

juin 2010

Proposition de cadre légal pour l'utilisation et la gestion de l'information électronique en Haïti

« UNE HAÏTI
MODERNE,
COMPETITIVE,
CHAMPIONNE
TIC DE LA
CARAÏBE D'ICI
2020 »



**GROUPE DE TRAVAIL SUR LES
TECHNOLOGIES DE L'
INFORMATION ET DE LA
COMMUNICATION**

(GTIC) [HTTP://COMMISSIONTIC.HT](http://COMMISSIONTIC.HT)

Table des matières

Remerciements

I.- Note de Synthèse

II.- Mise en contexte

III.- La révolution numérique du droit haïtien, un impératif, par Dr. Bernard H. Gousse
L'admissibilité de la force probante du document numérique
La fourniture de biens et de services par les moyens électroniques
L'administration électronique
La lutte contre la cybercriminalité
La propriété intellectuelle dans l'environnement numérique
Conclusion

Annexes

Annexe 1: Avant projet de loi sur la signature électronique

Chapitre 1 : De la preuve et de la signature électronique
Chapitre 2 : Des prestataires de service de certification électronique
Chapitre 3 : Du Conseil National des Télécommunications

Annexe 2 : Projet d'arrêté sur la signature électronique

Chapitre 1 : Définitions
Chapitre 2 : Des dispositifs sécurisés de création de signature électronique
Chapitre 3 : Des dispositifs de vérification de signature électronique
Chapitre 4 : Des certificats électroniques qualifiés
Chapitre 5 : Des prestataires de service de certificat électronique
Chapitre 6 : Des notifications

Annexe 3 : Avant projet de loi sur les échanges électroniques

- Titre 1 : Les échanges électroniques en général

Chapitre 1 : Dispositions générales
Chapitre 2 : Application des exigences légales aux messages de données
Chapitre 3 : Communication des messages de données

- Titre 2 : Le commerce électronique dans certains domaines d'activités

Chapitre unique : Le transport des marchandises

Annexe 4 : Avant projet de loi sur l'administration électronique

Titre préliminaire : Du champ d'application et des principes généraux

Titre 1 : Du droit des administrés à utiliser les moyens électroniques dans leur rapport avec l'administration publique

Titre 2 : Du régime juridique de l'administration électronique

Chapitre 1 : Du site électronique

Chapitre 2 : De l'identification et de l'authentification

Chapitre 3 : Des registres, communications et notifications électroniques

Chapitre 4 : Des documents et archives électroniques

Titre 3 : De la gestion électronique des procédures

Chapitre 1 : Dispositions communes

Chapitre 2 : L'utilisation des moyens électronique dans le déroulement des procédures

Titre 4 : Coopération entre entités administratives pour la mise en œuvre de l'administration électronique

Chapitre 1 : Champ institutionnel de coopération en matière d'administration électronique

Chapitre 2 : Coopération en matière d'interopérabilité des systèmes et applications

Chapitre 3 : Réutilisation d'applications et transfert de technologies

Titre 5 : Dispositions finales

Annexe 5 : Termes de référence

Annexe 6 : Rapport d'atelier sur la signature et les échanges électroniques

Annexe 7 : Rapport de mission eGA

Annexe 8 : Rapport de mission RedGEALC

Annexe 9 : Mission BID

Annexe 10 : Membres du GTIC

Remerciements

A Son Excellence, Monsieur le Président de la République, pour avoir mis en place le groupe de travail sur les technologies en janvier 2009 ; aux Premiers Ministres Madame Michèle Pierre-Louis et Monsieur Jean-Max Bellerive, et à leurs Collaborateurs, qui ont été toujours à l'écoute du GTIC ; aux institutions internationales et nationales, le Secrétariat Général de la Présidence, l'Office de Management des Ressources Humaines (OMRH), pour le support fourni dans le cadre de son projet « Gouvernance territoriale et Réforme administrative », la Fondation Réseau de Développement Durable d'Haïti (FRDDH), la Chambre Franco-Haïtienne de Commerce et d'Industrie (CFHI), la Banque Interaméricaine de Développement (BID), en particulier son ancien Représentant, M Philippe Dewez, disparu le 12 janvier 2010, et la Fondation Connaissance et Liberté (FOKAL), qui ont permis la réalisation des travaux ; aux membres du sous-groupe de réflexion sur le Cadre Légal (Henri Cassion, Schiller Jean-Baptiste); aux membres du Comité Exécutif (Tayana Etienne, Stéphane Bruno, Jaunasse Elysée, Raymond Noël), et à notre Directrice Exécutive (Marlène Sam) qui n'ont ménagé ni leurs temps ni leur énergie, y compris dans les moments les plus difficiles d'après séisme.

I. Note de Synthèse :

Contexte :

Les technologies de l'information et de la communication (TIC) ont révolutionné les rapports et intensifié les échanges entre particuliers et institutions en intégrant les télécommunications, l'informatique et l'audiovisuel (bureautique, téléphonie mobile, bases de données numérisées,...). Les TIC sont des outils qui changent radicalement les modalités selon lesquelles s'effectuent le commerce, la compétitivité, la communication, l'apprentissage, mais aussi toutes les autres formes de rapports humains, culturels, sociaux... Elles ont une forte propension à abolir la distance et le temps. De plus, elles offrent des moyens plus efficaces et rationnels de gouverner en transformant les rapports que le Citoyen entretient avec l'État, et vice-versa.

Les secteurs scientifiques et technologiques sont, à travers le monde, et en particulier dans les pays émergents, les principaux vecteurs de création de richesse et de développement économique. En Haïti, la création d'emplois et la mise en place durable d'un véritable projet e-gouvernance sont ralenties par l'absence d'un cadre légal.

Approche :

Le GTIC, créé en janvier 2009, a mis sur pied un sous-comité dont le mandat était d'analyser le cadre légal en vigueur et de formuler des propositions pour le modifier ou le renforcer aux fins d'accroître le **développement**, l'**utilisation** et l'**exploitation** des TIC. En Octobre 2009, le Comité Exécutif, s'étant prononcé sur la proposition de loi-cadre modifiant le secteur des Télécommunications d'initiative gouvernementale, et muni d'un copieux cahier des charges a été en mesure, grâce à sa

collaboration avec l'OMRH et un financement du PNUD, de commanditer une consultation dont certains des résultats, aujourd'hui compilés dans un rapport, ont déjà fait l'objet d'un atelier, mi-décembre. Ont suivi plusieurs rencontres et mises à jour, notamment au lendemain du séisme du 12 janvier 2010.

Les propositions du GTIC sont concrètes, pragmatiques et fondées sur le Corpus juridique et sur la jurisprudence. Elles se sont inspirées d'expériences, des tendances contemporaines, des pratiques et engagements locaux et internationaux. Elles sont dûment argumentées et visent à doter l'Exécutif d'outils idoines pour démarrer le processus d'adaptation des dispositions légales de la République d'Haïti pour prendre en compte les progrès technologiques récents et actuels – tout en ne figeant pas la loi – en raison de la rapide évolution qui caractérise le secteur TIC, en Haïti, d'abord, et à l'échelle planétaire, ensuite.

Objectifs :

L'objectif poursuivi dans l'élaboration de ce cadre legal est double : d'une part, faciliter les rapports entre l'Etat et les administrés (entreprises, institutions et citoyens), et de l'autre, donner une impulsion volontariste à l'essor de l'exploitation et de l'utilisation des TIC en Haïti au profit du bien-être :

- économique (création de PME/PMI innovantes, facilitation des transactions en temps réel, externalisation des processus d'affaires),
- politique (accroissement quantitatif et qualitatif de l'offre de services publics, participation citoyenne, gestion systémique, transparente et décentralisée),
- culturel (revalorisation du patrimoine historique, artistique, musical, linguistique,...) et
- social (rapprochement ville/campagne, diaspora/Alma Mater) de toutes les haïtiennes et haïtiens.

Ces propositions d'aménagements de textes de loi s'inscrivent résolument dans le contexte plus général d'une politique de décentralisation et d'une gouvernance locale rendue plus dynamique grâce aux TIC.

Les Propositions contenues dans les textes soumis à l'Exécutif:

Il s'agit d'un ensemble d'avant-projets de loi, d'arrêtés, de modifications et de recommandations d'études plus approfondies portant sur :

- la signature électronique *¹
- la preuve électronique *
- l'accès à l'information publique et à l'administration en ligne *
- les échanges électroniques *

¹ * TEXTE OU SUJET TRAITE DANS LE CADRE DU RAPPORT SOUMIS EN ANNEXE

- la protection des données personnelles et institutionnelles *
- la propriété intellectuelle
- le cadre institutionnel TIC
- la cybercriminalité

II - Mise en contexte :

Partons de l'état des lieux décrit dans le document d'orientation du GTIC, à savoir :

« Le secteur des Télécommunications est encore régi par des textes juridiques datant de la fin des années 70 et du début des années 80, dont les objectifs sont contraires aux normes actuelles d'ouverture à la compétition et de développement de l'initiative privée. Il en résulte de nombreuses anomalies dans la gestion du secteur et l'obligation pour les entreprises d'évoluer sur la base de consensus et de la bonne foi des instances de régulation. Cet environnement fragilise les initiatives et les entreprises créées. De même que, souvent, les dispositions légales ne sont pas mises en œuvre, comme, par exemple, sur le plan de la régulation, le Conseil d'administration du CONATEL, qui n'a jamais vu le jour.

Les principaux textes légaux sont :

- *La convention de concession du 20 août 1969 conclue pour une durée de 99 ans et concédant à la TELECO le monopole des systèmes de communications téléphonique et télégraphiques tant sur le plan national que sur le plan international.*
- *Le décret du 12 octobre 1977 qui accorde à l'Etat haïtien le monopole des services de télécommunications et l'autorise à décerner des licences ou des permis d'exploitation à des personnes privées (physiques ou morales).*
- *Le décret du 26 juin 1987 qui fixe le mode de taxation des différents services de radiocommunications.*
- *Le décret du 27 septembre 1987 applicable à l'organisation et à la mission du CONATEL.*

Sur le plan réglementaire, il existe un ensemble de dispositions discrétionnaires qui entravent le développement du secteur.

Un avant-projet de loi tendant à réglementer l'ensemble du secteur des Télécommunications a donné lieu à divers débats et prises de position, par la plupart des secteurs concernés. Ce texte n'a pas encore été présenté au parlement. Il existe aussi un avant-projet de loi sur la signature électronique en attente d'être introduit aux législateurs. »

De plus, l'exploitation des TICs en Haïti doit satisfaire un ensemble de **finalités que le GTIC a définies comme suit dans son document d'orientation (finalisé en novembre 2009) :**

- Le renforcement de la **Compétitivité** de l'économie haïtienne ;
- L'amélioration de la **Gouvernance** de l'Etat et des entreprises ;
- La création d'**Emplois**;
- L'amélioration de la **Cohésion Sociale**.

C'est ainsi que le premier **objectif général** visé consiste en « **la mise en place d'un dispositif de gestion proactive et transparente du secteur TIC** ».

Les **objectifs spécifiques** suivants ont ainsi été identifiés (extrait du document d'orientation)

« La mise en place d'un cadre légal et institutionnel adapté aux changements en profondeur qu'induisent les nouvelles technologies de l'information et de la communication, est un besoin fondamental aux fins d'assurer l'utilisation et l'exploitation efficace des TIC et les mettre au service du bien commun. Ce cadre devra assurer la prise en compte des évolutions technologiques déjà enregistrées et celles à venir tout en favorisant l'essor d'une industrie des TIC en Haïti, en intégrant les acteurs, pour répondre aux besoins, attentes, défis et opportunités liés aux contextes culturels, économiques, politiques et sociaux qui leur sont spécifiques.

- *Objectif spécifique 1.1 :Créer un cadre légal favorable à l'éclosion du secteur, à l'investissement et au développement d'applications*
- *Objectif spécifique 1.2 :Créer un cadre institutionnel favorable à l'éclosion du secteur, à l'investissement et au développement d'applications*
- *Objectif spécifique 1.3 :Instituer un fonds de développement du secteur TIC*
- *Objectif spécifique 1.4 : Faciliter le développement de partenariats multi-acteurs »*

En raison de l'approche systémique employée par le GTIC, rendue d'autant plus pertinente par le séisme du 12 janvier 2010, séisme qui a mis à nu et accru la complexité et l'interdépendance des problématiques, il a paru urgent et important de présenter une proposition de cadre légal pour l'utilisation et la gestion de l'information électronique en Haïti. Cette proposition s'inscrit dans le cadre de la stratégie de réflexion-action prônée par le GTIC qui souhaitait lancer trois chantiers: cadre légal, e-gouvernance et environnements technologiques.

Un tel cadre légal est d'autant plus indispensable qu'il vise à accompagner la modernisation de l'administration publique et la dynamisation du marché des technologies.

III - La révolution numérique du droit haïtien, un impératif :

Dr. Bernard H. GOUSSE,
Professeur à l'Université Quisqueya, Avocat.

Présentation des projets de lois et des règlements d'application, accompagnés de leur argumentaire, devant permettre au droit haïtien de se moderniser pour l'admission des documents électroniques dans les rapports privés et dans l'administration publique.

L'essor de l'internet et les échanges qu'il permet pose un défi au droit. Il s'engage une course de vitesse dont le droit, pris dans son acception d'ensemble de normes applicables à une activité sociale, se retrouve perdant. La phrase de Me. Robert Stein, Directeur Exécutif de l'American Bar Association des Etats-Unis, illustre éloquemment cette réalité : « *Ceci est la nouvelle frontière, il y a une certaine qualité de type Ouest Sauvage à propos de l'Internet. Les lois sont assez incertaines et personne ne sait avec certitude qui est le shérif, le marshall ou le maire de la ville... Il n'existe pas de meilleur lieu que cette nouvelle frontière pour que des juristes créatifs et visionnaires consacrent leur attention* ». ²

Les domaines juridiques touchés par l'internet sont multiples. Nous citerons dans le désordre la propriété intellectuelle, le droit de la preuve, le droit pénal, la protection de la vie privée, le droit du travail, la protection de l'enfance et des bonnes mœurs, le droit fiscal, etc. On voit donc qu'il est impossible d'aborder de manière simpliste le droit de l'internet.

Néanmoins ce secteur bouillonne d'activités. Les échanges se nouent sur le net, des engagements sont pris. Des paiements sont effectués. Des œuvres intellectuelles ou artistiques sont dématérialisées. Tout ceci nécessite encadrement et protection.

Le droit, sommé par les internautes, ne reste pas indifférent au développement des technologies et sans remettre en cause les notions traditionnelles, s'adapte peu à peu aux particularités de cette nouvelle réalité virtuelle. Peu à peu, à coups de lois, de décisions judiciaires, d'ouvrages doctrinaux, se forge peu à peu un droit de l'internet qui englobe les domaines connus du droit énumérés plus haut....sans nous.

Haïti ne peut assister impuissante à ce bouillonnement sans y prendre part ; ce serait irresponsable vis-à-vis de la population et des générations futures. De là est née l'idée d'inclure dans le mandat du Groupe du Travail sur les Technologies de l'Information la responsabilité de penser la modernisation de notre cadre légal pour l'adapter à ce nouvel environnement qui est le quotidien d'un nombre croissant de nos concitoyens. Il fallait éviter que, par manque de structures d'accueil juridique, la toile mondiale ne tisse ses mailles sans nous et que nous ne ratons définitivement le mouvement de la modernisation.

En effet les défis posés sont les suivants³. Si, juridiquement, on ne peut, en cas de litige, assurer l'authentification des transactions électroniques ou la sécurité des paiements, les réseaux ne seront pas le lieu majeur de la réalisation de ces opérations. La sécurité de certaines transactions

² PRÉFACE IN JACOBSEN PAUL, *NET LAW : HOW LAWYERS USE THE INTERNET*, ED. O'REILLY, CALIFORNIA, U.S.A, 1997

³ BERNARD H. GOUSSE, LE NOUVEAU DROIT DES TELECOMMUNICATIONS. DEFIS ET PERSPECTIVES. IN AIHC, *CONFERENCE HAÏTI TELECOM 1996. L'AVENIR DU SECTEUR DES TELECOMMUNICATIONS EN HAÏTI. QUESTIONS JURIDIQUES ET REGLEMENTAIRES*, QUEBEC, 1997

particulièrement dans le milieu bancaire réclame que certaines communications soient cryptographiées ; alors que les pouvoirs publics ont légitimement besoin d'y avoir accès pour lutter contre la cybercriminalité, le blanchiment des avoirs et le financement du terrorisme. Un équilibre devra être trouvé entre d'une part la liberté de communication et de l'autre le respect de l'ordre public. Le fichage et l'archivage de données personnelles donne une nouvelle actualité au principe du respect de la vie privée. Le développement et la vulgarisation des nouvelles technologies représentent une opportunité à saisir pour rapprocher l'administration publique de la population et améliorer la gouvernance. Ces défis juridiques se doublent donc d'enjeux politiques et culturels d'intégration nationale et de protection des langues et de la culture nationales.

Le GTIC présente ici un ensemble de textes législatifs et réglementaires qui constituent les premières salves de la révolution numérique du droit haïtien qui ne doit pas s'arrêter avec eux. D'autres textes devront les enrichir ; la pratique leur donner vie. Ils permettent d'une part de sécuriser les rapports privés en réglementant la prise en compte par le droit des documents, des contrats et de la signature électroniques (Première Partie). D'autre part, ils sont les outils par lesquels la fourniture de services par l'administration renforcera la démocratie et amoindrira la distance entre l'administration publique et l'administré, son patron ; tout en garantissant que la collecte et la conservation de renseignements personnels ne servent d'outil à une oppression insidieuse (Deuxième Partie). On devra enfin envisager les moyens d'assurer la sécurité de l'environnement électronique (Troisième Partie).

PREMIERE PARTIE
LE DOCUMENT NUMERIQUE
DANS LES RAPPORTS DE DROIT PRIVÉ

CHAPITRE I

L'ADMISSIBILITÉ DE LA FORCE PROBANTE DU DOCUMENT NUMÉRIQUE

Les nouvelles technologies de l'information et de la communication ont entraîné une véritable mutation des modes de commercialisation. Grâce à l'Internet, le marché des opérateurs économiques s'est étendu à l'échelle du globe. Il suffit de constater le succès rencontré par les nouveaux marchands électroniques tels Amazon.com. L'Internet permet non seulement les ventes à distance, mais encore l'échange de données informatisées entre entreprises, les transactions bancaires à distance ou la signature de contrats.

Il s'ensuit une dématérialisation des échanges contractuels, manifestée par la substitution des messages électroniques au support papier. L'environnement juridique traditionnel ne connaissait jusqu'alors que ce dernier support, puisqu'il était ainsi possible de prouver le contenu du contrat et d'authentifier son signataire. Mais là où la loi requiert un écrit pour prouver une obligation, le message électronique satisfait-il à cette exigence? La signature manuscrite remplit la fonction d'identification des contractants, et marque leur adhésion au contenu du contrat. A l'ère du contrat virtuel, il faudra s'habituer à la notion de signature électronique. Quelle en est la validité juridique ?

Une réponse satisfaisante à ces interrogations est nécessaire si on veut sécuriser les transactions électroniques. Les partenaires impliqués doivent pouvoir s'assurer que le texte auquel ils ont donné leur adhésion ne peut plus être altéré, et que les messages qu'ils reçoivent proviennent effectivement de leur auteur présumé.

Pour transposer les concepts d' « écrit », d' « original » et de « signature » au monde des télécommunications la réponse ne peut être que légale. ***Prisonnier de l'écrit et de la signature manuscrite, le droit haïtien de la preuve ne permet pas à l'heure actuelle la prise en compte du document et de la signature électroniques*** (section I). Il faut quand même constater que de par le monde, des initiatives nationales et internationales, surtout parmi nos concurrents économiques apportent des réponses à leur admissibilité et permettent ainsi de sécuriser les transactions électroniques. Il est donc impératif que notre droit se mette au niveau et s'adapte. La présentation du projet de loi sur la signature électronique et modifiant le droit de la preuve, ainsi que le projet d'arrêté d'application sont les premiers éléments de la modernisation de la législation haïtienne (Section II).

Section I - Les Obstacles Mis par le Droit de la Preuve en Haïti à la Prise en Compte du Document et de la Signature Electroniques

Le droit de la preuve s'articule autour de deux systèmes⁴. Dans le système de la preuve légale, le législateur établit une hiérarchie entre les modes de preuve et limite l'admissibilité de certains procédés. A l'opposé, le système de la liberté de la preuve, dit encore système de la preuve morale, abandonne aux parties le choix des modes de preuve sans aucune hiérarchisation entre eux. Les deux systèmes coexistent en Haïti et pour schématiser, nous dirons que le *système de la preuve légale s'applique aux actes juridiques, et que celui de la liberté de la preuve s'applique en droit pénal, aux engagements commerciaux [réserve faite des actes mixtes], aux faits juridiques et aux actes juridiques civils d'une valeur inférieure à seize gourdes.*

Il convient tout de même de remarquer à ce stade que les règles sur la preuve ne sont pas d'ordre public, et qu'il s'ensuit que des parties peuvent à l'avance et valablement convenir de l'admissibilité de tel ou tel mode de preuve, exception faite des matières qui relèvent de l'ordre public (état des personnes, force probante des actes authentiques). Néanmoins, dans le cadre d'un réseau ouvert comme l'Internet où les parties se rencontrent et contractent sans convention préalable, pour l'essentiel, des transactions, les règles légales s'appliqueront.

Or, les modes de preuve sont réglementés par la loi. Il s'ensuit que les procédés nouveaux comme *la dactylographie, la photocopie ou les supports magnétiques, ou un document électronique, ne peuvent être utilisés que dans la mesure où la loi les consacre, et où ils s'insèrent dans les catégories de preuves reconnues* (commencement de preuve par écrit ou présomptions).

Les transactions électroniques rentrent dans la catégorie des actes juridiques conclus entre des personnes dont au moins l'une n'est souvent pas commerçante, et entre lesquelles une convention préalable sur la preuve n'a pu être établie. La force probante de ce document électronique souffre de la primauté faite à l'écrit dans le régime de la preuve (#1), et de la difficulté de trouver à ce document une place à l'intérieur de ce régime (#2).

1 - La primauté de l'écrit dans le régime de la preuve

Dans notre code civil, la preuve des actes juridiques n'est pas libre. *«Il doit être passé acte devant notaire ou sous signature privée, de toutes choses excédant la somme ou valeur de seize gourdes»⁵. Dès lors qu'il s'agit de prouver une obligation résultant d'un acte juridique, la production de l'écrit est indispensable, à l'exclusion de tout autre mode de preuve.* La nécessité d'un écrit n'est qu'une règle de preuve qui n'atteint pas la validité de l'obligation. La preuve testimoniale ne sera pas admise là où il faudrait un écrit et toujours selon le même article 1126, il est interdit de prouver par témoins contre et outre le contenu de l'écrit.

Cette primauté de l'écrit se justifie parce qu'il présente les avantages suivants: premièrement, il représente une preuve préconstituée, deuxièmement il contient une valeur probante objective non attachée à la déposition éventuellement subjective des témoins et enfin, sa valeur probatoire ne diminue pas avec le temps. Ce sont ces avantages qui amènent les parties à se préconstituer une

⁴ WEILL ALEX, TERRE FRANÇOIS, *DROIT CIVIL. INTRODUCTION GÉNÉRALE*, 4E. ÉD., 1979, PRÉCIS DALLOZ, NO. 438 s.

⁵ ART. 1126 C.CIV

preuve de leurs engagements grâce à l'écrit, même lorsque la loi ne l'exige pas, notamment dans les rapports entre commerçants.

Pour acquérir cette force probante l'écrit doit satisfaire à certaines formalités. Pour les besoins de la démonstration nous nous limiterons aux formalités requises pour l'acte sous seing-privé, quoique la possibilité d'établir des actes authentiques de manière électronique devienne de plus en plus proche.

L'écrit sous seing privé doit porter la signature manuscrite de l'auteur de l'acte ou de ses représentants. La signature manuscrite ne peut être portée sur un document électronique convenu entre des personnes se trouvant à des milliers de kilomètres de distance.

L'acte relatant des conventions synallagmatiques est soumis à la formalité du double ou de l'original multiple, et chaque original doit contenir la mention du nombre d'originaux qui ont été faits⁶. L'inobservance de cette formalité n'entraîne pas la nullité de la convention, mais la nullité de l'instrument probatoire. L'acte non rédigé en double ne pourra servir que comme commencement de preuve par écrit. La règle du double ne s'applique pas aux actes commerciaux, cependant s'il s'agit de prouver ses engagements contre un non commerçant, la partie commerçante devra prouver son droit conformément aux dispositions de l'article 1110 c.civ. Le document électronique, le contrat électronique par sa nature même ne peut satisfaire à l'exigence du double. L'original étant l'assemblage de données numériques qui se trouvent enregistrées sur le disque dur d'un ordinateur; il n'a pas de double et ne peut être signé ; ce qui sort de l'imprimante n'est qu'une copie.

En troisième lieu, les actes constatant des promesses unilatérales de sommes d'argent ou de choses appréciables en argent, s'ils ne sont pas rédigés en entier de la main du débiteur, doivent comporter, outre la signature manuscrite, la mention manuscrite *bon* ou *approuvé* portant en toutes lettres la somme ou la quantité de la chose⁷. Sinon le document ne pourra servir comme preuve écrite, il pourra tout au plus être utilisé comme commencement de preuve par écrit, l'obligation devant si possible être prouvée par d'autres moyens. Or nous savons qu'au delà de seize gourdes, la preuve de l'obligation ne peut se faire que par écrit. Il est matériellement impossible avec le document électronique de satisfaire à cette exigence du bon manuscrit comportant le montant de la somme écrite de la main du débiteur. Face à cette primauté de l'écrit, il convient d'apprécier la prise en compte du document électronique par le droit civil.

2 - La difficile prise en compte du document électronique dans le régime de la preuve

Lorsqu'on considère la primauté de l'écrit dans le régime de la preuve des actes juridiques, nous ne pouvons faire que ces deux constatations : le document électronique ne peut être assimilé à un écrit, il peut difficilement être considéré comme un commencement de preuve par écrit.

