé des données est tenu de répondre dans le cas où il est estimé que la réponse à une note d'information est insuffisante, notamment en ordonnant la cessation des opérations ayant trait à la collecte, au traitement ou la divulgation d'informations à caractère personnel.

88. Les Articles 62 à 66 établissent la procédure nécessaire permettant au Commissaire chargé des données d'entreprendre un audit ou une enquête, notamment la réception d'une plainte individuelle, la notification subséquente du Contrôleur des données concernant l'enquête en cours et les dispositions relatives aux pouvoirs d'entrée, de recherche et de saisie (sous réserve de l'émission d'un mandat et de la présence d'un agent de police)[38].

Article 62: Réaction du Commissaire chargé des données à réception d'une plainte

89. L'Article 62 a trait à l'obligation du Commissaire chargé des données d'agir de façon particulière à réception d'une plainte. Ces mesures obligatoires comprennent le fait de mener enquête et d'aviser le plaignant du résultat de ladite enquête dans un délai raisonnable. Le paragraphe 3 réitère les dispositions antérieures relatives aux personnes agissant pour le compte de la personne à l'origine du processus.

Article 63: Format et contenu d'une plainte

90. L'Article 63 décrit le format général que doit observer une plainte déposée par un plaignant et oblige le Commissaire chargé des données à apporter toute l'aide possible pour s'assurer de la recevabilité du format de la plainte. Le Commissaire chargé des données ne doit pas intervenir sur le fond de la plainte.

[38] Principe politique 3.9: « L'organisme désigné pourra demander certains documents destinés à faciliter ses investigations, demande à laquelle devront obtempérer les personnes concernées. L'organisme pourra bénéficier d'un mandat du tribunal à cette fin si cela se justifie. »

Article 64: Lancement d'une enquête par le Commissaire chargé des données à la suite d'une plainte

91. L'Article 64 décrit la procédure à suivre par le Commissaire chargé des données pour solliciter le Contrôleur des données objet d'une plainte. Le mécanisme proposé (l'avis d'enquête) doit être remis au responsable du Contrôleur des données avant le commencement de l'enquête.

Article 65: Pouvoir d'ordre général d'effectuer des recherches et des saisies d'effets au cours d'une enquête

92. L'Article 65 autorise de façon générale le Commissaire chargé des données à entrer dans les locaux d'un Contrôleur des données, à entreprendre des recherches et, le cas échéant, à saisir toute documentation pertinente dans le cadre d'une enquête. Le paragraphe 2 de cet article limite l'application de cette autorisation d'ordre général, dans la mesure où un mandat à cet effet doit être obtenu au préalable et où les agents du Commissaire chargé des données doivent être accompagnés d'un agent de police.

Article 66: Exceptions à la saisie

93. L'Article 66 rappelle que les dispositions antérieures de la présente loi relatives à certains documents visés par une exception au traitement sont également applicables dans le cas d'une recherche et d'une saisie.

94. Une fois l'enquête terminée, il peut arriver que le Commissaire chargé des données estime que le Contrôleur des données ne respecte pas, dans ses opérations, ses obligations en matière de protection de la vie privée. Dans ce cas, les Articles 67 à 69 établissent le mécanisme et la procédure permettant au Commissaire chargé des données d'émettre des recommandations à l'intention des Contrôleurs des données opérant de façon non conforme à la loi.

Article 67: L'avis d'exécution

95. L'Article 67 autorise le Commissaire chargé des données à remettre le mécanisme proposé (l'avis d'exécution) au Contrôleur des données, délimite l'application appropriée de ce mécanisme et, afin d'éviter le moindre doute, en limite l'objet.

Article 68: Contenu et format de la note d'exécution

96. L'Article 68 définit le format particulier de l'avis d'exécution et inscrit dans ce mécanisme l'autorité contraignante nécessaire pour ordonner aux Contrôleurs des données en infraction d'intervenir pour rectifier l'infraction déterminée. Cet article prévoit également le mécanisme, ainsi que la forme du mécanisme, par lequel le Contrôleur des données doit répondre à l'avis d'exécution et précise le délai maximal dans lequel cette réponse est attendue. De cette manière, les Contrôleurs des données sont obligés de répondre ou d'obtempérer aux instructions de l'avis d'exécution.