Pour résumer ce qui a été démontré au paragraphe précédent, le document électronique n'est pas un écrit. Il n'est pas signé par son auteur, au sens où on comprend ce concept de signature de manière traditionnelle. La formalité du double original imposée par l'article 1110 c.civ. dans le cas des conventions synallagmatiques ne peut être respecté, puisqu'un document numérique n'a pas d'original. Les promesses unilatérales de sommes d'argent ne peuvent absolument comporter ni la mention manuscrite et en lettres de la somme d'argent, ni la signature manuscrite.

⁶ ART. 1110 C.CIV.

⁷ ART. 1111 C.CIV

L'admission du document électronique comme commencement de preuve par écrit n'est pas non plus garantie. Le commencement de preuve par écrit, défini par l'article 1132 c.civ, est « *l'acte par écrit émané de celui contre lequel la demande est formée, ou de celui qu'il représente, et qui rend vraisemblable le fait allégué* ». Par écrit il faut entendre ici un écrit auquel il manque les conditions légales de la preuve littérale. L'existence du commencement de preuve par écrit permet de compléter les informations du document par les témoignages ou des présomptions. Or l'admissibilité du commencement de preuve par écrit et par voie de conséquence des indices, présomptions ou témoignages suppose que le créancier se soit trouvé dans l'impossibilité de se procurer un écrit⁸. Or à l'ère du courrier aérien express, il est difficile de convaincre un tribunal de l'impossibilité matérielle d'établir un document contractuel écrit.

Le droit haïtien oppose donc une barrière infranchissable à l'admission du document électronique comme mode de preuve des engagements des parties. Pourtant les opérateurs économiques individuels et institutionnels recourent de plus en plus à l'Internet pour leurs transactions. Pour sécuriser les acteurs et permettre l'expansion de ce type d'échanges, une réforme législative s'impose. Un bref survol des solutions apportées à ce problème à l'étranger nous permettra de justifier les réponses proposées dans le projet de loi sur la signature électronique et son arrêté d'application.

Section II - Les Réponses Proposées pour l'Admissibilité du Document et de la Signature Electroniques

Les défis posés au droit par l'existence des documents électroniques ont entraîné les pouvoirs publics, aiguillonnés par les acteurs économiques à adapter le droit de la preuve pour tenir compte de cette nouvelle réalité. Les concepts d' « *écrit* » et de « *signature* » ont dû être revisités et les réponses à ces défis se retrouvent tant au niveau international (#2) que national (#3). Auparavant, il est nécessaire, pour la compréhension des approches législatives, de se familiariser avec les concepts sur lesquels se base ce mouvement quasi universel de l'adaptation du droit à la technique (#1).

1 - La définition des concepts

L'objectif des réformes législatives actuelles est de conférer au document électronique une force probante égale à celle de l'écrit pour qu'il puisse être admis en justice. Dans les textes législatifs ou dans les études consultées, les expressions « *document électronique* » et « *document numérique* » sont le plus souvent interchangeables. Le **document électronique** est l'ensemble de données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable et qui peuvent être lues ou perçues par une personne ou par un tel système ou dispositif⁹. L'admissibilité du document électronique en justice est subordonnée à la certitude de l'inaltérabilité du contenu du texte sur lequel les parties s'étaient arrêtées. Cette certitude provient de la signature électronique.

⁸ ART. 1133 C.CIV.

⁹ ART. 31, LOI CANADIENNE DU 13 AVRIL 2000 SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ELECTRONIQUES

Comme dans le domaine de l'écrit, la signature permet de garantir l'authenticité de l'identité de celui qui a effectué l'opération et d'établir son adhésion. La **signature électronique** en plus des fonctions traditionnelles garantit l'intégrité, l'inaltérabilité du document échangé. Il existe plusieurs catégories de signatures électroniques. Certaines sont très simples. Les plus sophistiquées permettent d'identifier le signataire à partir des données biométriques qui lui sont uniques comme l'iris de l'oeil ou les empreintes digitales.¹⁰

Les systèmes de signature électronique qui se développent depuis quelques années reposent sur des algorithmes de chiffrement asymétriques, où, de plus, chaque utilisateur dispose de deux clés, une clé publique et une clé privée. Ces deux clés sont elles-mêmes créées à l'aide d'algorithmes mathématiques. Elles sont associées l'une à l'autre de façon unique et sont propres à un utilisateur donné. Un message chiffré à l'aide d'un algorithme asymétrique et d'une clé privée, qui constitue l'un des paramètres de l'algorithme, ne peut être déchiffré qu'avec la clé publique correspondante, et inversement. La clé publique doit donc être connue de tous, tandis que la clé privée reste secrète. Ce type de signature est parfois qualifié de numérique ou de digitale. Une définition communément admise provient de la loi-type sur le commerce électronique proposée par la Commission des Nations Unies pour le Droit Commercial International (CNUDCI).

D'après la CNUDCI une signature numérique est « *une valeur numérique apposée à un message de données et qui, grâce à une procédure mathématique bien connue associée à la clé cryptographique privée de l'expéditeur, permet de déterminer que cette valeur numérique a été créée à partir de la clé cryptographique privée de l'expéditeur. Les procédures mathématiques utilisées pour créer les signatures numériques sont fondées sur le chiffrement de la clé publique. Appliquées à un message de données, ces procédures mathématiques opèrent une transformation du message de telle sorte qu'un personne disposant du message initial et de la clé publique de l'expéditeur peut déterminer avec exactitude: a) si la transformation a été opérée à l'aide de la clé privée correspondant à celle de l'expéditeur; et b) si le message initial a été altéré une fois sa transformation opérée ...* ». Telle une signature manuscrite, la signature électronique ne peut être produite que par une unique personne, le détenteur de la clé privée correspondant à la clé publique utilisée pour la vérification. Si le document a été modifié durant son transport, la vérification de signature donnera un résultat négatif.

Mais à l'inverse de la signature manuscrite, la signature numérique, composée de chiffres, de lettres et d'autres signes, ne comporte aucun élément permettant de l'attribuer à une personne donnée. Chaque utilisateur doit donc établir avec certitude l'identité de ses correspondants. D'où le recours à des services de certifications, souvent désignés comme **tiers de certification**, ou prestataires de services de certification de signature électronique, qui disposent de la confiance de chacun et qui garantissent l'appartenance d'une signature à une personne. La vérification par le destinataire de la signature électronique de l'expéditeur suppose que le tiers certifie au destinataire que la clé publique qu'il utilise correspond bien à la clé privée de l'expéditeur signataire, et que ce dernier est bien celui qu'il prétend être. Le tiers de certification délivre donc des certificats d'authentification qui contiennent, d'une part, divers renseignements sur la personne dont on souhaite vérifier l'identité (nom, prénom, date de naissance ...) et, d'autre part, sa clé publique.

Il s'ensuit qu'un système accordant force probante au document et à la signature électronique ne peut fonctionner que dans un environnement juridique contenant des règles strictes assorties de sanctions dissuasives pour la protection de la vie privée et des renseignements personnels.

¹⁰ SUR L'ENSEMBLE DE LA QUESTION VOIR SENAT FRANÇAIS. SERVICE DES AFFAIRES EUROPEENNES. NOTE DE SYNTHÈSE SUR LA SIGNATURE ELECTRONIQUE. DECEMBRE 1999. WWW.SENAT.FR/LCC67/LC670.HTML

La tendance générale de la législation comparée en la matière consiste à ne pas présumer des avancées techniques et à adopter une neutralité technologique en établissant toutefois les critères permettant à un document et à une signature électroniques d'acquérir la force probante: identification certaine du signataire, intégrité du document échangé. Cette attitude de neutralité technologique, prônée par la Directive du 13 décembre 1999 du Parlement Européen et du Conseil Européen sur un Cadre Communautaire pour les Signatures Electroniques, et la Loi-type de la CNUDCI sur le Commerce Electronique, se retrouve dans la plupart des pays européens, de l'Amérique Latine et au Canada. Concernant les tiers de certification, certains Etats préfèrent qu'il s'agisse de personnes publiques, d'autres laissent libre cours à l'initiative privée, et un dernier groupe assortit l'exercice de certification à l'obtention d'une reconnaissance des pouvoirs publics. Cette dernière approche est la solution prônée dans les textes proposés. La reconnaissance de la certification en dehors des frontières de l'Etat n'est pas abordée par toutes les lois, même aux Etats Unis, et toutes ne se soucient pas d'établir la responsabilité de ces prestataires de services, laissant ce soin au droit commun.

2 - Les réponses internationales

Les projets de loi relatifs aux transactions électroniques et plus particulièrement à la preuve des transactions électroniques s'inspirent, en Europe, de la directive européenne sur un cadre communautaire pour les signatures électroniques adoptée le 30 novembre 1999 et, en dans le reste du monde, particulièrement dans une majorité écrasante de pays d'Amérique Latine, de la loi-type de la CNUDCI sur le commerce électronique adoptée le 16 décembre 1996.

A.- La Directive 1999/93/CE du Parlement Européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour /es signatures électroniques

Dans la hiérarchie des normes juridiques européennes, les directives occupent la place la plus élevée puisqu'elles s'imposent aux Etats membres et les obligent à harmoniser leurs législations en conséquence.

La directive se fixe pour objectif de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique, et institue un cadre juridique pour les signatures électroniques et certains services de certification¹¹. Elle opère une distinction entre la signature électronique et la signature électronique avancée. Cette dernière basée sur un certificat qualifié et créé par un dispositif sécurisé de création de signature doit pouvoir avoir la même valeur que la signature manuscrite et être recevable en justice¹². Pour cela, la signature électronique avancée doit satisfaire aux exigences suivantes :

- a) être liée uniquement au signataire ;
- b) permettre d'identifier le signataire ;
- c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; et
- d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.¹³

¹¹ ART.1, DIRECTIVE 1999/93/CE DU PARLEMENT EUROPEEN ET DU CONSEIL DU 13 DECEMBRE 1999 SUR UN CADRE COMMUNAUTAIRE POUR LES SIGNATURES ELECTRONIQUES

¹² ART. 5, IBID

¹³ ART. 2, IBID

On voit ici le refus de parti pris technologique. La directive proclame la liberté d'entreprise en matière de fourniture de service de certification de signature puisqu'elle interdit toute autorisation préalable¹⁴ tout en permettant aux Etats d'instaurer des régimes volontaires d'accréditations.

La directive incite les Etats membres à prévoir un régime de responsabilité à l'égard des prestataires de services de certification qui ont failli à leur mission¹⁵.

Dans le but de faciliter les échanges internationaux, la directive reconnaît l'équivalence aux certificats de signature délivrés par un prestataire de service de certification établi en dehors de l'Union Européenne, si le prestataire de service a reçu une accréditation dans un pays européen, ou si un prestataire de service de certification établi dans l'Union Européenne garantit le certificat ; ou si le prestataire de service est reconnu en vertu d'un accord international entre l'Union et des pays tiers¹⁶.

Elle insiste pour que les informations personnelles recueillies dans le cadre de la création de signature électronique avancée et de certification de signature ne puissent faire l'objet de diffusion indue¹⁷.

La directive est accompagnée d'annexes spécifiant les exigences concernant les certificats qualifiés, les prestataires de service de certification délivrant des certificats qualifiés, les dispositifs sécurisés de création de signature électronique, et énumérant les recommandations pour la vérification sécurisée de la signature.

B.- La Loi-type de la CNUDCI sur le commerce électronique

Dans le processus d'élaboration de cette loi, la Commission s'est penchée sur les travaux qui étaient en cours par la Commission Economique de l'Europe. Les obstacles relevés par la CNUDCI à la force probante des échanges électroniques sont ceux qui existent dans notre législation: a) nécessité de l'écrit ; b) nécessité de la signature manuscrite; c) utilisation d'original. Dans son approche, elle a décidé de réexaminer les règles juridiques en vertu desquelles ces obligations de formes étaient requises par la loi. Cette analyse a abouti à la théorie de l'équivalent fonctionnel, un des objectifs recherchés par les législateurs. C'est ainsi que la loi-type de la CNUDCI ne traite pas des relations dans le commerce électronique d'un point de vue technique, mais crée un cadre juridique aussi sûr que possible, de manière à faciliter le commerce électronique entre les parties.¹⁸

Cette loi dont le champ d'application s'étend au commerce en général fixe, en son chapitre II, les conditions générales de la reconnaissance juridique des messages de données comme écrit, comme signature, à titre d'original, et leur admissibilité comme preuve. Elle prévoit, toutefois les cas où les messages de données sont exclus et laisse aux législations nationales le soin d'établir les mécanismes de certification des signatures électroniques.

¹⁴ ART. 3, IBID

¹⁵ ART. 7, IBID.

¹⁶ IBID.

¹⁷ ART. 8, IBID.

¹⁸ LOI TYPE DE LA CNUDCI SUR LE COMMERCE ELECTRONIQUE ET GUIDE POUR SON INCORPORATION 1996
[HTTP://WWW.UNCITRAL.ORG/PDF/FRENCH/TEXTS/ELECTCOM/05-89451_EBOOK.PDF](http://www.uncitral.org/pdf/french/texts/electcom/05-89451_EBOOK.PDF)

3 - Les réponses nationales à l'étranger

Nous passerons en revue la manière dont les législateurs ont abordé la question des transactions et de la signature électroniques dans certains pays européens et américains.

A. - Les pays européens de droit civil

Les initiatives législatives dans les pays de ce continent se plient aux principes, exigences et recommandations exprimés dans la directive européenne.

A l'heure actuelle presque tous les pays européens ont adopté une législation appliquant la directive mentionnée précédemment. Ils furent précédés dans leur démarche par l'Allemagne et l'Italie. L'Allemagne par le biais d'une loi adoptée en juin 1997 sur la signature digitale, et l'Italie par un décret présidentiel de 1997 sur la réforme de l'administration publique, précisé en ce qui nous concerne par un décret du président du conseil promulgué en 1999. Ils ne reconnaissaient que certaines formes de signature électronique et leur accordaient des effets différents. Leur domaine d'application se limitait à la signature numérique, c'est-à-dire créée à l'aide d'un procédé de chiffrement asymétrique, laissant au juge le soin d'examiner les autres formes de signature électronique. Le décret italien accordait à la signature numérique la même force probante que la signature manuscrite. La loi allemande laisse au juge le soin d'examiner sa force probante, se contentant de définir les conditions dans lesquelles le destinataire peut être sûr de l'identité de l'émetteur et de l'intégrité des données transmises.

Les autres pays s'inspirent dans leurs législations de la directive européenne et définissent la signature électronique comme une donnée électronique qui sert de méthode d'authentification. N'excluant aucune forme de signature électronique, ils respectent le principe de neutralité technologique qui sous-tend la directive. Ces textes considèrent comme équivalentes aux signatures manuscrites les signatures électroniques créées dans des conditions de sécurité maximales, c'est-à-dire les signatures avancées qui, de plus, sont associées à un certificat fiable et sont créées par un dispositif sécurisé.

La notion de fiabilité optimale découle de la mise en place d'un dispositif d'accréditation qui, selon la directive européenne, doit être mis en place par les professionnels. Ce dispositif est intégré pratiquement dans tous les textes en vigueur en Europe.

B.- Le Canada

Nous relaterons ici, au niveau provincial le texte québécois, et la loi fédérale.

1) Le Québec

En 1993 le Québec a modifié son code civil en vue de reconnaître une valeur probante aux inscriptions informatisées. Une section spécifique, la Section VI, a été consacrée aux données informatisées, ces dernières n'entrant dans le champ d'application ni de la Section IV, consacrée aux actes sous seing privé, ni de la Section V consacrée aux autres écrits. L'article 2826 précise malgré tout, et ceci constitue une originalité par rapport à ce qui a été vu jusqu'ici, que le document signé sur support papier l'emporte sur le document conservé sur support électronique. Par ailleurs, la valeur probante de l'acte reproduisant les données est présumée dès lors que certaines conditions sont réunies (document intelligible, caractère intègre et intégral des données conservées).

2) La loi fédérale sur la protection des renseignements personnels et les documents électroniques

Cette loi fédérale a été sanctionnée le 13 avril 2000. Elle comprend deux parties, la première visant la protection des renseignements personnels dans le secteur privé, et la deuxième consacrée aux documents électroniques. Elle a pour objet de prévoir l'utilisation de moyens électroniques dans les cas où les textes législatifs envisagent l'utilisation d'un support papier pour enregistrer ou communiquer de l'information ou des transactions. Après avoir énuméré les situations où la version électronique d'un document, d'un paiement, ou même d'un serment sera acceptée, elle prévoit les conditions dans lesquelles le Gouverneur prendra des règlements pour entériner des technologies ou des procédés répondant aux critères d'une signature électronique sécurisée, la seule pouvant être assimilée à l'écrit. Ces critères se rapprochent de ceux préconisés par la CNUDCI et gardent une neutralité technologique¹⁹.

Premièrement, la signature électronique résultant de l'utilisation de la technologie ou du procédé est propre à l'utilisateur.

Deuxièmement, l'utilisation de la technologie ou du procédé pour l'incorporation, l'adjonction ou l'association de la signature électronique de l'utilisateur au document électronique se fait sous la seule responsabilité de ce dernier.

Troisièmement, la technologie ou le procédé permet d'identifier l'utilisateur.

Quatrièmement, la signature électronique peut être liée au document électronique de façon à permettre de vérifier si le document a été modifié depuis que la signature électronique a été incorporée, jointe ou associée au document.

3) Législation sur la signature électronique

Il convient de signaler qu'en 1999 la Conférence sur l'Uniformisation des Lois du Canada a adopté une loi uniforme sur le commerce électronique s'inspirant de la loi type de la CNUDCI et qu'à ce jour la majorité des provinces et territoires l'ont intégrée dans leurs législations internes²⁰.

C.- Les Etats-Unis d'Amérique

La législation américaine en matière de signature électronique est dispersée dans les divers Etats de l'Union²¹. Il convient de noter qu'en 1998 fut promulguée la Loi sur la Signature Numérique et la Certification Electronique²². Cette loi adopte le principe de la neutralité technologique et se rapproche des critères définis internationalement. C'est ainsi que la certification électronique d'un

¹⁹ ART.48, LOI FEDERALE CANADIENNE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ELECTRONIQUES

²⁰ CNUDCI. OP.CIT

²¹ MORGAN JOHN, GIDARI ALBERT, INTERNET LAW & POLICY FORUM, *SURVEY OF STATE ELECTRONIC & DIGITAL SIGNATURE LEGISLATIVE INITIATIVES*, WWW.ILPF.ORG/DIGSIG/DIGREP/HTM

²² DIGITAL SIGNATURE AND ELECTRONIC AUTHENTICATION LAW (SEAL)

document électronique, défini comme un moyen électronique cryptographique ou autre, doit permettre à son utilisateur d'authentifier l'identité de l'expéditeur d'un document électronique et de lui associer le contenu du document, de certifier l'intégrité du document de sa transmission à sa réception, et que le document reçu est bien celui envoyé par la personne identifiée comme celle se prétendant en être l'expéditeur²³.

A la fin de l'année 1999, quarante Etats avaient soit envisagé soit promulgué des lois d'authentification électronique. Toutefois, l'essentiel de cette activité législative se donnait un champ d'application étroit, à l'exemple de lois applicables seulement dans un contexte gouvernemental ou à un secteur restrictif de l'activité privée, comme le secteur financier, l'utilisation de la signature électronique par les établissements de soins médicaux ou pour l'enregistrement de véhicules à moteur.

Trois Etats²⁴ avaient une législation s'inspirant de la loi-type de la CNUDCI en application des recommandations de la Conférence Nationale des Commissions des Juristes sur l'uniformisation des législations des Etats qui en 1999 avait adopté et proposé l'Uniform Electronic Transactions Act. Un regard sur la législation californienne permet de dégager les caractéristiques de cette législation relativement au standard d'identification. Une signature électronique est recevable en justice si elle est unique à la personne de son utilisateur, est capable de vérification, demeure sous le contrôle exclusif de son utilisateur, est liée aux données informatisées d'une manière telle qu'une altération du contenu du document invalide la signature, et est conforme aux règlements adoptés par l'autorité de l'Etat compétente, généralement le Secrétaire d'Etat. Cette approche se rapproche des modèles européens, canadiens et latino-américains en ce qu'elle s'inspire de la loi-type de la CNUDCI sur le commerce électronique et de la directive européenne. En effet les critères sont flexibles, conservent une neutralité technologique et laissent le soin aux autorités réglementaires d'accréditer les technologies au fur et à mesure de leur évolution. Aujourd'hui, cette approche a prévalu sur les autres modèles et quarante-huit Etats ont une législation s'inspirant de la loi-type²⁵.

D.- Autres pays du continent américain

Des textes législatifs fondés sur la loi-type de la CNUDCI sur le commerce électronique ont été adoptés dans onze pays²⁶. Parmi eux, la Colombie, l'Equateur, le Panama, le Pérou et la République Dominicaine ont édicté une législation spécifique modifiant leur code civil pour adapter leur droit de la preuve aux signatures électroniques. Il convient de noter que la République Dominicaine s'est dotée depuis 2002 d'une loi qui englobe dans son champ d'application non seulement la signature électronique, mais les échanges électroniques d'une manière générale²⁷. Le 8 avril 2003, un décret d'application de ladite loi²⁸ est venu compléter le dispositif en réglementant de manière précise et exhaustive l'établissement et le fonctionnement des prestataires de service de certification électronique, leur responsabilité vis-à-vis de leurs clients et l'admissibilité des certificats émanant de

²³ SEC 3(G) DE LA LOI SEAL

²⁴ ILLINOIS (1998), CALIFORNIE (1999), PENNSYLVANIE (1999)

²⁵ CNUDCI OP.CIT.

²⁶ COLOMBIE (1999), EQUATEUR (2002), GUATEMALA (2008), MEXIQUE (2000), PANAMA (2001), PEROU (2000), REPUBLIQUE DOMINICAINE (2002), VENEZUELA (2001), BERMUDES (1999), ILES CAÏMANS (23000), TURKS AND CAICOS (2000)

²⁷ LOI NO 126-02 DU 14 AOUT 2002 SUR LE COMMERCE ELECTRONIQUE, LES DOCUMENTS ET LES SIGNATURES NUMERIQUES

²⁸ DECRET NO 335-03 DU 8 AVRIL 2003, PORTANT REGLEMENT GENERAL D'APPLICATION DE LA LOI NO 126-02 SUR LE COMMERCE ELECTRONIQUE, LES DOCUMENTS ET LES SIGNATURES NUMERIQUES

l'étranger. Le rôle de l'Institut Dominicain des Télécommunications (INDOTEL), l'équivalent de notre CONATEL, est précisé quant à son pouvoir de police à l'égard des services de certification de signature électronique.

4 - La réponse proposée en Haïti

Pour la modernisation du droit haïtien en la matière, et pour permettre que le pays tienne son rang dans les échanges commerciaux internationaux, il fallait doter les opérateurs économiques haïtiens d'instruments légaux leur permettant de sécuriser leurs échanges dans une économie de plus en plus pénétrée par l'internet. Tout en gardant les spécificités de l'architecture de notre droit, il était impératif de coller au plus près de meilleures pratiques internationales en la matière et d'y refléter les grands principes adoptés par le droit international et le droit comparé. Les textes proposés pour l'adoption législative sont de deux ordres. Le premier est un projet de loi sur la signature électronique, adaptant le droit de la preuve aux technologies de l'information et élargissant les compétences du Conseil National des Télécommunications.

A.- Le projet de loi sur la signature électronique.

Ce projet de loi traite d'abord de la signature électronique et établit l'équivalence de force probante entre le document électronique et le document papier. *Ces questions étant traitées dans le Code Civil, pour en garder la cohérence, il nous a semblé plus opportun d'y modifier directement les articles pertinents.* Ce faisant on évite les difficultés d'interprétation entre le texte du code et celui d'un texte spécial, limitant ainsi l'éparpillement du droit civil entre diverses lois particulières.

1) Valeur probante de l'écrit informatique

Le projet introduit une nouvelle définition de la notion de preuve littérale ou par écrit, indépendante de son support physique et des modalités de sa transmission en cas de commercialisation à distance, pour y inclure le document électronique²⁹. Il établit les conditions nécessaires à l'admission comme preuve du document électronique comme preuve : intelligibilité, identification de l'expéditeur, fiabilité de la conservation pour en garantir l'intégrité³⁰. Lorsqu'il est signé il a la même force probante que l'acte sous seing privé sur support papier.³¹

2) Signature électronique

Le projet consacre pour la première fois la définition doctrinale de la signature qui est une définition fonctionnelle. La signature identifie l'auteur de l'acte et manifeste son consentement au contenu de l'acte. Cette définition générale pourra s'appliquer tant à l'acte sur support papier qu'au document électronique.³² La signature électronique y est précisée en termes généraux de manière à pouvoir s'adapter aux évolutions techniques : elle « *consiste en l'usage d'un procédé fiable*

²⁹ NOUV. ART. 1101 AL. 2 C.CIV

³⁰ NOUV. ART. 1101 AL. 3 C.CIV

³¹ NOUV. ART. 1101 AL. 5 C.CIV

³² NOUV. ART. 1101 AL. 5 C.CIV

d'identification garantissant son lien avec l'acte auquel elle s'attache ». ³³ Ainsi à la fiabilité du processus employé, s'ajoute un lien indissociable entre la signature et le message.

La fiabilité de la signature et du document électroniques dépendent de la certification effectuée par des prestataires de services de certification électronique. D'où l'importance cruciale de l'arrêté d'application qui viendra en réglementer le fonctionnement et en établir les exigences techniques.

3) Mentions manuscrites

Le projet de loi adapte les exigences de mentions manuscrites concernant les engagements de payer une somme d'argent, en remplaçant les expressions « *écrit en entier de la main de celui qui le souscrit* » et « *écrit de sa main* » figurant aux articles 1111 et 1112 du code civil par celle de « *écrit en entier par celui qui le souscrit* » et « *écrit par lui-même* ».

4) Conventions de preuve et règles de conflit de preuve

Le projet de loi laisse au juge le soin de régler le conflit de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support ³⁴. Est ainsi éliminée toute hiérarchie entre la preuve sous forme électronique et la preuve littérale traditionnelle. Les parties demeurent toutefois libres d'établir toutes conventions portant sur la preuve de leurs échanges et des documents qu'ils produisent et signent. Cette disposition sera particulièrement utile pour le secteur bancaire et financier.

5) Actes authentiques

Quoique cette possibilité soit demeurée ouverte, les avancées en ce domaine ne nous paraissent pas encore avoir fait leur preuve à l'étranger d'où l'absence d'arrêté d'application en ce domaine.

6) Les prestataires de services de certification de signature électronique

Vu l'importance des prestataires de services de certification électronique, le projet de loi y consacre un chapitre. L'initiative privée est consacrée dans ce domaine moyennant une attestation de qualification à délivrer par le CONATEL. Les conditions de leur établissement sont précisées de même que sont régis les rapports qu'ils entretiennent avec leurs clients, dans le respect de conditions de fiabilité, de permanence, de confidentialité. ³⁵

7) L'élargissement des compétences du CONATEL

La loi sur la signature électronique et modifiant le droit de la preuve reconnaît au CONATEL des pouvoirs assez étendus de contrôle de surveillance et de police des prestataires de services de certification. Ce choix participe du pragmatisme. L'Etat ne peut se désengager d'échanges où l'intégrité personnelle des utilisateurs et la sécurisation des échanges économiques sont en jeu. Il est nécessaire de pouvoir exercer une surveillance sur les institutions publiques ou privées utilisant les communications électroniques. Toutefois, il serait contre-indiqué de créer de toutes pièces une nouvelle administration dotée d'un nouveau budget. Il nous a semblé qu'il était plus opportun de partir de ce qui existe et d'élargir les compétences de cet organisme autonome. Pour ce faire, la procédure

³³ IBID.

³⁴ NOUV. ART. 1101 AL. 4 C.CIV

³⁵ CHAPITRE II DE LA LOI SUR LA SIGNATURE ELECTRONIQUE

législative étant un passage obligé, le troisième chapitre de la loi est consacré aux nouvelles compétences du CONATEL en ce qu'il modifie pour l'amplifier sa loi organique.

L'approche adoptée, tout en tenant compte des principes reconnus internationalement, est simple et souple. La modification législative du code civil admet en preuve les données électroniques, quels que soient leur support et leur nature. Dans cette catégorie, nous pourrions inclure les télécopies, les télex, les photocopies, tout en laissant au juge le soin d'examiner leur force probante. Par contre, la signature électronique admise en preuve au même titre que la signature manuscrite fait l'objet de conditions de formes définies par arrêté. Cette formule évite d'avoir à modifier la loi en raison de l'émergence de nouvelles technologies de l'information.

B.- Le projet d'arrêté d'application de la loi sur la signature électronique

Cet arrêté est le complément indissociable de la loi sur la signature électronique. Le texte sans lequel la loi ne trouvera pas application. Il précise les conditions de sécurité, d'intégrité et de fiabilité auxquelles doivent obéir les dispositifs de création de signature électroniques de manière à éviter les usurpations d'identité et les impostures ainsi que la fiabilité de la transmission des données informatisées.

Il établit les exigences techniques pour qu'un dispositif de vérification de signature électronique soit certifié par le CONATEL. Ces exigences ont pour but de garantir le résultat de la vérification par le destinataire du message de telle sorte qu'il ait la certitude que le message est reçu est bien celui qui lui a été expédié et que l'expéditeur est bien celui qu'il prétend être.

A cette fin, les certificats électroniques qualifiés font l'objet d'une réglementation minutieuse pour satisfaire aux objectifs exprimés dans le paragraphe précédent en prévoyant notamment les modalités de suspension ou de révocation de certificats électroniques en cas de procédure d'absence, de disparition ou de mise sous tutelle.

Les prestataires de services de certification électroniques seront soumis à des exigences techniques auxquelles ils devront satisfaire pour l'obtention de l'attestation de qualification devant être délivrée par le CONATEL. Ces exigences, en dépit de leur précision, ne prennent aucun parti pris technologique en vue de préserver l'intégration de nouvelles techniques induites par les avancées de la science. Les modalités du contrôle du CONATEL à toutes les étapes de leur existence sont aussi incluses dans le projet d'arrêté en vue de diminuer les possibilités d'arbitraire.

La loi sur la signature électronique et son arrêté d'application constituent le premier volet de l'ensemble juridique destiné à adapter le droit haïtien aux nouvelles technologies. Les rapports privés ont besoin de sécurité surtout en ce qui a trait aux échanges ayant pour objet la fourniture de biens ou de services.

CHAPITRE II

LA FOURNITURE DE BIENS ET DE SERVICES

PAR DES MOYENS ELECTRONIQUES

(Le Commerce Electronique)

Les développements qui suivent se concentreront sur la manière d'appréhender juridiquement le commerce électronique et les contrats que permet l'internet. Seront délibérément écartés les considérations sur l'importance économique croissante de ce type d'échanges. Tout d'abord qu'est-ce que le commerce électronique ? Défini simplement, le commerce électronique regroupe les relations à fins économiques au moyen d'instruments utilisant des données numériques³⁶. Nous préférons, parce que plus complète, la définition retrouvée dans la Résolution 51/162 de l'Assemblée Générale de la Commission des Nations Unies pour le Droit Commercial International du 16 décembre 1996 recommandant aux Etats membres de tenir compte de la loi-type de la CNUDCI sur le commerce électronique. Par commerce électronique, il faut entendre les opérations commerciales recourant à l'échange de données informatisées et à d'autres moyens de communication et supposant l'utilisation de moyens autres que les documents papier pour communiquer et conserver l'information.³⁷

Le commerce électronique peut utiliser des réseaux ouverts ou fermés.³⁸ Dans un réseau fermé, les problèmes juridiques sont réglés d'avance. Le réseau fermé existe à l'intérieur d'une entreprise, relie une entreprise à ses clients privilégiés ou des entreprises semblables. Un accord ou un règlement existent précisant l'objet, la loi compétente, les responsabilités, les règles de preuve ou de confidentialité. Un exemple de réseau fermé est le SWIFT, Society for Worldwide Interbank Financial Transactions, association belge créée en 1973 et regroupant presque toutes les banques mondiales. A travers le réseau SWIFT s'effectuent les transactions bancaires entre banques. L'accès au réseau est réservé exclusivement aux banques membres. Un autre exemple est le SITA qui est la Société Internationale de Télécommunications Aéronautiques, société coopérative regroupant près de six cents compagnies aériennes et utilisée, en matière de transport aérien, pour la réservation de places et les informations sur les vols.

Il en va autrement dans un réseau ouvert comme l'internet, grâce auquel beaucoup de contrats se concluent ponctuellement entre des parties qui se rencontrent occasionnellement. L'internet ne fait pas appel à un service ou à une technologie appartenant à une personne déterminée ; et le réseau est à la fois public, gratuit et coopératif. En conséquence, les règles du jeu ne sont pas fixées à l'avance. Les contrats conclus grâce à l'internet présentent des caractéristiques qui

³⁶ BLAISE CYRIL, *LE COMMERCE ELECTRONIQUE ENTRE PROFESSIONNELS EN RESEAU OUVERT (INTERNET)*, MEMOIRE DEA, PARIS, WWW.ERIDIA.COM/CBLAISE/MEMOIRE/CFM

³⁷ CNUDCI, *LOI-TYPE DE LA CNUDCI SUR LE COMMERCE ELECTRONIQUE ET GUIDE POUR SON INCORPORATION 1996*, [HTTP://WWW.UNCITRAL.ORG/PDF/FRENCH/TEXTS/ELECTCOM/05-89451_EBOOK.PDF](http://WWW.UNCITRAL.ORG/PDF/FRENCH/TEXTS/ELECTCOM/05-89451_EBOOK.PDF)

³⁸ BLAISE CYRIL, *IBID.*

sont autant de défis posés au droit. Tout d'abord la dématérialisation qui induit le problème de la preuve des transactions électroniques et de l'admissibilité en justice des données informatiques. Ensuite la délocalisation qui rend difficile les réponses à apporter aux questions relatives au lieu de conclusion ou d'exécution du contrat. En troisième lieu l'identification du cocontractant est parfois difficile, or il est important que les parties soient certaines de l'identité de leurs partenaires, non seulement pour en faire la preuve, mais également pour déterminer la loi applicable en matière de capacité. Enfin le contrat électronique est souvent international, rendant malaisé, à défaut de stipulation expresse des parties, la détermination de la loi applicable.

Lors de la conclusion du contrat, les informations échangées peuvent amener à se poser des questions relatives à la responsabilité civile ou même pénale d'un intermédiaire. Le fournisseur d'accès à l'internet (FAI)³⁹ est-il obligé de fournir l'identité de l'utilisateur ? Quelle est la responsabilité du site marchand quant à la licéité des services ou biens offerts ?⁴⁰ Certains contrats peuvent-ils être annulés comme étant contraires à l'ordre public ? Mais l'ordre public de quel pays ? Et on revient à la question de la loi applicable.

Les questions qui viennent d'être mentionnées n'ont pu trouver de réponse juridique que très récemment. Dans la foulée des réflexions universitaires, aiguillonnés par la nécessité de normes pour encadrer ce nouveau mode de relations interpersonnelles et commerciales, les Etats ont légiféré soit pour englober l'ensemble du commerce électronique, soit pour n'en appréhender que certains aspects, particulièrement celui de la preuve et de la signature électronique. La réponse est également internationale. Les institutions internationales ont à cet égard émis des normes que nous aborderons plus tard. Surtout la Commission des Nations Unies pour le Droit du Commerce International a élaboré une loi-type dont s'inspirent nombre de pays.⁴¹ Haïti a emboîté le pas et dans le cadre du Groupe de Travail sur les Technologies de l'Information et la Communication institué par le Président de la République, un ensemble de lois et d'arrêtés d'application est ici proposé à l'approbation de l'Exécutif et à la sanction du Parlement.

Le constat qui peut être fait à ce niveau est double. Premièrement le commerce électronique n'a pas bouleversé les règles du droit des obligations. En conséquence, les normes édictées ailleurs et proposée ici ne sont que des adaptations du droit existant nécessitées par l'évolution technique. Deuxièmement les règles édictées à l'étranger sont très récentes, datent en général de moins de dix ans, ce qui nous amène à apprécier avec beaucoup d'indulgence le retard relatif du législateur haïtien, retard d'autant plus excusable que le phénomène de l'internet est chez nous assez peu répandu. Tout de même ceci ne saurait justifier l'immobilisme, car tous nos concurrents économiques de la Caraïbe et de l'Amérique Latine se sont dotés de législations qui mettent le monde au bout de leurs doigts.

A l'instar des autres pays, nous nous sommes inspirés largement de la loi-type de la CNUDCI adoptée en 1996. Mais en l'analysant et en examinant les législations latino américaines qui l'ont adaptée, nous nous sommes rendus compte que ses dispositions avaient vocation à s'appliquer

³⁹ ENCORE APPELE INTERNET SERVICE PROVIDER (ISP)

⁴⁰ VOIR LA DIVERGENCE ENTRE LA LEGISLATION FRANÇAISE QUI INTERDIT LA VENTE DE PRODUITS OU DE LIVRES FAISANT L'APOLOGIE DU NAZISME OU DU RACISME ET LA LEGISLATION AMERICAINE COMMUNICATIONS DECENTRY ACT OF 1996 [47 USC #230 (c)(1)] QUI PROTEGE DES COMPAGNIES COMME YAHOO DE TOUTE RESPONSABILITE QUANT A DES INFORMATIONS NOCIVES PROVENANT DE TIERS. VOIR CEPENDANT TOUJOURS AUX ETATS-UNIS LE CHILDREN'S ONLINE PROTECTION ACT DU 19 OCTOBRE 1998 [47 USC ##223,230-231] ET LE CHILDREN'S ONLINE PRIVACY PROTECTION ACT (15 USC ##6501-6506)

⁴¹ VOIR SUPRA N. 35 ; ET POUR LE DETAIL DES ETATS AYANT ADOPTE LA LOI-TYPE DE LA CNUDCI CONSULTER

[HTTP://WWW.UNCITRAL.ORG/UNCITRAL/FR/UNCITRAL_TEXTS/ELECTRONIC_COMMERCE/1996MODEL_STATUS.HTML](http://www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/1996model_status.html)

largement au-delà du cercle des relations strictement commerciales pour englober l'ensemble des relations de droit privé où s'effectuent des échanges d'information ou la fourniture de biens ou de service. D'où son intitulé de projet de loi sur les échanges électroniques.

Les questions relatives à la preuve des documents électroniques, à leur admissibilité en justice et à la signature électronique faisant l'objet de textes législatif et réglementaire spécifiques, le projet de loi présenté ici s'attache exclusivement à la formation du contrat électronique en général (section I), quelques dispositions particulières s'intéressant au contrat électronique relatif au transport de marchandises (section II).

Section I.- La Formation du Contrat Electronique

Le contrat électronique se forme entre deux personnes qui ne se voient pas, à moins que, toujours grâce à la technologie de l'internet, elles aient pu négocier par visioconférence. En dehors des règles générales de formation du contrat, trois questions attirent particulièrement notre attention : l'identification des contractants, le moment de la rencontre de volontés et la preuve de l'engagement contractuel.

1.- L'identification des contractants

La problématique de l'identification des contractants rejoint par certains côtés celle de la preuve du contrat abordé dans la loi sur la signature électronique et la preuve des documents électroniques. Ici, il s'agit de décider si les données reçues émanent de l'expéditeur supposé. Car de même que sur support papier une signature manuscrite peut être contrefaite, en cas de support électronique, une personne non autorisée aura peut-être envoyé le message, mais l'authentification par codage, chiffage ou toute autre méthode pourra être néanmoins correcte. En principe un message de données émane de l'expéditeur lui-même. Dans l'impossibilité d'apporter une certitude absolue, le Projet de Loi sur les Echanges Electroniques prône l'établissement de présomptions selon laquelle dans certaines circonstances un message de données serait considéré comme émanant de l'expéditeur. Cette présomption tient lorsque le message a été envoyé par une personne autorisée à agir à cet effet au nom de l'expéditeur ou grâce à un système d'information programmé par l'expéditeur ou en son nom pour fonctionner automatiquement. A moins qu'il n'ait été averti d'une erreur ou d'une imposture par l'expéditeur lui-même, le destinataire est fondé à considérer qu'un message émane de l'expéditeur si pour s'assurer que le message de données émanait de l'expéditeur, il a correctement appliqué une procédure que l'expéditeur avait précédemment acceptée à cette fin ; ou si le message tel qu'il a été reçu résulte des actes d'une personne qui, de par ses relations avec l'expéditeur ou un agent de celui-ci, a eu accès à une méthode que l'expéditeur utilise pour identifier comme étant de lui les messages de données⁴².

⁴² ART. 9, PROJET DE LOI SUR LES ECHANGES ELECTRONIQUES

2.- Le moment et le lieu de conclusion du contrat

Un contrat électronique, c'est la rencontre d'une offre et d'une acceptation par terminal interposé. Le moment de l'offre, celui de l'acceptation et celui important de la formation du contrat doivent être déterminés. Cette opération ne remet pas en cause les mécanismes connus des juristes dans le cadre des contrats entre absents. L'internet ne bouleverse pas le droit mais oblige le juriste à appréhender les nouvelles technologies et à redécouvrir la richesse des solutions élaborées au cours des âges. Le commerçant propose ses produits sur la page web. L'acheteur après avoir inscrit des données personnelles et financières clique ou double clique. Dans les deux sens, il y a eu transmission de données, les deux parties se retrouvent alternativement expéditeur : le vendeur expéditeur de l'offre, l'acheteur expéditeur de l'acceptation.

La chronologie de ces messages est réglée par le projet de loi proposé⁴³. Sauf convention contraire, l'expédition d'un message de données intervient lorsque celui-ci entre dans un système d'information ne dépendant pas de l'expéditeur, qui peut être le système d'information d'un intermédiaire ou un système d'information du destinataire. La réception d'un message de données intervient au moment où le message entre dans le système d'information désigné ou à défaut dans le système d'information du destinataire. Un message de données entre dans un système d'informations lorsqu'il peut y être traité.

Néanmoins, dans le cadre du commerce électronique, très souvent, le système d'information du destinataire dans lequel le message est reçu ou à partir duquel le message est retiré est situé dans une juridiction autre que celle dans laquelle se trouve le destinataire final. L'emplacement du système d'information ne doit pas être considéré comme déterminant. D'où la solution de l'article 13 du projet de loi qui propose que sauf convention contraire le message est réputé avoir été expédié du lieu où l'expéditeur a son établissement et avoir été reçu au lieu où le destinataire a le sien ; l'établissement principal étant privilégié en cas de pluralité d'établissements et, à défaut d'établissement, la résidence habituelle.

Pour déterminer le moment de la conclusion du contrat, il faudra choisir entre deux options possibles. Soit le contrat est formé au moment où l'acheteur expédie son message, c'est la théorie de l'émission. Soit le contrat est formé au moment où le vendeur reçoit le message d'acceptation de l'acheteur, c'est la théorie de la réception. Le choix entre l'une ou l'autre des théories ayant des incidences pratiques sur l'antériorité de commandes à satisfaire et le lieu de conclusion du contrat et le transfert de propriété. Ces deux théories ont fait l'objet de controverses doctrinales et de solutions divergentes selon les pays. La jurisprudence française penche en faveur de la théorie de l'émission, mais dans beaucoup d'autres pays de common law et de droit civil la théorie de la réception est privilégiée. Par ailleurs, beaucoup de contrats électroniques sont des contrats internationaux, en ce sens où ils mettent en jeu des intérêts du commerce international, les frontières étant traversées par les biens. La Convention des Nations Unies, dite encore Convention de Vienne portant Loi Uniforme sur les Contrats de Vente Internationale de Marchandises trouve ainsi de plus en plus matière à s'appliquer vu le nombre croissant de pays qui la ratifient⁴⁴. Cette convention tranche nettement en

⁴³ ART. 12, IBID.

⁴⁴ AUJOURD'HUI AU NOMBRE DE 73, CNUDCI, CONVENTION DE 1980 SUR LES CONTRATS DE VENTE INTERNATIONALE DE MARCHANDISE, ETAT DES RATIFICATIONS, [HTTP://WWW.UNCITRAL.ORG/UNCITRAL/FR/UNCITRAL TEXTS/SALE GOODS/1980CISG STATUS.HTML](http://www.uncitral.org/uncitral/fr/uncitral_texts/sale_goods/1980CISG_status.html)

faveur de la théorie de la réception⁴⁵. Enfin la pratique du commerce électronique nous renseigne que l'offreur se considère lié à la réception du message de l'acceptant, ce pourquoi il confirme son engagement contractuel par l'envoi d'un accusé de réception.

3.- La preuve du contrat ; la signature électronique

Quoique la loi-type de la CNUDCI consacre des dispositions sur la signature et le document électroniques, ces dernières ne constituent pas à notre avis un modèle. Consciente de cette insuffisance, la CNUDCI a proposé en 2001 une loi-type sur la signature électronique. Pour notre part, ces questions font l'objet d'un projet de loi spécifique et d'un arrêté d'application présentés dans le chapitre précédent.

Section II.- Le contrat électronique de transport de marchandises

Le projet de loi sur les échanges électronique contient un chapitre sur le contrat de transport de marchandises conclu par le biais d'échanges de données informatiques. Toutes les dispositions générales de la loi sur les échanges électroniques lui sont applicables. Il est seulement précisé en les énumérant les divers aspects de ce type de contrat qui gardent leur validité s'ils sont stipulés sous la forme électronique.⁴⁶ Ces dispositions sont particulièrement utiles puisqu'elles permettent l'endossement du contrat de transport de marchandises par la voie électronique sans recourir nécessairement à la documentation papier.

L'adoption de ce projet de loi vient renforcer le dispositif ébauché avec la loi sur la signature électronique et adaptant le droit de la preuve aux nouvelles technologies. Dès lors que les moyens techniques seront mis en place pour assurer la sécurité et la conservation des échanges de données, les rapports privés contractuels pourront chez nous se développer sans limite, mais surtout dans les échanges internationaux, il pourra sans réserve être fait référence au droit haïtien.

⁴⁵ ART. 18, CONVENTION SUR LA VENTE INTERNATIONALE DE MARCHANDISES,
[HTTP://WWW.UNCITRAL.ORG/PDF/FRENCH/TEXTS/SALES/CISG/CISG-F.PDF](http://www.uncitral.org/pdf/french/texts/sales/cisg/cisg-f.pdf)

⁴⁶ ART. 14, PROJET DE LOI SUR LES ECHANGES ELECTRONIQUES

BIBLIOGRAPHIE SOMMAIRE

Textes législatifs

Textes internationaux

Loi type de la CNUDCI sur le commerce électronique, www.uncitral.org/fr

Directive 1999/93/CE du Parlement Européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *Journal Officiel des Communautés Européennes L. 13 du 19.01.2000 pp.12-20.*

Textes nationaux

Code civil haïtien

Projet de loi brésilien sur la signature électronique

Code civil du Québec

Loi canadienne sur la protection des renseignements personnels et les documents électroniques du 13 avril 2000, <http://lois.justice.gc.ca/fr/P-8.6/74408.htm/>

Loi française no. 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, *Journal Officiel no. 62 du 14 mars 2000 p. 3968.*

Décret français no. 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, *Journal Officiel no. 77 du 31 mars 2001 p. 05070*

Loi péruvienne no 27269 du 28 mai 2000 sur la signature et la certification numériques.

Loi péruvienne no 27291 du 25 juin 2000 modifiant les articles 141 et 1374 du code civil.

Loi dominicaine no. 126-02 du 14 août 2002 sur le commerce électronique, les documents et les signatures digitales

Décret dominicain no. 335-03 du 8 avril 2003 portant application de loi no. 126-02

Ouvrages

BOCHURBERG Lionel, *Internet et commerce électronique*, Dalloz, 2000

WEILL Alex, TERRE François, *Droit civil. Introduction Générale*, 4e. éd., 1979, Précis Dalloz.

Articles

AZZABI Sofian, Signature électronique et droit de la preuve. Approche juridique du sujet, www.ifrance.com/signelec/presentation.htm

COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL (CNUDCI), Etat d'adoption de la loi-type sur le commerce électronique de 1996
http://www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/1996Model_status.html

CONSEIL D'ETAT(France), SECTION DU RAPPORT ET DES ETUDES, Internet et réseaux numériques, www.internet.gouv.fr/francais/textesref/rapce98/rap2.htm#2

GIDARI Albert, MORGAN John, INTERNET LAW &POLICY FORUM, Survey of State Electronic &Digital Signature Legislative Initiatives, www.ilpf.org/digsig/digrep.htm

PREMIER MINISTRE (France), DIRECTION DU DEVELOPPEMENT DES MEDIAS, La signature numérique, www.internet.gouv.fr/francais/textesref/signnum.htm

PREMIER MINISTRE (France), DIRECTION DU DEVELOPPEMENT DES MEDIAS, La certification électronique, www.internet.gouv.fr/francais/textesref/certif/htm

SENAT (France), SERVICES DES AFFAIRES EUROPEENNES, Note de synthèse sur le régime juridique de la signature électronique en Europe, www.senat.fr/lc/lc67/lc670.html

DEUXIEME PARTIE
LE DOCUMENT NUMERIQUE
DANS LES RAPPORTS DE DROIT PUBLIC

CHAPITRE I

L'ADMINISTRATION ELECTRONIQUE : UN IMPERATIF⁴⁷

Introduction

A.- Etat des lieux

L'administration publique haïtienne se caractérise par une accumulation de procédures souvent opaques qui laissent le citoyen sans recours face à la lenteur et l'incompétence des fonctionnaires. Le recours aux connaissances personnelles ou à la corruption demeure trop souvent le seul moyen du citoyen pour obtenir ce à quoi il a normalement droit. La notion même de service public est dépourvue de toute réalité. Les services sont rarement organisés et gérés de manière rationnelle dans une optique de résultats ; les services sont souvent inexistants, sinon fournis avec telle mauvaise foi qu'ils paraissent jetés comme une faveur. D'autre part, le public, l'ensemble de la population, n'est pas perçu comme un client à satisfaire mais comme une orange à pressurer. L'expérience avec l'administration laisse comme dans beaucoup de pays une impression de temps perdu, mais particulièrement chez nous, un mauvais goût d'humiliation et de dégoût.

La centralisation géographique excessive des services administratifs empêche l'Etat d'atteindre le citoyen dans un pays à la topographie tourmentée et aux voies de communication terrestres largement insuffisantes. Le citoyen, mal ou pas du tout informé, ne peut trouver dans sa commune ou son département les services publics essentiels grâce auxquels il sera identifié, obtiendra un permis de conduire ou un passeport, accomplira les formalités douanières, créera une entreprise, une coopérative etc. Il se crée ainsi autant de « bantoustans » repliés sur eux-mêmes, la République unitaire se révélant dans bien des cas un leurre. Les grands principes du droit administratif sont assénés dans les facultés de droit et les écoles d'administration avec le plus grand sérieux à des étudiants ébahis persuadés qu'on leur dépeint une chimère : égalité devant les services publics, accessibilité de ces services, légalité des actes administratifs. Comment oser glorifier la continuité du service public lorsque fait défaut le minimum de continuité géographique du centre vers la périphérie ?

Les dossiers administratifs, les archives écrites de notre existence nationale ne jouissent pas de procédés de conservation qui les mettent à l'abri du feu, de l'humidité. Impossible de relier notre présent à un passé inaccessible donc inexistant.

Aujourd'hui, après le tremblement de terre du 12 janvier 2010, même les preuves de notre présent gisent sous des sarcophages de béton, bientôt emportées vers les fosses communes de l'oubli. Prouver qui nos sommes, nos liens de famille, nos droits réels, notre situation fiscale risque d'être impossible. De même, des procédures administratives ou judiciaires stoppées net le 12 janvier ne pourront reprendre, l'administration publique ou judiciaire en ayant perdu la trace, les administrés n'étant plus en mesure de fournir à nouveau des pièces justificatives.