Article 69: Instauration de l'infraction de non-respect d'un avis d'exécution

97. L'Article 69 détermine que le fait de ne pas obtempérer à un avis d'exécution tel que décrit dans l'Article 68 est considéré comme une infraction importante à la loi et expose le Contrôleur des données à des sanctions pénales[39].

[39] Principe politique 3.8, *sic*.

Article 70: Conditions de l'enquête

98. L'Article 70 établit les conditions logistiques complémentaires dans lesquelles l'enquête doit être menée. Le paragraphe 1 précise que toute enquête doit être réalisée en insistant sur son caractère confidentiel.

99. Le paragraphe 2 autorise les parties à présenter des observations au Commissaire chargé des données dans le cadre de l'enquête. Néanmoins, on notera qu'à ce stade de l'enquête la disposition prévoit que les parties ne peuvent pas assister à la présentation des observations de l'autre partie.

Article 71: Renvoi de l'affaire devant le Directeur général de la police

100. L'Article 71 définit l'action que doit engager le Commissaire chargé des données afin de renvoyer le dossier à la personne compétente lorsqu'il estime qu'une infraction a été commise.

Article 72: Rapport annuel du Commissaire chargé des données au Parlement

101. L'Article 72 fait obligation au Commissaire chargé des données de présenter un rapport de ses activités au Parlement, conformément aux bonnes pratiques parlementaires[40].

TITRE VIII: INSTITUTION DES INFRACTIONS ET DES PEINES POUR VIOLATION DES DISPOSITIONS DE LA LOI

102. Le **Titre VIII du modèle de loi** décrit les infractions pénales associées à la violation de dispositions particulières de la loi.

Article 73: Collecte d'informations à caractère personnel sans en avoir avisé la personne concernée

103. L'Article 73 établit que toute atteinte à l'Article 8 constitue une infraction. Lorsque les juridictions décident de distinguer les informations à caractère personnel sensibles et les informations à caractère personnel non sensibles, il est possible de prévoir des sanctions différentes pour cette infraction selon que l'infraction présumée concerne des informations à caractère personnel ou des informations à caractère personnel sensibles. Dans ce cas, il est préférable que la peine associée à la violation de ces dernières soit plus répressive.

104. Bien que les obligations définies par les Articles 8 à 15 et 20 soient toutes essentielles à l'application effective de la protection des données, les infractions à celles-ci peuvent faire l'objet de mesures correctives adéquates, sans qu'il soit nécessaire d'imposer des sanctions pénales. Cependant, il est suggéré que les atteintes à l'Article 19, compte tenu de leurs implications sur les accords de commerces internationaux, soient traitées avec plus de sévérité que les autres.

[40] Principe politique 3.11: « L'organisme désigné présentera chaque année au Parlement/Conseil législatif un compte rendu de ses activités au cours de l'année précédente. »

Article 74: Transfert extra-juridictionnel d'informations à caractère personnel sans autorisation en bonne et due forme

105. Ainsi, l'Article 74 établit que toute atteinte à cette disposition particulière de l'Article 19 est une infraction pénale et définit la peine standard associée à celle-ci[41].

Article 75: Entrave à un agent du Commissaire chargé des données

106. L'Article 75 a trait aux entraves directes ou indirectes aux agents habilités du Commissaire chargé des données dans l'exercice de leurs fonctions lors d'une enquête; il définit la peine standard associée à cette infraction.

Article 76: Présentation de faux arguments au Commissaire chargé des données ou à ses agents

107. L'Article 76 évoque les personnes dont on estime qu'elles ont abusé des droits conférés par le Titre III de la loi. Les infractions créées et les peines définies doivent dissuader d'une utilisation vexatoire abusive de ces dispositions qui nuirait à la viabilité opérationnelle du Contrôleur des données et du Bureau du Commissaire chargé des données.