⁴⁷ Cf. OCDE, L'ADMINISTRATION ELECTRONIQUE : IMPERATIF. PRINCIPALES CONCLUSIONS, *SYNTHESES*, MARS 2004, WWW.OECD.ORG/DATAOECD/34/54/31229653.PDF

Une réforme de notre administration s'avère donc urgente en vue de la rendre plus présente, plus transparente, plus responsable et plus efficiente et afin d'améliorer les rapports entre elle et les administrés. Les outils aujourd'hui disponibles grâce aux technologies de l'information et de la communication (TIC) jouent déjà un rôle de plus en plus éminent dans la transformation de l'Etat dans de nombreux pays particulièrement ceux du Tiers-Monde. Elles permettent de réaliser un saut qualitatif par la mise en place d'une administration électronique. En Haïti, le saut qualitatif est à notre portée et la mise en place de l'administration électronique permettra de résoudre les problèmes les plus cruciaux qui la gangrèment.

B.- Définition et contexte

L'administration électronique se définit par l'usage des technologies de l'information et de la communication par les entités administratives pour améliorer qualitativement les services et informations offerts aux citoyens ; augmenter l'efficacité et l'efficacités de la gestion publique et augmenter de manière substantielle la transparence du secteur public et la participation citoyenne⁴⁸.

La notion d'administration électronique est à placer dans le contexte de ce qu'il est convenu d'appeler « le consensus de Washington »⁴⁹. Le « consensus de Washington » plaide pour une deuxième génération d'ajustements structurels en vue de moderniser l'Etat par le biais de la réforme de la justice, de la participation du secteur privé dans la fourniture de services publics, de la réforme de la fonction publique et de l'amélioration de la gestion de l'Etat. L'administration électronique participe de la modernisation de l'Etat et constitue une des formes de la société de l'information⁵⁰. Elle implique que soient pris en compte non seulement des questions de pure gouvernance mais également les rapports qu'entretiennent le secteur public et les administrés. Elle met l'emphase moins sur les procédures que sur les résultats. L'administration électronique permet aussi à l'Etat de s'adapter à la réalité contemporaine de la globalisation économique et à son corollaire, la compétitivité. Dans un monde interconnecté, les Etats et les entreprises qui se maintiennent en dehors de l'univers technologique sont condamnés à être perdants. De par les économies qu'elle favorise en termes de temps et d'argent, l'administration électronique figure parmi les exigences d'un secteur privé avide de rentabilité pour sa survie économique. Elle représente enfin l'un des outils qui tiennent compte d'un autre facteur universel : la pression interne et internationale en vue de la transparence et de la probité des gouvernements. En conclusion l'administration électronique ne se résume pas à une question d'internet et d'ordinateurs. Elle exige une réflexion sur la gestion publique, la gestion et l'impact des nouvelles technologies.⁵¹

Les objectifs de l'administration électronique, que l'on retrouve dans sa définition, visent l'amélioration des services publics, la simplification des procédures et le renforcement des processus démocratiques. Quand sa mise en œuvre est réussie on constate les avantages en termes de services

⁴⁸ OEA AG 0/06

⁴⁹ JOHN WILLIAMSON, *LATIN AMERICA ADJUSTMENT : HOW MUCH HAS HAPPENED ?*, INSTITUTE FOR INTERNATIONAL ECONOMICS, WASHINGTON, 1990

⁵⁰ A NOTER QUE DANS LES AMERIQUES LE CONCEPT DE « SOCIETE DE L'INFORMATION » EST REMPLACÉ PAR CELUI DE « SOCIETE DU SAVOIR », TRADUISANT L'IDEE QUE L'INFORMATION NE JOUE SON ROLE QUE POUR AUTANT QU'ELLE EST REÇUE, DIGEREE ET UTILISEE. VOIR EN CE SENS LE TITRE DE LA DECLARATION DE SANTO DOMINGO DE L'ASSEMBLEE GENERALE DE L'OEA DU 6 JUI 2006 INTITULEE « *GOUVERNANCE ET DEVELOPPEMENT DANS LA SOCIETE DU SAVOIR* ».

⁵¹ SUR TOUS CES POINTS VOIR CLAUDIO ORREGO LARRAÍN, LOS CAMINOS HACIA EL E-GOBIERNO. ESTRATEGIAS Y RECOMENDACIONES, IN RODRIGO ARAYA DUJISIN, MIGUEL PORRUA VIGÓN ET AL., *AMERICA LATINA PUNTOGOB. CASOS Y TENDENCIAS EN GOBIERNO ELECTRONICO*, ED. FLASCO-OEA, SANTIAGO, CHILI, PP. 41,42

à la population, aux entreprises et entre entités administratives. La population jouit d'une disponibilité continue des informations, profite de la réduction des délais et entretient une relation directe avec les décideurs. Pour les entreprises, la réduction des délais et la simplification des procédures fiscales et douanières, pour ne citer que celles-là, se traduit en gains de productivité et de compétitivité, et induit une diminution des coûts des services administratifs. Grâce à l'administration électronique, les entités administratives peuvent renforcer leur coopération tant au niveau local, national et même international.⁵²

C.- Haïti et l'administration électronique

Les citoyens haïtiens ont commencé à se familiariser à certains aspects de l'administration électronique grâce aux consulats étrangers qui offrent sur leurs sites électroniques des formulaires à télécharger pour les demandes de visas.

Au sein de l'administration publique il existe un embryon d'administration électronique manifesté par le système électronique de paiement des fonctionnaires (SYSPAY), le système de gestion des dépenses publiques (SYSDEP), le système informatisé de l'Office d'Assurance Véhicules Contre Tiers. Ces systèmes se présentent davantage comme des outils de gestion interne et méconnaissent l'approche de services à la population. A noter l'existence de sites web de certains ministères qui d'une part n'obéissent à aucune stratégie globale et d'autre part ne sont pas interactifs. L'informatisation de l'administration publique n'a pas fait l'objet d'une impulsion venue d'en haut et a abouti à des résultats très inégaux⁵³. D'un point de vue légal le seul texte qui voit l'ébauche d'une procédure administrative partiellement électronique est la Loi du 10 juin 2009 sur les Marchés Publics qui admet la possibilité de la publication de l'appel d'offres sous format électronique et le principe de la soumission de la candidature et des offres par voie électronique à l'autorité contractante sauf disposition contraire prévue dans l'avis d'appel d'offres⁵⁴. Toutefois les garanties de sécurité, de confidentialité et d'horodatage des communications électroniques transmises dans ce cadre ne sont pas établies. L'Administration Générale des Douanes a récemment annoncé que les procédures de déclaration douanière et de paiement des taxes y afférentes pouvaient s'effectuer par voie électronique ; et l'Université d'Etat d'Haïti a expérimenté à la rentrée de 2009 les procédures d'inscription en ligne. Dans le domaine de l'interopérabilité, il convient de mentionner le partage des bases de données de l'administration fiscale avec le Service de la Circulation des Véhicules de la Police Nationale en vue de la délivrance des permis de conduire.

On ne peut pour autant dire qu'Haïti se soit mise sur la voie de l'administration électronique ; ces expériences sont isolées ne participent pas d'un plan d'ensemble, aucun standard commun de création, de nommage et de fonctionnement ne gouverne les sites électroniques existants.

Il est intéressant à ce stade de notre développement de comparer la situation haïtienne avec celle des pays de l'Amérique Latine et des Caraïbes. Nous nous reportons pour cela au « *Rapport 2010 de l'ONU sur l'Indice de Développement de l'Administration Electronique* »⁵⁵ et aux commentaires qu'en a fait le Réseau Administration Electronique de l'Amérique latine et des Caraïbes

⁵² EUROPA, COMMISSION EUROPEENNE, *E-GOUVERNEMENT : L'ADMINISTRATION EN LIGNE*,

[HTTP://EUROPA.EU/LEGISLATION_SUMMARIES/IN](http://europa.eu/legislation_summaries/in)

⁵³ STÉPHANE BRUNO, *E-GOVERNMENT. BRIEF OVERVIEW OF THE CURRENT SITUATION IN HAITI*, 2008, 4 PAGES

⁵⁴ LOI DU 10 JUIN 2009 SUR LES MARCHES PUBLICS, ART. 39, 40-1, *LE MONITEUR*, NO. 60, 12 JUIN 2009

⁵⁵ WWW2.UNPAN.ORG/EGOVKB/DATACENTER/COUNTRYVIEW.ASPX

[Red Gobierno Electrónico de América Latina y Caribe]⁵⁶. L'Indice de Développement de l'Administration Electronique utilisé dans le rapport de l'ONU comprend trois composantes : les services administratifs disponibles par internet, ensuite l'infrastructure en matière télécommunications et l'accès à cette infrastructure, et enfin le capital humain. Sur 184 pays étudiés dans le monde, le champion de l'Amérique Latine et Caraïbes est la Colombie qui occupe le 31^e rang mondial, suivie de peu par le Chili, 34^e, et l'Uruguay, 36^e. Ces pays devançant l'Italie et le Portugal, respectivement 38^e et 39^e. Le leader de la Caraïbe est la Barbade qui se hisse au 40^e rang. Haïti occupe la dernière place de la région, au rang peu honorable de 169^e mondial. La comparaison avec nos voisins immédiats et concurrents économiques rend plus criant l'écart qui nous sépare d'eux. En effet, la République Dominicaine est 84^e, la Jamaïque 89^e et Cuba communiste est 96^e.

Si on s'attarde sur la composante des services administratifs disponibles sur internet nous découvrons que pour un maximum possible de 1, la Colombie avec 0,71 et le Chili avec 0,61 dépassent la moyenne des pays développés qui est de 0,59. Au bas du tableau beaucoup de pays se situent en dessous de la moyenne régionale et nous y trouvons le Paraguay (0,26), le Nicaragua (0,25), Cuba (0,21) et, bonne dernière, Haïti (0,02).

Au classement mondial entre 2008 et 2010, Haïti a glissé de la 165^e à la 169^e place en raison des efforts accomplis par les autres pays et illustre le dicton « qui n'avance pas recule ». Il devient dès lors évident que l'objectif posé par le GTIC de faire d'Haïti le leader de la Caraïbe en matière d'utilisation des technologies de l'information apparaît, sinon utopique, un formidable défi et requerra une mobilisation et des efforts constants conduits par une politique d'Etat pilotée au plus haut niveau. La Constitution et les engagements internationaux du pays l'y obligent.

D.- Sources constitutionnelles d'une législation sur l'administration électronique

Nous trouvons dans la Constitution de 1987 l'énoncé de principes qui, appliqués à l'administration électronique, servent de base à toute législation, réglementation ou action dans ce domaine. Ils seront abordés dans l'ordre de leur apparition dans le texte constitutionnel.

L'article 5 établit les langues officielles : le français et le créole. Toute action dans ce domaine devra respecter le bilinguisme qui, réalité sociale et culturelle, n'est pas encore ressentie comme une exigence légale par nos pouvoirs publics.

Les articles 16 à 18 établissent l'égalité des citoyens dans la jouissance et l'exercice de leurs droits. La mise en place de l'administration électronique, loin de l'élargir, devra s'efforcer de réduire la fracture numérique entre ceux qui disposent d'infrastructure et d'équipements leur donnant accès aux services administratifs offerts par voie électronique et ceux qui en sont privés par leur niveau économique ou d'éducation et par des handicaps physiques.

L'article 28 consacre la liberté d'expression du citoyen en toute matière « *par la voie qu'il choisit* ». Ainsi, dans ses rapports avec l'administration publique, que ce soit pour formuler une requête ou émettre une plainte, le citoyen doit pouvoir, à sa seule discrétion, le faire en personne, par écrit ou par la voie électronique. D'où la nécessité de consacrer la validité juridique des documents électroniques.

⁵⁶ REDGEALC, *LES PAYS DE L'AMERIQUE LATINE ET DES CARAÏBES INEGAUX EN MATIERE D'ADMINISTRATION ELECTRONIQUE*, WWW.REDGEALC.NET

L'article 40 impose à l'Etat de publier les lois, décrets et tout ce qui touche à la vie nationale. On peut y lier les dispositions de l'article 125 sur la publication des lois et actes au Moniteur. La Constitution n'impose pas une publication sur support papier ; la publication des lois et actes par voie électronique devrait être reconnue légalement. De même, on peut déduire de l'article 40 que l'Etat, au sens le plus large du terme, trouve dans l'établissement de sites et de portails électroniques un moyen de diffusion des textes législatifs et réglementaires et des informations de toutes sortes à l'usage des administrés. C'est une manière d'améliorer la transparence de l'action administrative.

L'article 49 traite de la confidentialité des communications. L'utilisation des moyens électroniques doit être entourée de mesures garantissant la confidentialité des informations transmises, particulièrement celles portant sur des données à caractère personnel. Il devra être établi en outre que le partage de ces données entre entités administratives soit subordonné au consentement de l'administré.

L'article 54 aligne les droits civils des étrangers sur ceux des Haïtiens. Les étrangers pourront utiliser dans leurs rapports avec l'administration les moyens électroniques même pour les procédures qui les concernent en tant que tels (demandes de visa, de permis de séjour, de permis de travail etc.).

Le Protecteur du Citoyen a reçu à l'article 207 mission constitutionnelle de protéger les administrés contre les abus de l'administration publique. Il devra être à même de suivre l'implantation de l'administration électronique et de relayer auprès des différents responsables les griefs et insatisfactions des administrés. La loi devra lui fournir les outils nécessaires à cette mission.

Les principes de probité et d'efficacité de l'administration publique prônés à l'article 234 trouvent à s'appliquer dans le cadre de l'administration électronique. D'une part, par la simplification des procédures et les économies de temps et d'argent, l'efficacité de l'administration publique s'en trouvera améliorée. D'autre part, la possibilité pour l'administré d'être tenu au courant des différentes étapes et des agents publics en charge des procédures administratives électroniques contribuera à accroître la probité de l'administration et à diminuer la perception de corruption qui obère son image.

Enfin, il est nécessaire qu'une loi-cadre régie la mise en place de l'administration électronique ainsi que l'exige l'article 236 de la Constitution en vertu duquel le régime du fonctionnement de l'administration publique relève de la loi.

E.- Sources internationales de la législation sur l'administration électronique

En adoptant une loi sur l'administration électronique, la République d'Haïti traduit les engagements souscrits au niveau international et particulièrement ceux exprimés dans de multiples instruments internationaux dans le cadre de l'Organisation des Etats Américains.

Le Sommet Mondial sur la Société de l'Information tenue à Genève en 2003 a adopté dans une déclaration intitulée « *Construire la Société de l'Information : un Défi Global pour le Nouveau Millénaire* » ce qu'il est convenu d'appeler les Principes de Genève⁵⁷. Il y est proclamé que l'usage des technologies de l'information et de la communication et la création de contenus doivent respecter les droits humains et les libertés fondamentales, ce qui inclut la protection de la vie privée et la liberté d'opinion, de conscience et de religion, conformément aux instruments internationaux pertinents. Les

⁵⁷ [HTTP://OPENACCESS.INIST.FR/SPIP.PHP?PAGE=IMPRIMER&ID_ARTICLE=26](http://openaccess.inist.fr/spip.php?page=imprimer&id_article=26)

technologies de l'information et de la communication devant être vus comme un moyen et non comme une fin en soi.

Dans le cadre interaméricain la problématique des technologies de l'information et de la communication retient l'attention des Etats depuis les années 1990 et a fait l'objet de nombreuses déclarations et résolutions dont l'ancrage se situe dans la Charte Démocratique Interaméricaine adoptée par l'Assemblée Générale de l'OEA lors de sa première séance plénière tenue le 11 septembre 2001⁵⁸. La Charte Démocratique qui précise les dispositions de la Charte de l'OEA rappelle le droit des peuples des Amériques à la démocratie et l'obligation des gouvernements de la promouvoir et de la défendre ; ainsi que le droit des citoyens à participer aux décisions qui concernent leur développement. Elle identifie la transparence des activités gouvernementales, la probité et la responsabilité des gouvernements dans la gestion de la chose publique comme des composantes fondamentales de la démocratie.

Concernant les technologies de l'information et de la communication proprement dites nous trouvons une première référence dans la Déclaration des Chefs d'Etat et de Gouvernement adoptée à Miami lors du Premier Sommet des Amériques en 1994⁵⁹. Les télécommunications y sont mentionnées comme un des facteurs de l'intégration économique en vue de la promotion de la prospérité. La Déclaration de Québec adoptée lors du 3^e Sommet des Amériques de 2001⁶⁰ reconnaît le rôle de l'éducation dans la réduction de la fracture numérique et celui des technologies de l'information et de la communication dans l'efficacité de l'action gouvernementale afin de brancher les gouvernements et les peuples. A l'occasion du 4^e Sommet des Amériques tenu en 2005 à Mar del Plata en Argentine, la Déclaration qui y fut adoptée⁶¹ reflète l'engagement des Chefs d'Etats et de Gouvernements de la région à tirer parti des possibilités offertes par les technologies de l'information et de la communication pour accroître l'efficacité et la transparence du secteur public et faciliter la participation des citoyens à la vie publique, contribuant ainsi à consolider la gouvernance démocratique dans la région. Ils y prônent par conséquent l'adoption de programmes de formation des fonctionnaires publics à l'administration électronique et la mise en commun des meilleures pratiques dans le domaine.

Sur un plan plus institutionnel, l'Assemblée Générale de l'OEA qui eut lieu en Floride en 2005 adopta une déclaration intitulée « *Faire des bénéfices de la démocratie une réalité* »⁶² dans laquelle est reconnue le rôle important des technologies de l'information et de la communication pour le progrès de la prospérité, des valeurs démocratiques, des institutions démocratiques et de la sécurité de l'Hémisphère. Lors de la même session de l'Assemblée Générale, une résolution intitulée « *Promotion et Renforcement de la Démocratie* »⁶³ demande au Secrétaire Général, à travers les organismes pertinents de l'institution, de prendre en compte dans ses activités la contribution que peuvent apporter les technologies de l'information et de la communication au développement de sociétés plus justes, ouvertes et démocratiques.

Mais l'instrument le plus complet en la matière produit par l'OEA, est la Déclaration de Santo Domingo, « *Gouvernance et Développement dans la Société du Savoir* », adoptée le 6 juin 2006 par

⁵⁸ WWW.OAS.ORG/OASPAGE/FRN/DOCUMENTS/DEMOCRATIC_CHARTER.HTM

⁵⁹ WWW.FTAA-ALCA.ORG/SUMMITS/MIAMI/DECLARA_F.ASP

⁶⁰ WWW.FTAA-ALCA.ORG/SUMMITS/QUEBEC/DECARA_F.ASP

⁶¹ WWW.SUMMIT-AMERICAS.ORG/IV_SUMMIT/IV_SUMMIT_DEC_FR.PDF

⁶² AG/DEC.41 (XXXV-0/05)

⁶³ AG/RES.2119 (XXV-0/05)

l'Assemblée Générale de l'OEA⁶⁴. Les Etats américains s'y engagent à développer des stratégies nationales, à établir ou perfectionner leurs législations et cadre juridique et réglementaire en vue d'une sécurité juridique, pour le développement de la Société du Savoir. A cette fin, la déclaration comporte des engagements sur plusieurs points dont nous présentons ceux qui concernent plus spécifiquement l'administration électronique.

Dans la Déclaration de Santo Domingo, les Etats américains considèrent les technologies de l'information et de la communication comme un outil de développement équitable et durable ; de renforcement de la gouvernance ; de promotion et de protection des droits humains. D'où la nécessité de réduire la fracture numérique⁶⁵.

Ils demandent à l'OEA, ses organes et les entités qui y sont rattachées, d'appuyer les Etats membres en vue de l'incorporation des technologies de l'information et de la communication dans le processus de modernisation des institutions publiques. Ils favoriseront ceux qui envisagent la formation des fonctionnaires publics et qui ont pour but de renforcer la gouvernance et l'environnement démocratique, de promouvoir la transparence, la responsabilité, la participation citoyenne et l'efficacité dans la gestion et la fourniture de services dans le secteur public⁶⁶.

Ils s'engagent à accorder une attention spéciale à la modernisation de l'Etat au moyen de stratégies de mises en œuvre de l'administration électronique. Ces stratégies devront prendre en compte la formation des fonctionnaires, améliorer la fourniture de services et d'information à l'ensemble de la population et faciliter l'accès aux groupes défavorisés.⁶⁷

L'importance du multilinguisme en tant que richesse est reconnue. Donc les contenus de l'internet devront respecter cette diversité culturelle afin de déboucher sur une société du savoir plus inclusive.⁶⁸

Les Etats s'engagent à faciliter l'accès universel aux technologies de l'information et de la communication par la fourniture de points publics d'accès multimédia.⁶⁹

Ils promouvront l'usage des technologies de l'information et de la communication pour le suivi, le contrôle et l'évaluation de l'administration publique par les citoyens en vue de la concrétisation d'un gouvernement transparent et efficace ; une telle promotion devant renforcer la démocratie.

L'administration électronique se présente donc comme un impératif dans le contexte du vaste mouvement de modernisation de l'Etat dans lequel se sont investis l'ensemble des pays du continent. Sa mise en œuvre ne peut être abandonnée aux initiatives dispersées et désordonnées que nous avons identifiées. Pour que le classement d'Haïti s'améliore, pour que surtout l'administré ressente les changements promis en termes d'efficacité et de simplicité de l'administration publique il faut que soient remplies les conditions d'une implantation réussie de l'administration électronique (section I). L'aménagement du cadre légal pour accueillir de tels changements constitue l'un des outils de la stratégie mais en représente un point de départ incontournable (section II).

⁶⁴ AG/DEC.46 (XXVI-0/06)

⁶⁵ IBID. POINT 1

⁶⁶ IBID. POINT 2

⁶⁷ IBID. POINT 3

⁶⁸ IBID. POINT 8

⁶⁹ IBID. POINT 9

Section I.- Pour l'implantation réussie de l'administration électronique

En entamant le chemin de l'administration électronique, Haïti poursuit les initiatives de réformes de l'administration publique initiées par la Commission Nationale de Réforme Administrative et traduites par les deux décrets du 17 mai 2005 régissant désormais l'administration centrale de l'Etat et la fonction publique. Ces textes font du Conseil Supérieur de l'Administration et de la Fonction Publiques l'organe de pilotage de la réforme administrative. La création de l'Unité de Lutte contre la Corruption ou la réforme de la Cour Supérieure des Comptes et du Contentieux Administratifs complètent le dispositif. Le grand projet de mise en place de l'administration électronique constitue pour le Conseil Supérieur de l'Administration et de la Fonction Publique ayant à sa tête le Premier Ministre une occasion de légitimer son existence et d'exercer une influence décisive sur la transformation de l'Etat et de ses rapports avec les administrés. Le retard d'Haïti dans ce domaine représente une chance paradoxale. Elle n'aura pas à marcher à l'aveuglette, à tâtonner. Grâce aux avancées de ses voisins, elle ne peut se permettre de réinventer la roue. L'expérience des pays qui se sont résolument lancés dans cette voie aidera à identifier les obstacles à surmonter (#1), à formuler les objectifs à atteindre (#2), à poser les conditions du succès (#3) et à définir les étapes à franchir (#4). Pour finir seront avancées quelques recommandations en vue de progresser dans l'implantation de l'administration électronique (#5)^{70 71}

1.- Surmonter les obstacles

Les obstacles à surmonter pour l'implantation de l'administration électronique sont les suivants.

A.- L'absence de leadership et de volonté politique

Là où la mise en œuvre de l'administration électronique a échoué, la première cause identifiée est l'absence de leadership. Les plus hauts représentants de l'Etat ne s'en sont pas approprié et n'en ont pas fait une priorité de leur action. C'est exactement la situation dans laquelle se retrouve Haïti aujourd'hui.

B.- La fracture numérique

La fracture numérique est le fossé qui divise ceux qui ont accès aux équipements et au savoir informatique et ceux qui en sont privés. Il se mesure par l'accès aux réseaux de télécommunications, à

⁷⁰ SUR L'ENSEMBLE DE LA QUESTION VOIR SURTOUT, CLAUDIO ORREGO LARRAÍN, OP. CIT. P. 41-54. VOIR ÉGALEMENT JANE FOUNTAIN, *BUILDING THE VIRTUAL STATE*, BROOKINGS INSTITUTION PRESS, 2001 ; KATHERINE REILLY, ESTRATEGÍAS DE E-GOBIERNO EN OCHO PAÍSES DE AMÉRICA LATINA, IN RODRIGO ARAYA DUJISÍN, MIGUEL PORRÚA VIGÓN ET. AL., OP.CIT., P. 71-110 ; MARIA FRICK, DE LA TEORÍA A LA PRÁCTICA : CÓMO IMPLEMENTAR CON ÉXITO EL GOBIERNO ELECTRÓNICO. LA EXPERIENCIA REGIONAL Y LAS BARRERAS DE LA E-INNOVACION IN REDGEALC, SEDI-OEA, ICA/IDRC, *COLLECCION DE DOCUMENTOS DE TRABAJO SOBRE E-GOBIERNO*, NO. 3, P. 5

⁷¹ VOIR ÉGALEMENT LES 10 PRINCIPES DIRECTEURS POUR UNE ADMINISTRATION ELECTRONIQUE REUSSIE IN OCDE, *L'ADMINISTRATION ELECTRONIQUE : UN IMPERATIF*, OP. CIT.

l'accès chez soi ou dans un lieu public aux moyens de communications électroniques, à la pénétration de l'internet. Il est accentué chez nous par l'analphabétisme.

C.- Le manque de confiance des utilisateurs dans les technologies de l'information et de la communication

Pour vaincre cette méfiance, l'administré doit recevoir la garantie d'un accès sécurisé dans ses rapports avec l'administration et de la sécurité des transactions financières et autres communications effectuées par des moyens électroniques. La confidentialité des données à caractère personnel est également un facteur important de la confiance accordée à l'administration électronique.

D.- L'absence d'interopérabilité

L'administration électronique perdra de son intérêt et de sa légitimité si l'administré doit pour chaque nouvelle formalité fournir à nouveau à une entité administrative des pièces justificatives ou des renseignements dont cette même entité dispose déjà ou qu'une autre entité administrative détient. La raison réside dans l'absence de rapports entre les systèmes d'information de ces entités.

L'interopérabilité est le moyen par lequel les systèmes, les informations et les méthodes de travail sont interconnectés. Elle permet l'intégration de la fourniture des services en un guichet unique quel que soit le nombre de systèmes administratifs impliqués. Elle assure l'interfonctionnement avec des entités partenaires dont l'organisation et le fonctionnement peuvent diverger.

Pour prendre un exemple banal de l'absence d'interopérabilité des registres à l'intérieur d'une même administration, nous examinerons le système de l'état-civil. Les registres de naissance, de mariage et de divorces ne sont pas interconnectés. Quoique la loi punisse le crime de bigamie, un individu marié peut sans crainte se remarier dans un bourg où il est inconnu car l'extrait des archives de son acte de naissance ne mentionnera nullement son mariage. D'où l'inutilité pratique d'exiger un extrait récent d'acte de naissance car celui-ci ne renseigne nullement sur l'état civil actuel de cette personne.

#2.- Les objectifs à atteindre

Il ne suffit pas de proclamer que l'on veut mettre en place l'administration électronique. Encore faut-il que des objectifs soient clairement définis. Ceux qui sont proposés ici reflètent le consensus atteint par les chercheurs sur la question, sont étayés par les expériences réussies des pays qui nous ont devancé dans ce domaine et se conforment à la Déclaration de Santo Domingo.

A.- Améliorer la rapidité et la qualité des services publics offerts aux administrés

L'image d'Épinal de la bureaucratie la dépeint comme lente et multipliant comme par plaisir les démarches administratives. On ne peut sans repenser de fond en comble l'ensemble des procédures administratives se contenter d'inonder l'administration publique d'ordinateurs. La technologie ne doit

pas devenir le moyen de continuer à faire l'inutile de manière plus efficace. On ne peut plaquer l'outil technologique sur les anciennes manières de fonctionner. Le mouvement vers l'administration électronique doit être inscrit « dans un grand projet de réforme de l'Etat, qui est à dimension beaucoup plus managériale que technique »⁷².

B.- Générer des économies et une efficacité accrue

L'argument tiré des économies à attendre du fait de l'administration électronique quoique important ne peut être le seul. Toutefois, il mérite d'être développé. A ce titre il est intéressant de reproduire un extrait d'une étude réalisée par le cabinet de conseil en management et technologies de l'information Accenture. « Une étude réalisée par le gouvernement canadien montre qu'une transaction revient à 44 dollars canadiens lorsqu'elle est effectuée en personne, à 38 lorsqu'elle est réalisée par courrier et à 8 lorsqu'elle est traitée par téléphone. En comparaison, une transaction en ligne coûte à peine 1 dollar canadien. La direction irlandaise des impôts prévoit quant à elle une réduction de 500.000 euros sur les frais manuels, grâce à la télédéclaration. La disparition de centaines de milliers de formulaires, récépissés, relevés et autres aurait déjà permis d'économiser 600.000 euros sur les seuls frais de timbres (800.000 requêtes traitées par internet) »⁷³.

Du point de vue de l'efficacité, l'administration électronique doit déboucher sur de meilleures communication et coordination entre les organismes de l'Etat. Elle entraîne l'élimination des duplicata et un gain de temps.

C.- La massification de l'internet

Il n'est pas nécessaire d'attendre que l'internet soit universellement présent dans le pays ou dans les ménages. L'informatisation de l'Etat et la disponibilité des services en ligne a un effet multiplicateur. Dans les pays européens on a remarqué que le développement de l'administration électronique a été plus tiré par une logique d'offre que par la demande⁷⁴. De même dans les pays à faible taux de pénétration, comme en Amérique Latine, une offre de qualité de services administratifs en ligne génère la demande.

D.- La réduction de la fracture numérique

Le Rapport sur le Développement Humain de l'ONU paru en 2001 présente la réduction de la fracture numérique comme un des thèmes importants de ce début de siècle. Nous avons exposé plus haut à quel point il était présent dans tous les instruments et engagements internationaux relatifs à la Société du Savoir. La réduction de la fracture numérique requiert une action décisive de l'Etat passant par la création de contenus, la mise en place de points d'accès publics multimédia et la formation des citoyens à l'internet. Ce point constitue l'un des thèmes centraux du projet de législation sur

⁷² BRUNO LASSERRE, VERS UNE ADMINISTRATION A ACCES PLURIEL, IN UNIVERSITE DE PARIS I, L'INTERNET ET LE DROIT, DROIT FRANÇAIS, EUROPEEN ET COMPARE DE L'INTERNET, ACTES DU COLLOQUE DES 25-26 SEPTEMBRE 2000, COLLECTION LEGIPRESSE, VICTOIRE EDITIONS, PARIS, 2001, PP. 329-336

⁷³ ACCENTURE, LEADERSHIP EN MATIERE DE GOUVERNEMENT ELECTRONIQUE : HAUT RENDEMENT ET VALEUR MAXIMALE, 2004, CITE IN GERARD BRAUN, L'ADMINISTRATION ELECTRONIQUE AU SERVICE DU CITOYEN, RAPPORT AU SENAT (FRANÇAIS), 2004,

[HTTP://SENATRICE.FR/RAP/R03-402/R03-4021.PDF](http://senatrice.fr/rap/R03-402/R03-4021.pdf)

⁷⁴ BRUNO LASSERRE, OP. CIT.

l'administration électronique en Haïti, ainsi que dans l'avant projet de loi devant régir les télécommunications au travers de la création de points d'accès publics.

E.- Augmentation de la transparence et lutte contre la corruption

L'administration électronique, en permettant à l'administré de se maintenir au courant de l'état des démarches entreprises, de l'identité de l'agent public responsable apportera une contribution conséquente l'augmentation de la transparence et à la lutte contre la corruption.

F.- Meilleure participation citoyenne

Une stratégie d'administration électronique bien pensée doit rendre accessible au citoyen toute l'information publique, qu'il s'agisse de la législation, des missions et actions de l'administration, des procédures administratives. De la sorte la proximité entre les pouvoirs publics et la population sera accrue. A un stade supérieur de sophistication de l'administration électronique, les pouvoirs publics pourront, par le biais de forums ou de sondages en ligne, favoriser des débats publics, solliciter et obtenir les réactions des administrés sur des politiques publiques, des projets de législation ou d'action gouvernementale, ou des sujets d'intérêt local (municipalité) ou national. On renforcera ainsi la démocratie participative et le contrôle du gouvernement par les administrés.

L'ensemble de ces objectifs se retrouvent exprimés dans le projet de loi.

#3.- Les conditions du succès

Une fois posés les objectifs à atteindre, l'observation des expériences réussies permet d'identifier les raisons qui les ont amenées au succès.

A.- Une infrastructure minimum

La dotation de l'administration publique en matériel informatique doit atteindre une masse critique, car il constitue l'outil de base de l'administration électronique. Ensuite les entités administratives acquerront les logiciels performants propres à leurs secteurs d'intervention. Enfin l'exécution d'un programme de connectivité mettra en réseau les différents systèmes d'information.

B.- La capacité technologique des agents publics

La formation des fonctionnaires publics et autres agents de l'administration publique aux outils et aux nouvelles procédures de l'administration électronique est une des clés du succès. Si les fonctionnaires ne partagent pas la vision qui sous-tend le processus de transformation, s'ils craignent d'être rejetés ou marginalisés, ils peuvent constituer la plus grande force de blocage.

C.- Leadership

L'impulsion, la constance et la réussite de l'implantation de l'administration électronique reposent sur un leadership fort et clair. Un leadership qui se contente d'être technique et qui se situe à un niveau hiérarchique intermédiaire est insuffisant et ne donnera aucun résultat. Le leadership doit

obligatoirement se situer au niveau des plus hautes autorités politiques de l'Etat. Dans les pays d'Amérique Latine, les projets d'administration électronique sont conçus et pilotés par des organismes liés directement à la Présidence de la République ou la Primature. « Le leadership ne signifie pas bénéficier de l'appui politique du Président. Il faut une sagesse politique pour générer un agenda commun et une direction unifiée grâce à des processus clairs et la facilitation des rapports entre institutions. Cela signifie également qu'existe la volonté politique de concilier les diverses visions dans l'agenda de l'administration électronique, plutôt que de concevoir un agenda en fonction des personnes appuyant une vision déterminée »⁷⁵.

D.- Insertion de l'administration électronique dans des politiques publiques transversales.

L'administration électronique, nous le rappelons, ne peut être un projet isolé. Il est nécessaire que le projet soit géré, comme on vient de l'exposer, par une autorité jouissant d'une capacité de coordination interministérielle appuyée des équipes techniques générant des politiques publiques. En effet la mise en place de l'administration électronique induit nécessairement le développement de politiques relatives à la sécurité informatique, au degré acceptable d'inviolabilité des communications électroniques, à la protection de la vie privée, à l'externalisation de services publics etc. L'existence de ces politiques est un gage de la crédibilité du projet d'administration électronique.

E.- Un secteur des télécommunications concurrentiel et la pénétration de l'internet.

C'est presque un truisme d'affirmer que l'administration électronique ne peut exister si personne ne peut se connecter. La couverture du pays en matière de télécommunications est la condition de base pour que les administrés puissent accéder aux services publics offerts par la voie électronique. On a remarqué que dans les pays ayant développé leur infrastructure en matière de télécommunications et bénéficiant d'une pénétration de l'internet, comme le Singapour, la Finlande, la Suède ou le Canada, on assiste, presque par une relation de causalité, à une nette amélioration de la compétitivité du pays et à un décollage économique appuyé sur un système d'administration électronique performant.

F.- La désignation de projets emblématiques à fort impact et à court terme

On ne peut tout faire en même temps. Il faudra définir des priorités et identifier des projets phares réalisables dans un court délai dont les résultats sont visibles pour les citoyens. Ces projets menés à bien contribuent à générer la légitimité de la mise en place de l'administration électronique.

G.- L'alliance avec le secteur privé

Il serait hasardeux pour l'administration publique ou une de ses entités de tenter de créer sa propre technologie. Plutôt que de réinventer la roue il vaut mieux utiliser les entreprises privées pour développer les systèmes et faire fonctionner la technologie. L'alliance public-privé sera mutuellement profitable et productive pourvu que soient respectées les conditions de transparence.

⁷⁵ KATHERINE REILLY, OP. CIT., P. 104

#4.- Les étapes du succès

La mise en œuvre de l'administration électronique réclame que l'on sache par où commencer et comment progresser. Toujours en s'inspirant des pays qui ont réussi, nous présentons ici les étapes de la mise en œuvre en partant du plus simple vers le plus compliqué.

A.- L'informatisation

Il faudra commencer par doter les institutions publiques d'ordinateurs garnis des logiciels pertinents. Les ordinateurs ne peuvent être uniquement affectés à des tâches de secrétariat mais doivent tendre vers l'automatisation des tâches de calcul, de suivi du budget, de gestion de la correspondance etc.

B.- Rendre présente l'administration publique

Les entités administratives marquent leur présence par la réalisation de sites électroniques dont les pages d'accueil représentent la partie visible de l'administration électronique. La création d'un site portail général de l'administration publique doté d'un moteur de recherche doit permettre l'accès aux différents sites. Les sites électroniques ou le site portail rendent disponibles les informations utiles aux citoyens et aux entreprises. Ils concrétisent le principe de la continuité de l'État par la disponibilité de l'administration publique 24 heures sur 24 et 7 jours sur 7. L'accessibilité de l'administration publique est accrue de manière exponentielle grâce à la multiplication des lieux d'accès (n'importe quel ordinateur) et du nombre d'administrés que l'on peut servir avec le même personnel.

Mais pour éviter une multiplication désordonnée de sites électroniques il est opportun qu'une circulaire du Premier Ministre précise les critères de création de sites de l'administration centrale, des services déconcentrés et des organismes autonomes. La circulaire présentera les règles applicables au contenu, à la présentation, à la procédure de création, au nommage, à la sécurité des sites et à la protection de la vie privée des utilisateurs et des agents publics. La circulaire précisera les obligations de fiabilité, d'accessibilité et d'interactivité des sites, les obligations d'utilisation des deux langues officielles et la nécessité d'index thématiques et de moteurs de recherche⁷⁶.

C.- Réaliser l'interactivité

Il faut en effet dépasser le stade du site internet comparable à une simple vitrine pourvoyeuse d'informations statiques. Très rapidement les rapports électroniques entre l'administration et les administrés doit évoluer de l'information unidirectionnelle vers le dialogue virtuel. L'administré doit pouvoir interagir avec l'administration par le biais du courrier électronique, de la formulation de suggestions ou de réclamations, et par la possibilité de participer au débat sur des politiques publiques.

D.- Les téléprocédures

Les téléprocédures consistent en la possibilité d'effectuer les démarches administratives et d'obtenir des services administratifs par la voie électronique. On dépasse ainsi le simple stade de

⁷⁶ GEORGES CHATILLON, LES NOUVELLES PROCEDURES ADMINISTRATIVES DE L'ÉTAT, IN *L'INTERNET ET LE DROIT*, OP. CIT., P. 343.

Cf. CIRCULAIRE DU PREMIER MINISTRE FRANÇAIS RELATIVES AUX SITES INTERNET DES SERVICES ET DES ÉTABLISSEMENTS PUBLICS, *JOURNAL OFFICIEL*, 12 OCT. 1999, P. 1999

l'information et à ce niveau, les économies tant pour l'administration publique que pour ceux qui s'adressent à elles se font sentir. Les téléprocédures constituent le « fer de lance de la modernisation de l'Etat »⁷⁷.

Les contraintes juridiques liées à l'établissement des téléprocédures sont les suivantes ; elles sont abordées et réglées dans le projet de loi sur l'administration électronique : la valeur juridique de la transmission électronique, la datation de l'acte, la validité et le contrôle de la signature électronique, la confidentialité des contenus, les règles d'établissement des fichiers, et enfin le cryptage et la prévention de la cybercriminalité⁷⁸.

E.- L'interopérabilité

L'interopérabilité représente l'étape finale mais également la plus complexe de la mise en œuvre de l'administration électronique. Telle que définie précédemment elle vise à casser « les silos autarciques » présents dans tout gouvernement. En effet, le drame de tout administré réside dans la nécessité pour lui de passer par différents services en vue de remplir une formalité. Par exemple, avant qu'une société anonyme soit prête à fonctionner, il faut se rendre d'abord au Ministère du Commerce pour l'autorisation de fonctionnement, ensuite passer aux Presses Nationales pour acquitter les droits de publication des statuts, troisièmement à la Direction Générale des Impôts pour l'obtention de l'immatriculation fiscale et de la patente et retourner éventuellement au Ministère du Commerce pour l'enregistrement du nom commercial et du logo. Ces va-et-vient prennent du temps, et drainent une énergie lesquels auraient pu être plus utilement employés. L'interconnexion des différentes entités administratives, l'interopérabilité, est le remède, mais elle implique nécessairement une redéfinition des procédures, un changement de normes et la création de guichets uniques. Elle constitue une des obligations légales de l'administration publique dans le projet de loi sur l'administration électronique qui la prévoit et l'organise.

#5.- Les recommandations opérationnelles pour progresser

Les recommandations qui suivent rassemblent les opinions de ceux qui ont eu la tâche de conseiller mais surtout de mettre en œuvre des politiques d'implantation de l'administration électronique. Elles représentent en quelque sorte un condensé des bonnes pratiques dans le domaine. Elles sont complétées par des recommandations propres à l'environnement haïtien.

A.- Une étude sur l'état de préparation de l'administration

Une telle étude est nécessaire car elle permettra de prendre la photographie de l'administration au moment où démarre le projet en identifiant les forces et les faiblesses et servira de base pour l'élaboration du plan de mise en œuvre de l'administration électronique. L'étude doit prendre en compte les éléments suivants.

1.- L'état des télécommunications

L'infrastructure des télécommunications est un élément critique pour la réussite de l'administration électronique. Ainsi on mesurera avec certitude l'étendue de la fracture numérique.

⁷⁷ GEORGES CHATILLON, OP. CIT., PP. 337-348

⁷⁸ IBID.

2.- L'état des infrastructures physiques

On dressera par là l'inventaire quantitatif et qualitatif de l'équipement de l'administration en matériel informatique et en télécommunications.

3.- Le niveau et le type d'utilisation des technologies de l'information et de la communication actuellement dans l'administration

Ce volet permet d'évaluer la capacité de l'administration à gérer les informations et les projets d'administration électronique. Il permet également d'évaluer la capacité de l'administration à assurer des niveaux et des standards adéquats dans l'usage des technologies de l'information et de la communication. Il identifie enfin les bonnes pratiques existant au sein de l'administration.

4.- Les ressources humaines nécessaires à l'utilisation des technologies de l'information et de la communication

L'étude devra déterminer le personnel minimum capable d'utiliser les technologies de l'information et de la communication. Là où l'externalisation des services est nécessaire il faudra identifier un management interne compétent.

5.- Les ressources financières existantes et attendues.

Il est impératif de savoir si les objectifs et les projets bénéficieront de financement adéquat. Cela permet d'évaluer le degré de sérieux de la volonté politique.

B.- Rechercher les meilleures pratiques, faire appel à la coopération internationale et établir des repères

Dans ce cas il est recommandé de faire le « shopping » au niveau national et international en vue d'identifier les meilleures pratiques. Pour la mise en place de l'administration électronique, les responsables devront utiliser les mécanismes existant en ce domaine dans le cadre de la coopération internationale. Sur le plan de la coopération bilatérale, il faudra approcher les pays qui soit en raison de la langue, soit en raison de la proximité culturelle présentent l'avantage indéniable d'être parmi les leaders mondiaux ou régionaux en matière d'administration électronique. Nous pensons en ce sens au Canada, à la Colombie, au Chili ou à l'Uruguay. Sur le plan multilatéral des programmes existent qu'Haïti devra mettre à profit pour l'aider à la préparation du plan d'implantation, de la formation des fonctionnaires et des responsables du projet. Le RedGEALC⁷⁹, réseau de leaders en administration électronique de l'Amérique Latine et des Caraïbes, fut créée en 2003 à l'initiative du Secrétariat Exécutif pour le Développement Intégral de l'OEA et l'Institut pour la Connectivité dans les Amériques dans le but de favoriser la coopération horizontale entre les pays de l'Amérique Latine et des Caraïbes et de faciliter les échanges de solutions et d'experts entre ces pays. En plus des institutions fondatrices, le RedGEALC est aujourd'hui appuyé par la BID depuis 2005, et l'Agence Canadienne de Coopération Internationale (ACDI) depuis 2006. Il faut aussi mentionner que dans le cadre de l'OEA, l'Agence Interaméricaine pour la Coopération et le Développement développe un programme d'administration électronique. Dans le cadre onusien, l'UNPAN, le Réseau des Nations Unies pour l'Administration Publique⁸⁰ donne accès à un éventail des meilleures pratiques mondiales en matière d'administration électronique. Il dispose en particulier d'une intéressante banque de données sur

⁷⁹ WWW.REEDGEALC.NET

⁸⁰ WWW.UNPAN.ORG

l'administration électronique dans les Caraïbes⁸¹. Enfin il faudra toujours garder à l'esprit que la mise en place de l'administration électronique nécessite l'établissement de repères temporels et quantitatifs mesurables, rigoureux et quasiment impératifs.

C.- Etablir un plan ambitieux et intégral

On adoptera pour l'établissement de ce plan le slogan en vigueur dans le monde industriel : « Think big, start small, scale fast ». Penser grand, débiter petit mais grandir vite. Il faut un plan ambitieux qui fasse rêver, un plan intégral qui vise un impact profond et à long terme. Mais, il devra identifier des buts réalisables à court terme et à haut impact dont la réussite contribuera à construire progressivement chez les fonctionnaires et les administrés une coalition pro-changement. Le contenu du plan devra aborder au moins les domaines suivants.

1.- Le développement de contenus

On pense ici au développement des sites web incluant des informations et des téléprocédures. On pense également à la mise en œuvre de nouvelles applications comme la signature électronique.

2.- La formation des ressources humaines

Ce volet devra faire l'objet d'un effort sérieux et soutenu. Il visera en priorité les agents publics. Les organismes internationaux mentionnés plus haut offrent tous des modules de formation en administration électronique qui peuvent être dispensés sur place ou qui peuvent être suivis en ligne.

3.- La connectivité

S'assurer d'une connexion internet et intranet de bonne qualité accessible à toutes les entités administratives existantes.

4.- Mesures institutionnelles, législatives et réglementaires

Dans le cadre du Conseil Supérieur de l'Administration et de la Fonction Publique, devra être créée une cellule pluridisciplinaire pour l'administration électronique chargée de la conception, du développement et de la mise en œuvre du projet d'administration électronique. Le responsable de cette cellule devra avoir rang de ministre délégué auprès du Premier Ministre de façon à lui donner l'autorité nécessaire pour l'implantation du projet.

Le cadre juridique doit être mis en place pour rendre possible l'administration électronique. Il est indispensable que soient votées la loi sur les télécommunications, la loi sur la signature électronique, la loi sur le commerce électronique, la loi sur l'administration électronique. Les arrêtés d'application devront suivre immédiatement. Elles sont nécessaires à la mise en place d'un régime concurrentiel dans le secteur des télécommunications, à la validité des documents électroniques, à l'implantation d'entreprises de certification de signature électronique, au déroulement de procédures électroniques et à la gouvernance électronique. Sur ce dernier point, le régime juridique de l'interopérabilité et des communications électroniques entre autorités administratives et gouvernementales aura un impact positif sur l'efficacité de l'administration publique.

81

5.- Des politiques, des projets et l'institutionnalisation de l'administration électronique

Pour un plan sérieux d'administration électronique il est nécessaire de déterminer le contenu de base de politiques sur des thèmes centraux comme la sécurité, la connectivité, la fracture numérique, l'externalisation des services et la protection des données personnelles. Poursuivant le même objectif de sérieux, les principaux projets seront identifiés ainsi que les personnes qui en auront la charge et la responsabilité.

6.- L'internet pour tous

Il est nécessaire que soit élaborée et poursuivie une politique visant l'accès à l'internet pour tous en vue de la concrétisation de l'administration électronique. Les mesures tendant à la baisse du coût de l'internet, les actions se donnant comme objectif la dissémination territoriale des points d'accès électroniques dans les lieux publics devront être pris en compte dans l'élaboration de cette politique.

7.- Le financement

Le budget pour la mise en œuvre de l'administration électronique sera élaboré de la manière la plus complète possible, en estimant de manière réaliste la disponibilité des fonds publics d'origine locale et internationale qui y seront alloués. Il prendra le soin d'identifier des sources de financement alternatif.

D.- Découvrir, soutenir et former des leaders en administration électronique

L'existence de ces leaders à l'intérieur même des entités administratives est fondamentale. Ils constitueront le bataillon de choc, et le moteur de la réforme au sein de leurs administrations respectives. D'où la nécessité de les découvrir, de les soutenir et de les protéger s'ils sont déjà des agents publics, de les attirer s'ils évoluent aujourd'hui en dehors de l'administration publique. Ceci demande un effort de détection et de mise en valeur systématique de ces individus aux niveaux intermédiaires de l'administration publique.

E.- Toujours consulter les clients

L'expression « client du projet d'administration électronique » inclut les agents publics et les administrés. Il faut éviter à tout prix que le projet d'administration électronique devienne l'otage ou la propriété exclusive d'« équipes informatiques autarciques ». La réussite du projet repose sur l'exercice méthodique et périodique de consultations des clients sur la qualité du service, les besoins non encore couverts et les possibilités d'amélioration. On assure ainsi une culture de qualité pour le gouvernement en général et l'administration électronique en particulier.

On peut sous ce rapport s'inspirer de la méthodologie appliquée au Canada qui lui vaut d'être un des leaders mondiaux en matière d'administration électronique. Lisons ce qui ressort de l'étude menée en 2004 par Accenture « *Le leadership en matière de cybergouvernement : haute performance et valeur maximale* »⁸²

⁸² GRAEME GORDON, *BRAVO ! LE CANADA EST ENCORE UN FOIS EN TÊTE DE LISTE !*, WWW.ACCENTURE.COM/COUNTRIES/CANADA_FRENCH/RESEARCH_AND_INSIGHTS/BRAVOLISTE.HTM

« Au cours de la dernière année, l'importance que le Canada a accordée à l'auto-évaluation et ses sondages menés régulièrement auprès des utilisateurs lui ont permis de continuer à mettre au point un programme de services gouvernementaux en ligne axé sur les citoyens, qui est certainement l'un des meilleurs au monde... »

« Le plan d'action du Canada repose sur une base extrêmement solide de faits, c'est-à-dire des informations connues sur ses clients. Le programme du Canada consistant à interroger régulièrement les citoyens et les entreprises pour connaître leurs opinions et leurs besoins semble être le plus complet parmi tous les pays sondés. »

« De plus, le Canada examine minutieusement ses progrès globaux de façon régulière, au moyen d'un ensemble complet d'outils de gestion de la performance. Cette approche lui a permis d'améliorer les services déjà offerts en ligne et de concevoir des nouveaux services véritablement novateurs, qui répondent à la demande ou aux besoins des clients. Par exemple, sur le portail du pays, www.canada.gc.ca, certaines améliorations ont été apportées au site principal et à chacune des passerelles (links) axées sur les clients, qui ont été validées au cours des essais menés auprès de groupes de consultation ».

F.- Communication

Les responsables du projet d'administration électronique devront SANS CESSER consacrer leurs efforts à communiquer et faire passer leur vision auprès des agents de l'administration publique. Il faut que ces derniers soient convaincus de la manière et de l'objectif par lesquels leurs tâches se trouveront facilitées et eux-mêmes seront acteurs et bénéficiaires du changement. Communiquer la philosophie, la portée et les bénéfices de ces projets se traduira par les actions suivantes : expliquer, former, évaluer, obliger, obtenir les réactions, récompenser, stimuler, communiquer et partager les bonnes expériences.