Article 77: Violation du serment de confidentialité

108. L'Article 77 a pour but de traiter des personnes violant les serments de confidentialité prononcés lors de la prise de leurs fonctions au Bureau du Commissaire chargé des données. Il est destiné à limiter de tels événements et à préserver la continuité de la confiance publique dans le Bureau.

109. Les violations des dispositions de la loi qui ne sont pas explicitement traitées dans le présent Titre ou dans d'autres articles en vigueur pourront être résolues par les tribunaux civils.

TITRE IX: DISPOSITIONS GÉNÉRALES DESTINÉES À FACILITER L'APPLICATION DU CADRE LÉGISLATIF

110. Le **Titre IX du modèle de loi** prévoit diverses considérations qui favoriseront l'application des principaux aspects de la loi présentés dans les articles précédents.

Article 78: Protection des dénonciateurs

111. L'Article 78 prévoit la protection des personnes qui, alors qu'elles sont employées par un Contrôleur des données, prennent connaissance d'actes de celui-ci contraires à l'objet de la présente loi à de ses dispositions et qui avisent volontairement l'autorité compétente de ces actes. Cette disposition de « protection des dénonciateurs » est destinée à inciter les employés à agir dans l'intérêt du bien public en limitant les mesures de représailles de la part du responsable du Contrôleur des données. Cette disposition a pour effet d'élargir les moyens de signalement aux autorités des atteintes à la protection de la vie privée afin d'y remédier et/ou de faire appliquer la loi au plus vite.

[41] Principe politique 5.10 [6.6]: « Le mandat juridique/statutaire prévoit des sanctions civiles et pénales en cas de violation des dispositions définies relatives à l'utilisation ou au traitement [à la divulgation] des informations à caractère personnel. Ces sanctions pourront s'appliquer à la partie chargée du traitement, ou à tout agent ou administrateur dont il peut être prouvé qu'ils ont enfreint le mandat juridique/statutaire. »

Article 79: Redevance perçue pour les services du Commissaire chargé des données

112. L'Article 79 autorise le Ministre, agissant sur le conseil du Commissaire chargé des données, à établir une grille de redevances pour les services rendus par son Bureau. Cela a pour but de faciliter le recouvrement d'une partie des coûts liés au fonctionnement du Bureau.

Article 80: Ministre chargé de la règlementation nécessaire

113. L'Article 80 prévoit une disposition d'ordre général permettant au Ministre compétent de réglementer en tant que de besoin la prise d'effet ou le développement de dispositions particulières de la loi.

Article 81: Rôle des tribunaux

114. L'Article 81 clarifie le rôle des tribunaux en tant qu'instance de dernier ressort lorsque l'une des parties demeure insatisfaite du résultat d'une procédure de résolution de litige menée par le Commissaire chargé des données. Cet article réaffirme également le pouvoir des tribunaux d'imposer des peines civiles en cas de violations de la loi qui ne sont pas considérées comme des infractions en vertu du Titre VIII[42, 43, 44].

[42] Principe politique 4.8, *sic*.
[43] Principe politique 5.10, *sic*.
[44] Principe politique 6.6, *sic*.

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

Participants et observateurs officiellement désignés

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

Annexe 1

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

Participants des organisations régionales/internationales

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

Consultants pour le projet HIPCAR participant à l'Atelier

Nom	Prénom
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[45]	J Paul
PRESCOD	Kwesi

[45] 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 Frigate Bay, Saint-Kitts-Et-Nevis, du 19 au 22 juillet 2010

Participants et observateurs officiellement désignés

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

Annexe 2

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

Participants des organisations régionales/internationales

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

Annexe 2

Consultants pour le projet HIPCAR participant à l'Atelier

Nom	Prénom
GERCKE	Marco
MORGAN[46]	J Paul
PRESCOD	Kwesi

[46] Président de l'Atelier.

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

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

Genève, 2013