Il résulte de ce qui précède que la mise en place de l'administration électronique et sa réussite sont subordonnées à une politique résolue et constante menée avec vigueur au plus haut niveau en vue d'une réingénierie de l'administration publique. La modification du cadre légal n'en constitue qu'un des aspects aussi nécessaire soit-il.

Section II.- Le projet de loi sur l'administration électronique

Le projet de loi sur l'administration électronique se présente comme le premier volet des actions qui devront à terme voir l'implantation de l'administration électronique. Il s'articule autour de quatre axes qui en expriment la philosophie (#1). Ensuite les grandes lignes du projet de loi seront schématiquement exposées (#2)

#1.- Les grands axes du projet de loi

La législation proposée établit le droit de l'administré à l'utilisation de moyens électroniques dans ses démarches administratives (A), et prend en compte les conséquences de ce droit (B). Il régit l'incorporation des technologies de l'information et de la communication dans la machine administrative (C), tout en adhérant au principe de neutralité technologique (D).

A.- Le droit du citoyen à l'utilisation des moyens électroniques dans ses rapports avec l'administration

Alors que la première exigence de l'administration publique classique réside dans l'obligation implicite faite à l'administré de se déplacer, et de faire la queue, grâce à l'équipement informatique et une bonne connexion internet, une grande partie des procédures administratives pourra s'effectuer à partir du domicile du citoyen. Pour cela le projet de loi consacre le droit du citoyen à utiliser les moyens électroniques dans ses rapports avec l'administration. Ce droit du citoyen s'accompagne d'une obligation complémentaire à la charge des entités administratives de se doter des moyens et systèmes d'information adéquats.

La loi sur l'administration électronique s'attache à répondre à deux grands défis. Le premier est de vaincre la crainte ressentie relativement à la perception de fragilité des informations archivées sur support électronique, à l'érosion de la vie privée, au manque de confidentialité des données à caractère personnel, et à l'opacité des technologies de l'information et de la communication. Le deuxième défi relevé réside dans le souci de préserver les garanties constitutionnelles. Les sources constitutionnelles de cette législation ont été exposées précédemment. Elles sont réaffirmées dans le corps du texte et sont complétées par d'autres dérivant de l'utilisation des moyens électroniques. La défense de ces droits constitutionnels confère une nouvelle légitimité à la mission du Protecteur du Citoyen dont le rôle en ce domaine est précisé et élargi.

B.- Les conséquences juridiques du droit du citoyen à l'utilisation des moyens électroniques

L'utilisation des moyens électroniques par l'administré entraîne des conséquences que la législation proposée s'efforce de prendre en compte.

La première concerne la confidentialité des données personnelles. Celles-ci, lorsqu'elles sont fournies à une entité administrative, ne pourront être utilisées par d'autres sans le consentement exprès de l'intéressé.

La deuxième concerne l'obligation pour les entités administratives de revoir l'ensemble des procédures administratives dans un souci de simplification.

Troisièmement, l'administration électronique oblige à la définition et à l'établissement du régime de nouveaux concepts tels que site électronique et portail de l'administration publique, dossier électronique, documents registres et notifications électroniques, portée des mécanismes horodateurs.

La loi régit en quatrième lieu la problématique de l'archivage des informations et documents électroniques.

Cinquièmement, la loi garantit le droit de l'administré à accéder à tout moment à son dossier.

C.- L'incorporation des technologies de l'information et de la communication dans le fonctionnement interne de l'administration publique

Le principe fondamental en droit administratif de l'égalité d'accès de l'administré aux services publics interdit que l'incorporation de ces technologies ne débouche sur une discrimination entre citoyens basée sur leur possibilité d'accès aux moyens électroniques. La mise en place de l'administration électronique induit donc la coexistence de deux Etats, un Etat-papier et un Etat-

internet⁸³. Ce principe est clairement illustré dans un avis du tribunal administratif français rendu en 1997 qui sanctionne l'utilisation de la télématique comme seule procédure d'inscription dans une université⁸⁴. « *Une telle procédure, opine le Conseil d'Etat, méconnaît le principe d'égalité de traitement entre ces candidats, eu égard aux conditions d'équipement télématique et informatique des intéressés, aux possibilités techniques de connexion et aux différences qui en résultent dans les conditions d'acheminement de leurs appels vers le serveur télématique de l'université* ». L'administration publique est donc obligée d'être une administration à accès pluriel⁸⁵, l'administré conservant le libre choix du moyen utilisé pour entrer en contact avec l'administration.

L'incorporation des technologies de l'information et de la communication dans le fonctionnement interne de l'administration implique l'obligation juridique de mettre en place des programmes de formation à l'intention des fonctionnaires pour qu'ils puissent assister les administrés et leurs fournir les services administratifs. La législation proposée impose également l'établissement de points d'accès électroniques publics dans les lieux publics.

Il devient également indispensable de régir légalement la validité des documents électroniques et de leurs copies, de même que la transformation de documents papiers en documents électroniques.

D.- La neutralité technologique

La loi ne peut se permettre de figer l'utilisation des moyens électroniques en privilégiant une technologie alors que les avancées dans le domaine des communications électroniques évoluent constamment. Le principe de neutralité technologique prôné par toutes les instances en ce domaine est respecté dans le projet de loi. Il permet l'utilisation de toute plateforme permettant une communication électronique ; aujourd'hui il s'agit de l'ordinateur, demain on pourra utiliser les SMS et dans le futur la télévision numérique. En ce sens le projet consacre la liberté de choix par l'administré du canal par lequel il entend communiquer avec l'administration publique.

#2.- Les grandes lignes du projet de loi sur l'administration électronique

Le projet de loi sur l'administration électronique est structuré sur cinq titres précédés d'un titre préliminaire.

A.- Titre préliminaire

Le titre préliminaire présente l'objet et les finalités de la loi. Il expose les principes généraux auxquels est soumise l'administration électronique. Il en précise le champ d'application et procède à la définition des termes et concepts qui y sont employés. Il consacre le principe de l'accès égal des administrés au service public en interdisant toute discrimination contre les moyens non électroniques.

⁸³ GEORGES CHATILLON, OP.CIT.

⁸⁴ CONSEIL D'ÉTAT FRANÇAIS, AVIS DU 15 JANVIER 1997, GOUZIER, JOURNAL OFFICIEL, 5 MARS 1997, P. 3514

⁸⁵ BRUNO LASSERRE, OP. CIT.

B.- Titre I : Les droits des administrés

Dans ce titre, l'obligation est posée pour les entités administratives d'établir différents canaux ou moyens pour la fourniture de services. Le partage de données entre entités administratives est rendu possible moyennant le consentement de l'intéressé ; le consentement pouvant être émis et reçu par des moyens électroniques. Ainsi, l'administré est dispensé d'avoir à produire à nouveau des données et des documents dont l'administration publique dispose déjà. Le rôle du Protecteur du Citoyen et du Conseil Supérieur de l'Administration et de la Fonction Publiques est à ce titre précisé.

C.- Titre II : Le régime juridique de l'administration publique.

Ce titre est lui-même divisé en quatre chapitres.

Le premier chapitre est consacré aux sites électroniques des entités administratives. Ses dispositions concernent l'intégrité, la véracité et l'actualisation nécessaires des informations qui y sont contenues et des services qui y sont offerts. Il légitime les publications effectuées sur le site électronique du « Moniteur ». De même sont rendues possibles les annonces légales de toute sorte effectuées sur les sites électroniques des journaux à grand tirage.

Le deuxième chapitre traite de l'identification et de l'authentification des citoyens et des entités administratives. Il y est prévu le rôle futur d'une carte d'identification nationale comportant la signature électronique de son titulaire. L'Office National d'Identification reçoit à cette fin la mission légale d'étudier les voies et moyens de l'élaboration de ce nouveau type de carte d'identification. Parallèlement, les entités administratives seront obligées légalement d'admettre les certificats électroniques sécurisés émis par les prestataires de services de certification de signature électronique qualifiés. Dans le souci d'éviter la fracture numérique par l'exclusion de l'administration électronique des administrés défavorisés techniquement ou économiquement, les entités administratives devront habiliter certains agents publics à la constatation de l'identité et de la volonté de l'administré. Les mécanismes de délégation de pouvoir et de signature sont également prévus.

Le troisième chapitre est consacré aux registres, aux communications et aux notifications électroniques. Les registres électroniques conservent l'utilisation traditionnelle pour la présentation et la réception de tout écrit ou requête de la part des administrés. Dans le cadre de l'administration électronique ils constituent l'outil de coopération entre entités administratives. Les communications électroniques entre les administrés et l'administration publique, à l'intérieur des entités administratives ou entre entités administratives différentes font également l'objet de ce chapitre qui en établit les critères de sécurité juridique.

Le quatrième chapitre régit les documents et les archives électroniques. Il établit les conditions de validité du document électronique. Il définit le régime des copies électroniques réalisées à partir de documents sur support papier ou de documents électroniques ; il y définit à l'inverse le régime des copies papier réalisées à partir de documents électroniques.

D.- Titre III : La gestion électronique des procédures

Le titre troisième régit les procédures électroniques, leur début, leur instruction et leur clôture. Il établit et régit le droit pour l'administré à être informé à tout moment de l'état de la procédure.

E.- Titre IV : Coopération entre entités administratives

Le rôle éminent du Conseil Supérieur de l'Administration et de la Fonction Publique, organisme rattaché au bureau du Premier Ministre est fixé dans ses compétences d'élaboration et de mise en œuvre de la politique d'administration électronique. Ce titre établit les principes d'interopérabilité des systèmes d'information, de réutilisation des applications et de transferts de technologies entre entités administratives. Ces principes devront être consacrés dans des règlements d'application émis par le Premier Ministre. On y trouve prévu la possibilité légale d'établissement d'un intranet gouvernemental.

F.- Titre V : Dispositions finales

Ce titre débute par les règles régissant la réunion par des moyens électroniques d'organes collégiaux de l'administration publique, comme le cabinet ministériel ou les conseils d'administration d'organismes autonomes. Dans ce titre sont posées les conditions d'élaboration et de publication du plan d'implantation de l'administration électronique. De manière complémentaire est édictée l'obligation d'assortir au plan de mise en œuvre de l'administration électronique des moyens concrets et mesurables de réalisation. De même, le projet de loi pose le principe d'une réalisation graduelle et progressive du plan, grâce à un calendrier et l'établissement d'indicateurs de résultats. Enfin des dispositions relatives au bilinguisme sont imposées aux entités administratives dans le cadre de l'administration électronique.

Conclusion

La mise en place de l'administration électronique apparaît comme un impératif au regard des exigences de transparence, d'efficacité et de responsabilité de l'action administrative. Les engagements internationaux, exprimés particulièrement dans le cadre interaméricain, nous y obligent. Nos voisins de l'hémisphère s'y sont résolument engagés. Les objectifs énumérés et la simple lecture des dispositions du projet de loi indiquent l'ampleur de l'effort à accomplir pour que ce projet devienne réalité. Projet ambitieux, certainement, projet coûteux assurément. Mais un pays ne grandit pas parce qu'il choisit ce qu'il est facile de faire. Un pays fait rêver ses citoyens et les rend fiers par la grandeur des défis qu'il se donne et l'ardeur résolue à en résoudre les difficultés. Si ce projet est coûteux, il demeure à notre portée, des pays de la Caraïbe nous devançant dans cette entreprise et occupent aujourd'hui une place honorable dans le classement de l'ONU cité précédemment. Après la Barbade, 40^e mondial, championne de la région caraïbe, nous trouvons dans l'ordre, Antigua et Barbados, 55^e, les Bahamas, 65^e et Trinidad et Tobago, 67^e. Sur un indice maximum de 1 ces quatre pays dépassent la moyenne mondiale qui est de 0,441⁸⁶. Donc, ce qu'ils ont pu faire, nous le pouvons, nous le devons !

⁸⁶ TRINIDAD ET TOBAGO EST CREDITE D'UN INDICE DE 0,481

TROISIEME PARTIE

**LA SECURITE DES SYSTEMES D'INFORMATION, DES RESEAUX,
DES DONNEES ET DES ECHANGES ELECTRONIQUES**

CHAPITRE 1

LA LUTTE CONTRE LA CYBERCRIMINALITE

Le développement des technologies de l'information a favorisé l'émergence de nouvelles formes de criminalité. Les exploits des pirates informatiques, « hackers », ne se limitent pas aux jeux à peine innocents de jeunes se posant les défis de percer les remparts de sécurité des systèmes d'informations de leurs établissements scolaires ou d'un ministère de la défense. Grâce aux technologies de l'information, les syndicats du crime organisé blanchissent leurs avoirs illicites, les pervers mettent en scène leurs fantasmes pédophiles, des mélomanes indécents téléchargent gratuitement des œuvres de l'esprit. Pour avoir une idée de l'ampleur du problème, « aux Etats-Unis, le Pentagone a enregistré à lui seul, en 2001, plus de 22 000 agressions électroniques contre ses systèmes et le FBI a recensé 5 000 infrastructures "extrêmement vulnérables" à la criminalité informatique capable "de déstabiliser l'économie entière d'un pays", selon Ronald L. Dick, Directeur du Centre de la Protection des Infrastructures Nationales. Le point commun de ces catégories d'infractions est que celles-ci peuvent être commises à grande échelle et que la distance géographique entre le lieu où l'acte délictueux est effectué et ses effets, peut être considérable.

« La fraude et l'escroquerie en ligne prennent de plus en plus d'ampleur. En 2001, des groupes organisés en Ukraine et Russie ont piraté plus de 40 sites américains, détournant les numéros d'au moins un million de cartes de crédit. De Moscou à Tokyo en passant par Lausanne ou Paris, la police spécialisée semble dépassée par cette criminalité galopante qui profite des failles des systèmes informatiques. D'après le Conseil de l'Europe, la fraude sur les cartes de crédit s'élève à quelque 400 millions de dollars par an et les dégâts causés par les attaques de virus à près de 12 milliards de dollars. »⁸⁷

La lutte contre la cybercriminalité constitue désormais un volet important de la politique de sécurité publique tant il est vrai que les menaces peuvent attenter jusqu'à la souveraineté nationale. Les technologies de l'information se présentent donc à la fois comme outil de développement de la cybercriminalité et moyen de lutte contre cette nouvelle forme de délinquance.

Section I.- Définition de la cybercriminalité

Aujourd'hui l'accord n'existe pas sur la définition de la cybercriminalité⁸⁸. Mais si on s'inspire des documents présentés lors du Xe Congrès des Nations Unies sur la Prévention de la Criminalité et

⁸⁷ LA DOCUMENTATION FRANÇAISE, LA CYBERCRIMINALITE, [HTTP://WWW.LADOCUMENTATIONFRANCAISE.FR/DOSSIERS/INTERNET-MONDE/CYBERCRIMINALITE.SHTML](http://www.ladocumentationfrancaise.fr/DOSSIERS/INTERNET-MONDE/CYBERCRIMINALITE.SHTML)

⁸⁸ MOHAMED CHAWKI, LE DROIT PENAL A L'ÉPREUVE DE LA CYBERCRIMINALITE, IN INSTITUT INTERNATIONAL DE DROIT D'EXPRESSION ET D'INSPIRATION FRANÇAISE (IDEF), DROIT ET NOUVELLES TECHNOLOGIES, XXXE CONGRES, 16-18 DECEMBRE 2006, EGYPTE, 30 PAGES

le Traitement des Délinquants tenue à Vienne en l'an 2000 on peut avancer que « *l'infraction informatique est toute infraction commise dans un environnement électronique, infraction se référant à toute conduite généralement définie comme illégale ou susceptible d'être incriminée (tous les Etats ne punissant pas les mêmes actes). Une infraction informatique peut être commise au moyen d'un système ou d'un réseau informatiques, dans un système ou réseau informatiques ou contre un système ou réseau informatiques* ».

Cette définition nous permet de voir que le concept de cybercriminalité englobe à la vérité plusieurs types d'infractions qu'on peut regrouper sous deux catégories⁸⁹.

Une première catégorie, la criminalité informatique, constituée d'agissements appelés à devenir de nouvelles infractions spécifiques. Il s'agit d'une conduite illégale commise au moyen d'opérations électroniques visant la sécurité de systèmes informatiques et des données qui y sont traitées. On y trouve de manière principale le piratage informatique ou l'accès par effraction dans un système d'information, l'utilisation non autorisée de systèmes informatiques, le vandalisme informatique. Y sont incluses de manière secondaire les infractions indirectes préparant la commission d'infractions plus sérieuses comme le transfert de mots de passe, de clés de cryptage, de codes d'accès etc.

La deuxième catégorie recouvre des infractions traditionnelles plus classiques facilitées par les technologies de l'information. Ce sont d'abord des infractions contre les biens ou infractions économiques : la falsification de bilan, le vol sur des comptes bancaires. On trouve ensuite des infractions contre la vie privée : le viol de correspondance, l'accès à des bases de données protégées, la vente d'informations personnelles. En troisième lieu nous trouvons des infractions contre l'honneur comme les menaces ou la diffamation. Enfin il y a des infractions contre les mœurs : l'outrage aux bonnes mœurs comme la pornographie ou l'incitation des mineurs à la débauche comme la pornographie infantile.

Section II.- Les moyens de lutte contre la cybercriminalité

La lutte contre la cybercriminalité doit être multiforme et dynamique. Dynamique car elle devra, si elle se veut efficace évoluer en même temps que voient le jour de nouvelles facettes de cette délinquance. Multiforme en ce qu'elle mettra en œuvre de manière coordonnée l'action législative, la sophistication technique, la formation des personnels concernés et la participation aux mécanismes régionaux et internationaux de lutte. Le Gouvernement et particulièrement le Ministère en charge de la sécurité publique doit être pénétré de ce que la mise en œuvre des trois volets est essentielle à l'efficacité de la lutte et qu'on ne saurait se contenter du vote de quelques lois aussi bien rédigées soient elles.

⁸⁹ HANS CORELL, *DECLARATIONS LIMINAIRES ET CONCLUSIVES*, TABLE RONDE SUR LES DEFIS DE LA CYBERCRIMINALITE SANS FRONTIERES, IN COLLOQUE A L'OCCASION DE LA SIGNATURE DE LA CONVENTION DES NATIONS UNIES CONTRE LA CRIMINALITE TRANSNATIONALE, PALERME, ITALIE, 14 DECEMBRE 2000, 11 PAGES

#1.- L'action législative

L'action législative portera sur la création d'infractions spécifiques et l'adaptation de la procédure pénale et constitue le chantier pour lequel l'Etat devra mandater des juristes spécialisés en ce domaine.

A.- La création d'infractions spécifiques

Les actions qui méritent d'être criminalisées sont celles qui favorisent

- l'accès par infraction à un système informatique,
- l'interférence dans le fonctionnement licite d'un ordinateur ou d'un système informatique,
- la destruction ou l'altération de données dans un système informatique,
- le vol de biens incorporels, comme le téléchargement d'œuvres audio-visuelles,
- l'obtention d'avantages par la tromperie.

B.- La modification d'infractions existantes et de la procédure pénale

Des infractions existantes requerront que dans la définition de leurs éléments constitutifs soient pris en compte les agissements utilisant les technologies de l'information.

Les recommandations en matière d'ajustement de la procédure s'inspirent de celles formulées par le Groupe d'Experts Gouvernementaux sur la Cybercriminalité près la REMJA⁹⁰ lors de sa troisième rencontre en juin 2003.⁹¹ ⁹²Les nouvelles règles de procédure régiront les pouvoirs d'investigation en vue de la collecte et de la garde sûre d'indices et de preuves électroniques en rapport avec n'importe quel délit. Elles assureront l'équilibre entre d'une part l'exercice légitime des pouvoirs d'enquête et d'autre part la régularité procédurale et le respect des droits de la personne et des libertés fondamentales. Elles devront être applicables, compte tenu de la nature souvent transnationale des délits informatiques, dans le cadre de la coopération judiciaire internationale. Elles devront permettre le suivi et l'interception des communications des présumés délinquants à travers les fournisseurs de services de communications électroniques (FAI, téléphonie etc.) afin de déterminer le cours, le contenu, l'origine ou la destination des communications.

C.- Le problème lié à la territorialité du droit pénal

Le droit pénal vise à la préservation de l'ordre public de l'Etat qui le produit. Un Etat, ses lois et ses juridictions, ne peut, sans violer le principe de la souveraineté, légiférer et punir des actes qui se commettent sur le territoire d'un autre Etat⁹³. Or l'infraction informatique revêt souvent un caractère transnational. Par exemple l'accès illicite à un système d'information basé en Haïti, la diffamation dont pâtit une personne domiciliée en Haïti peut se commettre à partir d'un système d'information ou d'un serveur basé à l'étranger. L'agissement punissable ici peut n'être pas prévu et puni par la loi pénale

⁹⁰ REUNION DES MINISTRES DE LA JUSTICE DES AMERIQUES CONVOQUEE ANNUELLEMENT DANS LE CADRE DE L'OEA ET FORMULANT DES POSITIONS EN MATIERE DE JUSTICE ENTERINEES SUBSEQUEMMENT PAR L'ASSEMBLEE GENERALE DE L'OEA.

⁹¹ WWW.OAS.ORG/JURIDICO/SPANISH/RECOMENIII_FR.PDF

⁹² VOIR EGALEMENT PARLEMENT EUROPEEN, LA CRIMINALITE, 2005,

WWW.EUROPARL.EUROPA.EU/COMP/ARL/LIBE/ELSI/200M_IN/30_FR.HTM

⁹³ EXCEPTION FAITE DES CRIMES QUI HEURTENT LA CONSCIENCE UNIVERSELLE COMME LES ACTES DE TERRORISME CONTRE LESQUELS DES TRAITES INTERNATIONAUX PERMETTENT AUX TRIBUNAUX D'UN ETAT PARTIE DE JUGER LES CRIMES COMMIS DANS UN AUTRE ETAT.

étrangère. Les éléments constitutifs de l'infraction étant localisés à l'extérieur rendent incompétents la loi et les tribunaux répressifs haïtiens. Ce constat est frustrant lorsque les effets de l'acte malveillant se font sentir en Haïti, surtout s'ils s'y font sentir intentionnellement.

Une première réponse à cette frustration se trouve aux articles 5 et 6 du vénérable code d'instruction criminelle de 1835 toujours en vigueur qui rend compétent le droit pénal et les tribunaux répressifs haïtiens lorsqu'« *un crime attentatoire à la sûreté de l'Etat* » est commis « *hors du territoire d'Haïti* » par un Haïtien ou un étranger qu'on aura arrêté en Haïti ou dont le gouvernement aura obtenu l'extradition⁹⁴. Ces articles pourront donc être appliqués toutes les fois où les infractions informatiques qui seront définies sont de celles qui menacent la sécurité de l'Etat.

Pour les autres types d'infractions informatiques la frustration demeure, surtout lorsque sont menacés l'honneur et la réputation des individus ou l'intégrité morale des enfants. La législation à venir devrait, en modifiant les articles 5 et 6 C.I.C étendre le champ d'application territorial du droit pénal haïtien pour des infractions informatiques limitativement identifiées commises à l'étranger mais dont les effets se font sentir en Haïti.

D.- S'inscrire dans le cadre des efforts régionaux

Les Etats américains ont élaboré une Stratégie Interaméricaine Intégrée pour Combattre les Menaces à la Cybersécurité⁹⁵. Il est essentiel que la législation sur la cybercriminalité s'inscrive dans le cadre de cette stratégie. De manière plus générale, les rédacteurs de cette législation devront impérativement prendre connaissance des diverses résolutions de l'Assemblée Générale de l'OEA⁹⁶ et des recommandations du Groupe d'Experts Gouvernementaux sur la question⁹⁷. L'un des points essentiels étant que la législation sur la cybercriminalité applique les principes contenus dans la Convention du Conseil de l'Europe sur la Cybercriminalité.

#2 La sophistication technique

L'Etat devra concevoir et mettre en œuvre un politique de sécurité des réseaux et de l'information. Les entités administratives et les institutions du secteur privé devront se doter de logiciels et de mécanismes dissuadant l'accès illicite à leurs systèmes ou réseaux d'information. Ces mécanismes devront être à même de déceler tout acte de malveillance et faire entrer les systèmes ou réseaux dans un mode sûr de fonctionnement.

Les autorités de poursuite seront dotées du matériel et des logiciels informatiques permettant la collecte d'indices et de preuves électroniques des infractions, la détermination du contenu, de l'origine et de la destination des communications électroniques.

⁹⁴ ART. 5 C. INST. CRIM. : « *TOUT HAÏTIEN QUI SE SERA RENDU COUPABLE, HORS DU TERRITOIRE D'HAÏTI, D'UN CRIME ATTENTATOIRE A LA SURETE DE L'ETAT, DE CONTREFAÇON DES MONNAIES NATIONALES AYANT COURS, DE PAPIERS NATIONAUX, DE BILLETS DE BANQUE AUTORISES PAR LA LOI, SERA, AUSSITOT QU'IL SERA SAISI, POURSUIVI, JUGE ET PUNI EN HAÏTI, D'APRES LES DISPOSITIONS DES LOIS HAÏTIENNES.* »

ART. 6 C. INST. CRIM. : « *CETTE DISPOSITION SERA ETENDUE AUX ETRANGERS QUI, AUTEURS OU COMPLICES DES MEMES CRIMES, SERAIENT ARRETES EN HAÏTI, OU DONT LE GOUVERNEMENT OBTIENDRAIT L'EXTRADITION.* »

⁹⁵ AG/RES. 2040 (XXXIV-O/04)

⁹⁶ WWW.OAS.ORG/JURIDICO/ENGLISH/CYBER_DOCS.HTM

⁹⁷ WWW.OAS.ORG/JURIDICO/ENGLISH/CYBER_EXPERTS.HTM

#3 La formation des ressources humaines

Un effort sérieux devra être entrepris pour doter l'Etat des ressources humaines compétentes sur lesquelles s'appuiera effectivement la lutte contre la cybercriminalité. Un service spécialisé à cet effet sera créé au sein de la Direction Centrale de la Police Judiciaire de la police Nationale doté d'inspecteurs et coiffé par un commissaire familiarisés avec les méthodes d'investigation des infractions informatiques. Au niveau des parquets et des cabinets d'instruction des magistrats seront identifiés et, le cas échéant nommés, qui recevront une spécialisation en vue de la constitution des dossiers devant être portés devant les juridictions répressives.

Ces efforts seront pilotés par une cellule à installer au Ministère chargé de la sécurité publique. Ce ministère mettra sur pied un Groupe D'Alerte, de Surveillance et d'Avertissement ou Equipe de Réponse aux Incidents Relatifs à la Sécurité Informatique⁹⁸.

#4 La participation aux mécanismes régionaux et internationaux de lutte

Dans le cadre de la Stratégie Interaméricaine Intégrée pour Combattre les Menaces contre la Cybersécurité définie par l'OEA, ont été mis en place ou prônés des mécanismes de coopération régionale ou internationale et d'échanges d'information. En effet, face à une criminalité de nature transnationale, il faut une réponse globale de façon à éliminer les « havres cybernétiques » à l'abri desquels les délinquants pourraient opérer en toute impunité.

Haïti devra mettre à profit les programmes de formation à l'intention des enquêteurs et des magistrats du continent offerts par le Gouvernement des Etats-Unis d'Amérique.

Il est recommandé, une fois la législation mise en vigueur, qu'Haïti participe aux réunions techniques du Groupe d'Experts Gouvernementaux en matière de Cybercriminalité, constitué dans le cadre de l'OEA, de manière à être tenue au courant, et que soient disséminées auprès des autorités gouvernementales, policières et judiciaires les dernières avancées dans le domaine.

Il deviendra essentiel qu'Haïti adhère au Réseau d'Urgence 24/7⁹⁹ mis sur pied par le G-8 dans le but d'aider à effectuer des enquêtes sur les délits informatiques. Les alertes en cas de survenance d'infractions informatiques peuvent être relayées sitôt qu'elles sont sues, et les mesures conservatoires pour la collecte et la sauvegarde rapides des indices et des preuves prises immédiatement. Dans le même ordre d'idées, il sera important d'intégrer le réseau interaméricain des CSIRT's établi sous l'égide du CICTE¹⁰⁰ et abrité dans le serveur sécurisé de l'OEA. Le CICTE pourra nous assister dans la mise sur pied de l'Equipe de Réponse locale.

⁹⁸ DESIGNÉ AU NIVEAU INTERNATIONAL SOUS SON SIGLE ANGLAIS CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM)

⁹⁹ 24 HEURES PAR JOUR/7 JOURS PAR SEMAINE

¹⁰⁰ COMITÉ INTERAMÉRICAIN CONTRE LE TERRORISME

CHAPITRE 2

LA PROPRIETE INTELLECTUELLE DANS L'ENVIRONNEMENT NUMERIQUE

En passant en revue le droit haïtien à travers le prisme de l'environnement numérique, nous ne pouvons nous garder de poser la problématique de la propriété intellectuelle sur les œuvres numériques. En poursuivant la réflexion nous pensons qu'il serait également opportun de réfléchir à la protection par des moyens électroniques de la propriété intellectuelle. En parlant de propriété intellectuelle nous nous référons plus explicitement à la propriété littéraire et artistique. Si les questions sont légitimes, les réponses, comparativement aux autres domaines abordés dans ce rapport, sont surprenantes. En effet, d'une part, l'examen du droit positif en vigueur nous apprend que la législation accorde sa protection aux œuvres numériques (section I). D'autre part, les développements consacrés à l'administration électronique s'appliquent tout naturellement à la protection de la propriété intellectuelle par des moyens électroniques (section II).

Section I.- La protection des œuvres numériques par la législation sur les droits d'auteur

La fin du XXe et le début du XXIe siècle ont vu l'éclosion de productions de l'esprit immatérielles. On connaissait déjà les discours, les conférences ou les émissions radiophoniques conservées sur des bandes magnétiques. Nous découvrons aujourd'hui des œuvres musicales ou des œuvres littéraires, des cours diffusés sur internet, des logiciels ou programmes d'ordinateurs, des bases de données numériques. Qui sait ce que nous réserve demain l'imagination de nos enfants ? Œuvres de l'esprit, elles méritent d'être protégées contre le vol, le plagiat, la contrefaçon. Longtemps figée, la législation haïtienne a suivi le cours de la modernité par la promulgation du Décret du 12 octobre 2005 sur les Droits d'Auteur¹⁰¹. La propriété littéraire ou artistique est garantie et s'étend à toute œuvre de l'esprit. « Cette protection, y lit-on, est indépendante du mode ou de la forme d'expression et de toute formalité administrative ». La protection de la loi s'étend à toute œuvre qu'elle soit produite par écrit, qu'elle soit diffusée par des moyens audiovisuels, par internet ; qu'il s'agisse d'œuvres traditionnelles, d'œuvres multimédia, de programmes d'ordinateurs ou de bases de données numériques. Un autre décret paru le même jour régit le Bureau Haïtien du Droit d'Auteur¹⁰². Cet organisme public est l'organe de gestion collective et de protection des droits d'auteurs en Haïti. Tout auteur d'œuvre de l'esprit a vocation à devenir membre du BHDA. Les membres sont répartis en six sections dont une réservée aux auteurs d'œuvres multimédia. Pour adhérer à la section littéraire ou à la section musicale la publication de l'œuvre sur internet constitue une des conditions d'admission.¹⁰³

¹⁰¹ LE MONITEUR NO. 23, 9 MARS 2006

¹⁰² DECRET DU 12 OCTOBRE 2005 SUR LE BUREAU HAÏTIEN DU DROIT D'AUTEUR. LE MONITEUR NO. 21, 2 MARS 2006

¹⁰³ ART. 18 IBID.

Section II.- La protection par des moyens électroniques de la propriété intellectuelle

La protection effective de l'œuvre intellectuelle est soumise à une procédure obligatoire de déclaration. Cette déclaration s'effectue par le dépôt au BHDA d'un bulletin de déclaration accompagné d'un exemplaire de l'œuvre complète ou de la bande, feuille magnétique ou support numérique contenant l'œuvre¹⁰⁴. Les dispositions du Décret du 12 octobre 2005 sur le Bureau Haïtien du Droit d'Auteur définissent la forme du bulletin de déclaration en tenant compte des œuvres présentées sous une autre forme que l'écrit¹⁰⁵. Enfin le BHDA devra tenir un répertoire périodiquement mis à jour des œuvres enregistrées et protégées.

Toutefois la procédure simplement résumée ici est encore fidèle à la conception de l'Etat-papier, dont la catastrophe du 12 janvier 2010 nous a montré les limites. Avec la mise en place de l'administration électronique et l'adoption de la législation proposée pour la régir, la protection des droits d'auteurs poursuivra sa modernisation. Ainsi le BHDA pourra, en application de la loi sur l'administration électronique mettre en ligne des formulaires de bulletins de déclaration pour les œuvres qui ne se présentent pas sous forme de livres. De même, le répertoire du BHDA sera disponible et consultable en ligne et aura la même valeur probante que le répertoire physique.

¹⁰⁴ ART. 41 IBID.

¹⁰⁵ ART. 43 IBID.

CONCLUSION

Tout le long de ces lignes nous avons préconisé les moyens pour notre pays de s'arrimer au train de la modernité par l'adoption des textes normatifs et l'impulsion d'une action administrative orientée vers l'efficacité. Nous rappelons ici les implications institutionnelles induites par ces développements.

Les échanges électroniques dans les relations de droit privé et même entre administrés et administration publique vont entraîner l'introduction de métiers de la confiance chargés d'identifier les parties de manière sûre par l'établissement de signatures électroniques. Le CONATEL sera responsable de la qualification et du contrôle des prestataires de services de certification électronique.

Pour la prévention et la répression de la cybercriminalité le Ministère de la Justice devra élaborer la législation sur la cybercriminalité et renforcer la structure institutionnelle de la Secrétairerie d'Etat chargée de la Sécurité Publique, par la création du Groupe D'Alerte, de Surveillance et d'Avertissement ou Equipe de Réponse aux Incidents Relatifs à la Sécurité Informatique en liaison avec ses homologues interaméricains ou internationaux. De même une section dédiée à ce type de délinquance devra être instituée au sein de la Direction Centrale de la Police Judiciaire de la PNH. Les parquets et juges d'instruction devront également recevoir une formation spécifique en ce sens.

Les technologies de l'information multiplient de manière exponentielle les risques d'atteinte à la vie privée par la divulgation indue de données à caractère personnel à l'insu ou à l'encontre de la volonté de leurs titulaires. Il devint dès lors indispensable que soit créée une autorité dotée de pouvoirs de police afin de garantir la protection des données personnelles recueillies tant par des personnes privées que par l'administration publiques. Les moyens légaux, techniques et humains accordés à cette autorité seront le garant de la confiance que les citoyens accorderont à l'économie numérique et à l'administration électronique.

Nous croyons fermement qu'à ce tournant de notre histoire l'adoption des mesures et des normes présentées dans ce rapport permettra à notre pays d'entrer dans le XXIe siècle avec un arsenal juridique moderne lui permettant de relever le défi du développement et de faire face à armes égales à la concurrence de nos voisins pour l'attraction de l'investissement autochtone et étranger. L'administration ainsi renouvelée redonnera son véritable sens à l'expression « service public », renforçant par là-même la transparence et la responsabilité des gouvernants et la démocratie.

Enfin, le grand chantier de la modernisation de l'Etat par l'institutionnalisation de l'administration électronique devra être coordonné et géré par un responsable placé auprès du premier ministre doté de compétences et d'autorité ministérielles. Un simple secrétaire d'Etat ne jouira pas de l'autorité nécessaire pour faire appliquer les mesures nécessaires au sein de l'ensemble de l'administration publique et des organismes autonomes. On pourrait aller jusqu'à souhaiter que ce ministre délégué auprès du Premier Ministre soit le responsable et le chef d'orchestre de l'introduction des technologies de l'information et de la communication dans tous les domaines de la vie nationale, au niveau privé, administratif et éducatif.

Nul doute que les nouvelles règles du jeu ainsi définies libéreront les initiatives et les énergies créatrices pour le développement de nouveaux métiers où l'ingénuité de nos jeunes générations trouvera à s'investir, à s'enrichir et à transformer le visage d'une Haïti enfin fière !

ANNEXES

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

**ANNEXE 1 :
AVANT PROJET DE LOI SUR LA SIGNATURE
ELECTRONIQUE ADAPTANT LE DROIT DE LA PREUVE
AUX TECHNOLOGIES DE L'INFORMATION ET
ELARGISSANT LES COMPETENCES DU CONSEIL
NATIONAL DES TELECOMMUNICATIONS**

AVANT PROJET DE LOI

SUR LA SIGNATURE ELECTRONIQUE,

ADAPTANT LE DROIT DE LA PREUVE AUX TECHNOLOGIES DE L'INFORMATION ET

ELARGISSANT LES COMPETENCES

DU CONSEIL NATIONAL DES TELECOMMUNICATIONS

Le Pouvoir Exécutif

Vu les articles 111, 111-1, 119, 121, 125, 126, 159 de la Constitution;

Vu les articles 1100, 1101, 1102, 1111 du Code Civil ;

Vu les articles 933 et suivants et les articles 1168 et suivants du Code Civil ;

Vu l'article 30 du décret du 27 novembre 1969 sur le notariat ;

Vu le décret du 12 octobre 1977 sur les Télécommunications ;

Vu le décret du 10 juin 1987 organisant le Conseil National des Télécommunications

Considérant qu'il y a lieu d'harmoniser le droit de la preuve et l'évolution technologique ;

Considérant que les moyens électroniques sont de plus en plus utilisés dans le cadre des échanges et de la création d'obligations ; et que les opérations commerciales recourent de plus en plus souvent à l'échange de données informatisées et à d'autres moyens de communication, qualifiés généralement de « commerce électronique », qui supposent l'utilisation de moyens autres que les documents papier pour communiquer et conserver l'information ;

Considérant que les communications et le commerce électronique nécessitent des «signatures électroniques» et des services connexes permettant d'authentifier les données; que l'établissement d'un cadre légal contribuera à favoriser l'acceptation générale des actes électroniques ;

Qu'il y a lieu d'adapter la législation aux réalités actuelles;

Sur le rapport des Ministres de la Justice, de l'Economie et des Finances, du Commerce et de l'Industrie, des Travaux Publics, Transports et Communications et après délibération en Conseil des Ministres ;

A Proposé

Et le Pouvoir Législatif

A Voté la Loi Suivante :

CHAPITRE I : DE LA PREUVE ET DE LA SIGNATURE ELECTRONIQUE

Article 1^{er}.- L'article 1101 du Code Civil se lira désormais comme suit:

« Article 1101: Les règles qui concernent la preuve littérale, la preuve testimoniale, les présomptions, l'aveu de la partie et le serment, sont expliquées dans les sections suivantes.

« La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dument identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

« Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.

« L'écrit sur support électronique a la même force probante que l'écrit sur support papier.

« La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par arrêté présidentiel.

« Les règlements mentionnés au paragraphe précédent ne s'appliquent pas aux signatures électroniques utilisées exclusivement à l'intérieur de systèmes résultant d'accords volontaires de droit privé entre un nombre défini de participants. Il est reconnu aux parties la liberté de convenir entre elles des modalités et conditions dans lesquelles elles acceptent les données

signées électroniquement. La loi reconnaît l'efficacité juridique des signatures électroniques utilisées dans de tels systèmes et leur recevabilité comme preuves en justice. »

Article 2.- L'article 1102 du Code Civil se lira désormais comme suit :

« Article 1102.- L'acte authentique est celui qui a été reçu par un officier public ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises.

« Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par arrêté présidentiel. »

Article 3.- L'article 1111 du Code Civil se lira désormais comme suit :

« Article 1111.- Le billet ou la promesse sous seing privé, par lequel une partie s'engage envers l'autre à lui payer une somme d'argent ou une chose appréciable, doit être écrit en entier par celui qui le souscrit ; ou du moins, il faut qu'outre sa signature, il ait écrit par lui-même un « bon » ou un « approuvé », portant en toutes lettres la somme ou la quantité de la chose.

« Excepté dans le cas où l'acte émane de marchands, artisans, cultivateurs, gens de journée et de service. »

Article 4.- L'article 1112 du Code Civil se lira désormais comme suit :

« Article 1112.- Lorsque la somme exprimée au corps de l'acte est différente de celle exprimée au bon, l'obligation est présumée n'être que la somme moindre, lors même que l'acte ainsi que le bon sont écrits en entier par celui qui s'est obligé, à moins qu'il ne soit prouvé de quel côté est l'erreur. »

Article 5.- Le premier paragraphe de l'article 30 du Décret du 27 novembre 1969 sur le notariat se lira désormais comme suit :

« Article 30.- Les actes des notaires seront, sous la responsabilité de ces officiers publics, écrits à l'encre, manuellement ou mécaniquement, sur papier timbre ou visé pour timbre en un seul et même contexte, lisiblement, sans blanc, abréviation, lacune ou intervalle. »

CHAPITRE II : DES PRESTATAIRES DE SERVICES DE CERTIFICATION ELECTRONIQUE

Article 6.- Les personnes physiques ou morales, de droit public ou de droit privé, haïtiennes ou étrangères, pourront, sur requête, être qualifiées par le Conseil National des Télécommunications (CONATEL) à fournir des services de certification électronique. Elles devront satisfaire aux exigences établies dans les arrêtés d'application tout en respectant les conditions suivantes :

1. Démontrer la capacité financière suffisante pour fournir les services de certification électronique ;
2. Démontrer la capacité technique pour la création de signature électroniques, l'émission de certificats y afférant et la conservation de messages de données ;
3. Les personnes physiques et les administrateurs des personnes morales ne devront jamais avoir été condamnées à une peine privative de liberté, ni n'avoir été suspendues ou radiées de l'exercice de leur profession pour faute éthique grave. Cette disqualification demeurera en vigueur durant la validité de la sanction pénale, administrative ou disciplinaire.
4. La valeur juridique des certificats de signature électronique délivrés par des prestataires de services de certification électronique établis dans un pays étranger est conditionnée au respect des conditions établies par arrêté présidentiel.

Article 7.- Les prestataires de service de certification électronique qualifiés par le Conseil National des Télécommunications (CONATEL) pourront offrir les services suivants :

1. Délivrer les certificats de signature électroniques pour des personnes physiques ou morales
2. Offrir les services de création de signature électronique sécurisée.
3. Offrir les services d'enregistrement et d'impression dans l'ordre chronologique de la transmission et de la réception de données.

Le Conseil National des Télécommunications (CONATEL) peut par voie réglementaire modifier la liste.

Article 8.- Par l'effet de la présente loi, le pouvoir d'inspection reconnu au Conseil National des Télécommunications (CONATEL) par le Décret du 12 octobre 1977 sur les Télécommunications et celui du 10 juin 1987 organisant ledit Conseil s'exercera également à l'endroit des prestataires de service de certification électronique. En cas de modification du régime des télécommunications, le pouvoir d'inspection du CONATEL défini ici continuera à s'appliquer selon les procédures définies par la nouvelle loi.

Article 9.- Tout prestataire de services de certification électronique qualifié affichera au local du CONATEL durant le premier trimestre de chaque exercice fiscal une attestation de pratique contenant les informations suivantes :

1. Le nom, l'adresse et le numéro de téléphone du prestataire ;
2. La clé publique actuelle du prestataire ;
3. Le résultat de la plus récente inspection effectuée par le CONATEL ;
4. La suspension ou la révocation de la qualification du prestataire ainsi que leurs dates. Dans ces cas, est réputée suspendue ou éliminée la clé publique du prestataire ;
5. Les limites de l'attestation de qualification du prestataire ;
6. Toute autre information requise par le CONATEL.

Ces informations seront publiées sur le site internet du CONATEL.

Article 10.- La rémunération des services fournis par les prestataires de service de certification électronique sera fixée librement par eux.

Article 11.- Les prestataires de services de certification électronique devront :

1. Délivrer les certificats électroniques conformément à ce qui est convenu avec les titulaires des certificats ;
2. Mettre en place les systèmes de sécurité visant à garantir la création et la délivrance de signatures électroniques ;
3. Garantir la protection, la confidentialité et traitement responsable de l'information soumise par le titulaire du certificat ;
4. Garantir la permanence du service de certification électronique ;
5. Répondre diligemment aux requêtes et réclamations formulées par les titulaires de certificats ;
6. Procéder aux publications requises par la présente loi et ses règlements d'application ;
7. Fournir les renseignements requis par les autorités administratives ou judiciaires compétentes relatifs aux signatures électroniques et certificats délivrés et, en général, à tout message de données dont ils ont la garde et l'administration ;
8. Mettre à jour les dispositifs de création de signatures électronique, d'émission de certificat électronique, de conservation et d'archivage des documents prenant la forme de messages de données informatisées ; les éléments techniques relatifs à la fourniture de tout autre service autorisé, selon les règlements nécessaires à la protection des destinataires de leurs services ;
9. Collaborer aux missions d'inspection réalisées par le Conseil National des Télécommunications.

Article 12.- A moins que les parties n'en conviennent autrement, un prestataire de services de certification électronique pourra résilier le contrat qui le lie à un titulaire de certificat après un préavis qui ne peut être inférieur à quatre-vingt-dix jours. A l'expiration de ce délai, les certificats émis seront révoqués. Sauf convention contraire, le titulaire d'un certificat électronique pourra, dans le même délai, résilier le contrat qui le lie au prestataire de services de certification.

Article 13.- Sauf convention contraire des parties, la responsabilité contractuelle, délictuelle ou quasi-délictuelle d'un prestataire de services de certification électronique est régie par les dispositions pertinentes du code civil.

Article 14.- Les prestataires de service de certification électronique qui désirent mettre fin à leurs activités devront notifier leur décision au Conseil National des Télécommunications au plus tard quatre-vingt-dix jours avant la fin prévue de leurs activités. Le CONATEL s'assurera de la mise en œuvre de toutes mesures adéquates pour la protection des titulaires de certificats. Les prestataires de service et leurs administrateurs demeurent tenus postérieurement à la cessation des activités aux obligations de protection, de confidentialité et de traitement responsable des informations fournies par les titulaires de certificats.

CHAPITRE III : DU CONSEIL NATIONAL DES TELECOMMUNICATIONS

Article 15.- Le Conseil National des Télécommunications (CONATEL) exercera les compétences suivantes en plus de celles que lui reconnaissent sa loi organique et la législation sur les télécommunications :

1. Attester de la qualification des prestataires de services de certification électronique ;

2. Superviser le fonctionnement desdits prestataires ;
3. Effectuer les inspections et audits prévus par la présente loi et les règlements d'application ;
4. Suspendre ou révoquer la qualification des prestataires de services de certification électronique contrevenant aux exigences légales, réglementaires et techniques ;
5. Instruire et sanctionner les violations de ces exigences, ou ordonner les mesures de redressement ;
6. Publier sur son site internet ou sur tout réseau public de transmission de données, de manière permanente et ininterrompue, les domiciles, sièges sociaux, numéros de téléphone, adresses internet, date d'expiration de la qualification, certificats électroniques contenant les clés publiques des prestataires de services de certification électronique qualifiés, et des prestataires de services dont la qualification est suspendue ou révoquée ;
7. Fixer le montant des droits et coûts applicables aux prestataires de service de certification électronique ;
8. Veiller au respect de la confidentialité, par les prestataires de services de certification électronique, des informations relatives aux titulaires de certificats électroniques ;
9. Superviser l'exécution du plan de cessation d'activités des prestataires de services de certification électronique ;
10. Contrôler l'application des recommandations formulées lors des visites d'inspection et des audits ;
11. Recevoir les plaintes et les réclamations des titulaires et des usagers des certificats électroniques relativement à la qualité du service offert ;
12. Fixer le montant et recevoir des prestataires de services de certification électronique les droits de traitement de dossier et les droits de supervision.

Article 15.- Un arrêté présidentiel déterminera les critères à respecter pour l'admission en justice du document électronique, réglera le fonctionnement et la responsabilité des prestataires de services de certification de signatures électroniques, ainsi que l'admissibilité des certificats électroniques délivrés par des prestataires de services de certification électronique établis hors d'Haïti.

Article 16.- La présente loi abroge toutes lois ou dispositions de lois, tous décrets ou dispositions de décrets, tous décrets-lois ou dispositions de décrets-lois qui lui sont contraires et sera exécutée à la diligence des Ministres de l'Economie et des Finances, du Commerce et de l'Industrie, et de la Justice, chacun en ce qui le concerne.

Fait à la Chambre des Députés le...

Fait au Sénat le

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

**ANNEXE 2 :
PROJET D'ARRETE PRIS POUR L'APPLICATION DE LA
LOI SUR LA SIGNATURE ELECTRONIQUE ADAPTANT LE
DROIT DE LA PREUVE AUX TECHNOLOGIES DE
L'INFORMATION ET ELARGISSANT LES COMPETENCES
DU CONSEIL NATIONAL DES TELECOMMUNICATIONS**

**PROJET D'ARRETE
PRIS POUR L'APPLICATION DE LA LOI
SUR LA SIGNATURE ELECTRONIQUE
ADAPTANT LE DROIT DE LA PREUVE AUX TECHONLOGIES DE L'INFORMATION ET
ELARGISSANT LES COMPETENCES
DU CONSEIL NATIONAL DES TELECOMMUNICATIONS**

René Préval
Président de la République

Vu le code civil, notamment les articles 1100, 1101, 1102 et 1111 ;

Vu le décret du 12 octobre 1977 sur les télécommunications ;

Vu le décret du 10 juin 1987 organisant le Conseil National des Télécommunications ;

Vu la loi du 2010 sur la signature électronique ;

Considérant la part croissante des échanges numériques dans le commerce mondial ;

Considérant qu'il convient de modifier l'environnement légal en vue de sécuriser les rapports entre les opérateurs économiques en assurant la force probante aux échanges de données informatisées ;

Considérant qu'il convient de créer un cadre légal propice à l'éclosion d'une véritable économie numérique permettant la production de biens et services numériques ;

Considérant qu'il convient de réglementer le fonctionnement et la responsabilité des prestataires de certification de signatures électroniques, ainsi que l'admissibilité des certificats électroniques délivrés par des prestataires de services de certification électronique établis hors d'Haïti ;

Sur le rapport du Ministre de la Justice et de la Sécurité Publique, du Ministre du Commerce et de l'Industrie, du Ministre de l'Economie et des Finances et du Ministre des Travaux Publics, Transports et Communication ;

Arrête

CHAPITRE I : DEFINITIONS

Article 1.- Aux termes du présent arrêté on entend par

1. Signature électronique ; une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à l'article 1101 du code civil ;
2. Signature électronique sécurisée : une signature électronique qui satisfait, en outre, aux exigences suivantes :
 - Etre propre au signataire ;
 - Etre créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
 - Garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable
3. Signataire ; toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de signature électronique ;
4. Données de création de signature électronique ; les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;
5. Dispositif de création de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;
6. Dispositif sécurisé de création de signature électronique : un dispositif de création de signature électronique qui satisfait aux exigences définies à l'article 4;
7. Données de vérification de signature électronique : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;
8. Dispositif de vérification de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique ;
9. Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;
10. Certificat électronique qualifié : un certificat électronique répondant aux exigences définies à l'article 6;
11. Prestataire de services de certification électronique : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;
12. Qualification des prestataires de services de certification électronique : l'acte par lequel le CONATEL atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité.

Article 2.- La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

CHAPITRE II : DES DISPOSITIFS SECURISES DE CREATION DE SIGNATURE ELECTRONIQUE

Article 3.- Un dispositif de création de signature électronique est réputé sécurisé s'il satisfait aux exigences de l'article suivant et s'il est certifié conforme à ces exigences par le Conseil National des Télécommunications.

Article 4.- Un dispositif sécurisé de création de signature électronique doit :

1. Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :
 - a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;
 - b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
 - c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers ;
2. N'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

CHAPITRE III : DES DISPOSITIFS DE VERIFICATION DE SIGNATURE ELECTRONIQUE

Article 5.- Un dispositif de vérification de signature électronique peut faire l'objet d'une certification, s'il répond aux exigences suivantes :

1. Les données de vérification de signature électronique utilisées doivent être celles qui ont été portées à la connaissance de la personne qui met en œuvre le dispositif et qui est dénommée vérificateur ;
2. Les conditions de vérification de la signature électronique doivent permettre de garantir l'exactitude de celle-ci et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;
3. Le vérificateur doit pouvoir, si nécessaire, déterminer avec certitude le contenu des données signées ;
4. Les conditions et la durée de validité du certificat électronique utilisé lors de la vérification de la signature électronique doivent être vérifiées et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;
5. L'identité du signataire doit sans subir d'altération être portée à la connaissance du vérificateur ;
6. Lorsqu'il est fait usage d'un pseudonyme, son utilisation doit être clairement portée à la connaissance du vérificateur ;
7. Toute modification ayant une incidence sur les conditions de vérification de la signature électronique doit pouvoir être détectée.

CHAPITRE IV : DES CERTIFICATS ELECTRONIQUES QUALIFIES

Article 6.- Un certificat électronique est réputé qualifié quand il est délivré par un prestataire de services de certification électronique qualifié et qu'il comporte :

1. Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;
2. L'identité du prestataire de services de certification électronique ainsi que l'Etat où il est établi ;
3. Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;
4. Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;
5. Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;
6. L'indication du début et de la fin de la période de validité du certificat électronique ;
7. Le code d'identité du certificat électronique ;

8. La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;
9. Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

Article 7.- Un prestataire de services de certification électronique pourra suspendre la validité d'un certificat électronique dans l'un ou l'autre des cas suivants :

1. La requête du signataire ;
2. Le déclenchement d'une procédure d'absence, de disparition ou de mise sous tutelle concernant le signataire ;
3. La décision du prestataire de services de certification électronique pour des raisons techniques ; avis en étant donné par tous moyens dans les vingt-quatre heures au signataire et au CONATEL ;
4. Exécution de toute décision judiciaire ayant acquis l'autorité de la chose définitivement et souverainement jugée.

La suspension de la validité d'un certificat électronique en empêche l'utilisation par le signataire dès la notification au prestataire de services de certification électronique de la circonstance qui la déclenche. La suspension prend fin :

1. Par décision du prestataire de services de certification électronique de révoquer le certificat ;
2. Par la décision du prestataire de services de certification électronique de lever la suspension une fois disparues les raisons techniques qui l'avaient motivée ;
3. Par décision du signataire lorsque la suspension était due à son initiative ;
4. Par exécution d'une décision judiciaire définitive déclarant l'absence, la disparition ou la mise sous tutelle du signataire, et entraînant la révocation du certificat.

Article 8.- Un prestataire de services de certification électronique pourra révoquer le certificat dans l'un ou l'autre des cas suivants :

1. La requête du signataire ;
2. La requête d'un représentant légal du signataire, sur présentation des pièces prouvant sa qualité ;
3. L'établissement du certificat électronique sur la base de données ou de renseignements reconnus faux ;
4. Le résultat d'un audit déterminant le caractère peu fiable des procédures d'établissement et/ou de vérification
5. Une décision judiciaire ou administrative motivée, rendue par un tribunal ou une autorité administrative compétents ;
6. Le décès, la disparition, la mise sous tutelle ou la dissolution du titulaire du certificat ;
7. La cessation de la relation contractuelle ou de représentant liant le signataire à la personne morale au nom de laquelle il détient le certificat ;
8. La cessation des activités du prestataire de services de certification électronique dans les conditions prévues à l'article 16.

Article 9.- La requête en suspension ou en révocation sera adressée au prestataire de services de certification électronique.

La suspension ou la révocation du certificat sera notifiée à son titulaire dans un délai ne dépassant pas vingt-quatre heures.

En cas de suspension pour raisons techniques ou de révocations pour les raisons exprimées aux points 2, 6 ou 7 de l'article précédent, la requête contenant les motifs et les pièces justificatives seront notifiées au prestataire de services de certification au plus tard vingt-quatre heures avant sa prise d'effet.

CHAPITRE V : DES PRESTATAIRES DE SERVICES DE CERTIFICATION ELECTRONIQUE

Article 10.- Un prestataire de services de certification électronique qui demande à être reconnu comme qualifié adresse une requête à cette fin au Conseil National des Télécommunications. Le prestataire est tenu de fournir au CONATEL tous les éléments nécessaires au bon accomplissement de la procédure d'évaluation. Il devra satisfaire aux conditions de la loi sur la signature électronique et aux exigences techniques exprimées ci-après.

Article 11.- L'évaluation est effectuée par le CONATEL aux frais du prestataire de services de certification. Son objet est de vérifier que le prestataire se conforme aux spécifications techniques relatives aux prestataires de services de certification en vue de la reconnaissance de sa qualification. A l'issue de la procédure d'évaluation, le CONATEL établit un rapport qui est notifié au prestataire afin que celui-ci puisse, le cas échéant, formuler des observations sur son contenu.

Article 12.- Le prestataire de services de certification électronique doit satisfaire aux exigences techniques suivantes en vue de la qualification :

1. Faire preuve de la fiabilité des services de certification électronique qu'il fournit.
2. Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande.
3. Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat.
4. Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision.
5. Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique.
6. Appliquer des procédures de sécurité appropriées. Le prestataire de services de certification doit notamment appliquer une procédure de sécurité garantissant la confidentialité des causes révocation définitives des certificats électroniques qu'il a délivrés et s'assurer de l'accord du signataire avant de publier ces informations.
7. Utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent. Le module cryptographique utilisé par le prestataire de services de certification électronique pour les fonctions assurées doit être certifié conforme par le CONATEL aux exigences ci-après :
 - a) Assurer la confidentialité et l'intégrité des données de création de signature du prestataire de services de certification durant tout leur cycle de vie ;
 - b) Etre capable d'identifier et d'authentifier ses utilisateurs ;
 - c) Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
 - d) Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
 - e) Détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée ;
 - f) Permettre de créer une signature électronique sécurisée, pour signer les certificats, qui ne révèle pas les données de création de signature du prestataire de services de certification et qui ne peut pas être falsifiée sans la connaissance des données de création de signature du prestataire de services de certification ;
 - g) Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
 - h) Si une fonction de sauvegarde et de restauration des données de création de signature du prestataire de services de certification électronique est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.
8. Prendre toute disposition propre à prévenir la falsification des certificats électroniques.
9. Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données.

10. Veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification.
11. Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique.
12. Utiliser des systèmes de conservation des certificats électroniques garantissant que :
 - a) L'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;
 - b) L'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;
 - c) Toute modification de nature à compromettre la sécurité du système peut être détectée.
13. Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et cette qualité.

La vérification de l'identité de la personne à laquelle le certificat électronique qualifié est destiné est effectuée en sa présence sur présentation d'un document officiel d'identité comportant une photographie (carte d'identification nationale, passeport, permis de séjour) par le prestataire de services de certification électronique ou par un mandataire qu'il désigne et qui s'engage auprès de lui par contrat. Ce contrat prévoit notamment que le mandataire est soumis aux mêmes obligations que le prestataire de certification électronique.

Lorsqu'un signataire se voit délivrer un certificat électronique destiné exclusivement à être utilisé dans le cadre de l'activité professionnelle qu'il exerce pour le compte d'une personne physique ou morale, cette personne physique ou morale peut demander à ce que les vérifications d'identité et de qualité du signataire soient déléguées à un mandataire qu'elle désigne. Elle s'engage alors par contrat avec le prestataire de services de certification électronique à ce que le mandataire procède aux vérifications d'identité dans les conditions visées au paragraphe précédent. Le prestataire de services de certification électronique s'assure de l'origine de cette demande et que les données recueillies par le mandataire soient communiquées dans des conditions sécurisées permettant notamment d'en garantir l'origine et l'intégrité.

14. S'assurer au moment de la délivrance certificat électronique :
 - a) Que les informations qu'il contient sont exactes ;
 - b) Que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat.
15. Avant la conclusion d'un contrat de prestation de services de certification électronique, informer par écrit la personne demandant la délivrance d'un certificat électronique :
 - a) Des modalités et des conditions d'utilisation du certificat ;
 - b) Du fait qu'il s'est soumis ou non au processus de qualification des prestataires de services de certification électronique mentionnée à l'article 7 ;
 - c) Des modalités de contestation et de règlement des litiges.
16. Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au point 15 qui leur sont utiles.

Article 13.- Le CONATEL reconnaît ou non la qualification du prestataire de services de certification électronique au vu du rapport d'évaluation et des éventuelles observations du prestataire.

Lors qu'il reconnaît la qualification d'un prestataire, le CONATEL délivre une attestation qui décrit les activités couvertes par la qualification ainsi que la durée pendant laquelle l'attestation est valable. Pendant cette durée, qui ne peut excéder trois ans, le prestataire doit faire l'objet d'un audit de

surveillance au moins annuel de la part du CONATEL, qui peut conduire à une suspension ou à un retrait de l'attestation de la part du CONATEL.

Les prestataires dont la qualification est reconnue communiquent à toute personne qui en fait la demande une copie de l'attestation délivrée par le CONATEL.

Les prestataires qui fournissent des services techniques aux prestataires de services de certification électronique délivrant des certificats électroniques qualifiés peuvent solliciter auprès du CONATEL, dans les mêmes conditions, une attestation de conformité de ces services aux spécifications techniques figurant à l'article 9 qui leur sont applicables.

L'expression « *prestataire qualifié de services de certification électronique* » ou toute autre expression similaire ne peut être utilisée que par les prestataires de service de certification titulaires d'une attestation de qualification délivrée par le CONATEL. Tout contrevenant verra ses locaux fermés et son matériel saisi par le CONATEL dont les agents pourront pénétrer dans les locaux du contrevenant accompagné d'un officier de police judiciaire qui sera tenu de faire droit à toute requête du CONATEL pour l'entrée des lieux. Le contrevenant s'expose à la responsabilité civile envers ses clients et si des sommes ont été recueillies, le contrevenant ou ses administrateurs seront poursuivis pour escroquerie.

Article 14.- Les prestataires sont soumis à l'inspection ordinaire du CONATEL qui a lieu au moins une fois par an. L'inspection extraordinaire a lieu d'office ou sur dénonciation motivée d'un manquement aux exigences légales ou réglementaires et sera ordonnée par le Directeur Général du CONATEL.

Les inspections seront conduites par les fonctionnaires du CONATEL ou par des experts mandatés à cette fin par le CONATEL. Toute information ou tout document requis par les inspecteurs devra leur être fourni dans un délai ne dépassant pas cinq jours francs à partir de la notification de la requête.

Article 15.- Un certificat électronique délivré par un prestataire de services de certification électronique établi dans un Etat étranger a la même valeur juridique que celui délivré par prestataire établi en Haïti, dès lors :

1. Que le prestataire satisfait aux exigences fixées à l'article 9 et a été qualifié dans l'Etat où il est établi ;
2. Ou que le certificat électronique délivré par le prestataire a été garanti par un prestataire qualifié établi en Haïti ;
3. Ou qu'un accord auquel la République d'Haïti est partie l'a prévu.

Article 16.- En cas de cessation de leurs activités, les prestataires de services de certification électronique en aviseront les signataires au plus tard quatre-vingt-dix jours avant la date prévue de cessation en indiquant avec précision le prestataire qualifié auquel leurs certificats seront transférés. Les signataires ont quinze jours à dater de la réception de l'avis pour s'opposer au transfert. Toute opposition de leur part entraînera la révocation pure et simple de leurs certificats. Les prestataires qui entendent mettre fin à leurs activités en donneront avis au CONATEL au plus tard quatre-vingt-dix jours au plus tard avant la date prévue de cessation. Le CONATEL supervisera le transfert ordonné des certificats à un autre prestataire qualifié, veillant au respect de la confidentialité et de la sécurité et de l'intégrité des données.

En cas de cessation involontaire des activités, pour cause notamment de suspension ou de révocation de la qualification du CONATEL, les prestataires concernés en aviseront immédiatement les signataires et procéderont dans les quinze jours ouvrables précédant la date de cessation d'activités au transfert des certificats dans les conditions prévues au paragraphe précédent.

Article 17.- Les données fournies par les titulaires de certificats électroniques ainsi que les pièces justificatives seront conservées par les prestataires de services de certification vingt ans au moins après la révocation ou l'expiration des certificats correspondants.

En cas de cessation d'activités des prestataires de services de certification et de transfert des données à d'autres prestataires qualifiés, ces derniers conserveront lesdites données et pièces pour le temps qui reste à courir.

Articles 18.- Les prestataires de services de certification électronique sont assujettis au paiement des coûts et droits suivants applicables par le CONATEL :

1. Les droits de traitement de dossier qui se réfèrent aux coûts directement encourus pour le traitement du dossier, l'évaluation, la qualification et autres procédures déterminées par le CONATEL ; et
2. Les droits de supervision, correspondant à la réalisation des inspections et audits ordinaires ou extraordinaires.

Articles 19.- Les droits de traitement de dossier seront appliqués par service offert par le prestataire et seront perçus dès présentation des requêtes correspondantes :

1. Requête à fin de qualification comme prestataire de services
2. Avis de cessation d'activités et de transfert.

Les droits de traitement de dossier sont dus quel que soit le résultat de la requête.

Les droits de supervision tiendront compte des coûts correspondants aux inspections et audits ordinaires ou extraordinaires. Ils sont payables au plus tard quatre-vingt-dix jours suivant la réception de la facture qui les fixe, compte tenu des coûts occasionnés par les inspections et les audits.

Le montant des droits de traitement de dossier et de supervision sera établi et perçu par le CONATEL.

CHAPITRE VI : DES NOTIFICATIONS

Article 20.- Toutes les notifications auxquelles se réfèrent la loi sur la signature électronique et le présent arrêté seront formulées par écrit en utilisant l'une ou l'autre de ces méthodes :

1. Documents électroniques numériques ou messages de données porteur de signatures électroniques transmis selon un protocole de communication électronique.
2. Fac-simile (fax), à condition que le destinataire fasse état de la réception.
3. Correspondance avec accusé de réception.
4. Exploit d'huissier.
5. Tout autre moyen physique ou électronique .

Les prestataires de services de certification électronique fourniront au CONATEL une adresse de courriel où seront envoyées les communications et notifications. Toute notification effectuée par cette adresse sera réputée avoir été reçue.

Article 21.- Les prestataires de services de certification électronique qui sont des personnes morales devront communiquer au CONATEL le nom des membres du conseil d'administration.

Article 22.- Le Ministre des Travaux Publics, Transports et Communications est chargé de l'exécution du présent arrêté qui sera publié au Journal Officiel, Le Moniteur.

Fait au Palais National, le ..

Par le Président
[suivent les noms des ministres]

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

<p style="text-align: center;">ANNEXE 3 : AVANT-PROJET DE LOI SUR LES ECHANGES ELECTRONIQUES</p>
--

AVANT PROJET DE LOI
SUR
LES ECHANGES ELECTRONIQUES

Le Pouvoir Exécutif

Vu la Loi no. 18 du Code Civil ;

Vu les livres 1^{er} et 2^e du Code de Commerce ;

Vu la Loi du sur la signature électronique adaptant le droit de la preuve aux technologies de l'information et son arrêté d'application ;

Considérant la place croissante du commerce électronique dans les échanges commerciaux ;

Considérant que les nouvelles technologies de l'information et de la communication révolutionnent la manière de faire du commerce, en créant au niveau planétaire un unique marché virtuel ;

Considérant la production de normes d'origine internationale visant à harmoniser la manière d'appréhender les réalités du commerce électronique ; particulièrement la Loi-Type de la Commission des Nations-Unies pour le Droit du Commerce International (CNUDCI) ;

Considérant que la Résolution 51/162 de l'Assemblée Générale de la Commission des Nations Unies pour le Droit Commercial International du 16 décembre 1996 recommande aux Etats membres de tenir compte de la loi-type de la CNUDCI sur le commerce électronique ;

Considérant que la majorité des Etats de l'hémisphère, indépendamment de leurs systèmes juridiques, ont adapté les recommandations de la loi-type de la CNUDCI à leur droit national ;

Considérant que la compétitivité des opérateurs économiques haïtiens est handicapée par l'inadaptation du droit haïtien à ces développements technologiques ;

Considérant qu'il convient de moderniser les règles juridiques afin d'armer les opérateurs économiques haïtiens dans la compétition économique internationale ;

Considérant que le droit haïtien reconnaît déjà la validité des documents et de la signature électroniques et leur force probante au même titre que les documents sur papier et la signature

manuscrite ; qu'il est nécessaire de compléter ce dispositif par des règles propres à sécuriser les transactions et les opérations commerciales ;

A Proposé

Et le Pouvoir Législatif

A Voté

La Loi Suivante

TITRE I : LES ECHANGES ELECTRONIQUES EN GENERAL

CHAPITRE I : DISPOSITIONS GENERALES

Article 1.- La présente loi s'applique à toute information, de quelque nature que ce soit, prenant la forme d'un message de données utilisé dans le contexte de relations contractuelles ou extra contractuelles, civiles ou commerciales. Ces relations comprennent notamment :

- La fourniture ou l'échange de marchandises ou de services ;
- Tout accord de distribution ;
- La représentation commerciale ;
- L'affacturage ;
- La location-vente ;
- La vente avec clause de réserve de propriété ;
- La construction d'usines ;
- Les services de consultation ;
- L'ingénierie ;
- L'investissement ;
- Le financement ;
- Toute opération bancaire ;
- L'assurance ;
- L'accord d'exploitation ou de concession ;
- La coentreprise et les autres formes de coopération industrielle ou commerciale ;
- Le transport de marchandises ou de voyageurs par voie aérienne ou maritime, par chemin de fer ou par route.

La présente loi ne s'applique pas aux situations où la perfection de l'acte juridique est soumise à une formalité d'affichage ou à l'intervention d'un officier ministériel ou d'un service de l'Etat.

Article 2.- Aux fins de la présente loi :

1. Le terme « *message de données* » désigne l'information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie ;
2. Le terme « *échange de données informatisées (EDI)* » désigne le transfert électronique d'une information d'ordinateur à ordinateur mettant en œuvre une norme convenue pour structurer l'information ;
3. Le terme « *expéditeur* » désigne la personne par laquelle, ou au nom de laquelle, le message de données est réputé avoir été envoyé ou créé avant d'avoir été éventuellement conservé, mais non la personne qui agit en tant qu'intermédiaire pour ce message ;

4. Le terme « *destinataire* » désigne la personne qui, dans l'intention de l'expéditeur, est censée recevoir le message de données, mais non la personne qui agit en tant qu'intermédiaire pour ce message ;
5. Le terme « *intermédiaire* » désigne, dans le cas d'un message de données particulier, la personne qui, au nom d'une autre, envoie, reçoit ou conserve le message ou fournit d'autres services afférents à celui-ci ;
6. Le terme « *système d'information* » désigne un système utilisé pour créer, envoyer, recevoir, conserver ou traiter de toute autre manière des messages de données.

Article 3.- Pour l'interprétation de la présente loi, il est tenu compte des recommandations des organismes multilatéraux en la matière, de la nécessité de promouvoir l'uniformité de son application et le respect de la bonne foi. Les questions concernant les matières régies par la présente loi qui ne sont pas expressément réglées par elle sont tranchées selon les principes généraux dont elle s'inspire.

CHAPITRE II : APPLICATION DES EXIGENCES LEGALES AUX MESSAGES DE DONNEES

Article 4.- Lorsqu'un texte législatif ou réglementaire exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence

- S'il existe une garantie fiable quant à l'intégrité de l'information à partir du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre ; et
- Si, lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée.

L'intégrité de l'information s'apprécie en déterminant si celle-ci est restée complète et n'a pas été altérée, exception faite de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition.

Le niveau de fiabilité requis s'apprécie au regard de l'objet pour lequel l'information a été créée et à la lumière de toutes les circonstances y relatives.

Article 5.- Lorsqu'un texte législatif ou réglementaire exige que certains documents, registres ou informations soient conservés, cette exigence est satisfaite si sont conservés des messages de données, moyennant les conditions suivantes :

1. L'information contenue dans le message de données est accessible pour consultation ultérieure.
2. Le message de données est conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues.
3. Les informations permettant de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception, doivent être conservées si elles existent.

Article 6.- L'obligation de conserver des documents, registres ou informations conformément à l'article précédent ne s'étend pas aux informations qui n'ont pour but que de permettre l'envoi ou la réception du message de données.

L'exigence de conservation exprimée à l'article précédent peut être satisfaite en recourant aux services d'une autre personne, sous réserve que soient remplies les conditions fixées aux alinéas 1, 2 et 3 de l'article précédent.

CHAPITRE III : COMMUNICATION DE MESSAGES DE DONNEES

Article 7.- Lors de la formation des contrats, une offre et l'acceptation de cette offre peuvent être exprimées par un message de données, sauf convention contraire des parties. Ne peuvent être niées la validité ou la force exécutoire d'un contrat du seul fait de l'utilisation d'un ou de plusieurs messages de données lors de sa formation.

Article 8.- Lors de l'appréciation de la relation entre l'expéditeur et le destinataire d'un message de données, l'effet juridique, la validité ou la force exécutoire d'une manifestation de volonté ou autre déclaration ne sont pas niées du seul fait que cette manifestation de volonté ou autre déclaration a emprunté la forme d'un message de données.

Article 9.- Un message de données émane de l'expéditeur s'il a été envoyé

- par l'expéditeur lui-même ;
- par une personne autorisée à agir à cet effet au nom de l'expéditeur ; ou
- par un système d'information programmé par l'expéditeur ou en son nom pour fonctionner automatiquement.

Le destinataire est fondé à considérer qu'un message de données émane de l'expéditeur et à agir en conséquence ;

- si, pour s'assurer que le message de données émanait de l'expéditeur, il a correctement appliqué une procédure que l'expéditeur avait précédemment acceptée à cette fin ; ou
- si le message de données tel qu'il l'a reçu résulte des actes d'une personne qui, de par ses relations avec l'expéditeur ou un agent de celui-ci, a eu accès à un dispositif que l'expéditeur utilise pour identifier comme étant de lui les messages de données.

Le paragraphe précédent ne s'applique pas

- dès lors que le destinataire a été avisé par l'expéditeur que le message de données n'était pas de lui et qu'il a eu un délai raisonnable pour agir en conséquence ;
- lorsque, dans la seconde éventualité du paragraphe précédent, le destinataire savait, ou aurait dû savoir s'il avait pris des dispositions raisonnables ou utilisé une procédure convenue, que le message de données n'émanait pas de l'expéditeur.

Lorsqu'un message de données émane ou est réputé émaner de l'expéditeur, ou lorsque le destinataire est en droit d'agir sur cette présomption, le destinataire est fondé à considérer le message de données tel qu'il l'a reçu comme étant celui que l'expéditeur se proposait de lui faire parvenir, et à agir en conséquence. Le destinataire ne peut agir ainsi s'il savait, ou aurait dû savoir s'il avait pris des dispositions raisonnables ou utilisé une procédure convenue, que la transmission avait entraîné une erreur dans le message de données tel qu'il a été reçu.

Article 10.- Le destinataire peut considérer comme distinct chaque message de données reçu et agir en conséquence, à moins que le message ne soit la répétition d'un autre et que le destinataire ne sache, ou n'aurait dû savoir s'il avait pris des dispositions raisonnables ou utilisé une procédure convenue, qu'il s'agissait du même message.

Article 11.- Le présent article s'applique dans le cas où l'expéditeur, avant ou au moment d'envoyer un message de données ou dans ce message même, a demandé au destinataire un accusé de réception ou est convenu avec lui qu'il y aurait un accusé de réception.

Si l'expéditeur et le destinataire n'ont pas convenu d'une forme particulière, la réception peut être accusée

- par toute communication, automatisée ou autre, émanant du destinataire, ou
- par tout acte du destinataire

suffisant pour indiquer à l'expéditeur que le message de données a été reçu.

Si l'expéditeur subordonne l'effet du message de données à la réception d'un accusé de réception, le message de données est considéré comme n'ayant pas été envoyé tant que l'accusé de réception n'a pas été reçu.

Si l'expéditeur ne subordonne pas l'effet du message de données à la réception d'un accusé de réception, s'il n'a pas reçu d'accusé de réception dans le délai fixé ou convenu ou, quand aucun délai n'a été fixé ni convenu, l'expéditeur peut, dans les quarante-huit heures de l'envoi de son message ou de l'expiration du délai fixé

1. aviser le destinataire qu'aucun accusé de réception n'a été reçu et fixer un délai n'excédant pas quarante-huit heures à partir de l'expédition du nouveau message de données dans lequel l'accusé de réception doit être reçu ; et
2. si l'accusé de réception n'est pas reçu dans le délai fixé à l'alinéa 1 précédent, et sur notification adressée au destinataire, considérer que le message de données n'a pas été envoyé ou exercer tout autre droit qu'il peut avoir.

Lorsque l'expéditeur reçoit l'accusé de réception du destinataire, le message de données en question est réputé avoir été reçu par le destinataire. Cette présomption n'implique pas que le message de données correspond au message reçu.

Lorsque l'accusé de réception indique que le message de données en question est conforme aux conditions techniques convenues ou fixées dans les normes applicables, ces conditions sont présumées remplies.

Le présent article ne régit que les effets relatifs à l'accusé de réception. Les conséquences juridiques du message de données demeurent régies par les règles applicables à l'acte juridique ou à la transaction exprimés dans ledit message de données.

Article 12.- Sauf convention contraire entre les parties, l'expédition d'un message de données intervient lorsque celui-ci entre dans un système d'information ne dépendant pas de l'expéditeur.

Sauf convention contraire entre les parties, le moment de la réception du message de données est défini comme suit :

1. Si le destinataire a désigné un système d'information pour recevoir des messages de données, la réception a lieu au moment où le message de données entre dans le système d'information désigné ;
2. Si le destinataire a désigné un système d'information pour recevoir des messages de données et que le message est envoyé à un autre système d'information du destinataire, la réception a lieu au moment où le message est relevé par le destinataire.
3. Si le destinataire n'a pas désigné de système d'information, la réception a lieu au moment où le message de données entre dans un système d'information du destinataire.

Les dispositions du paragraphe précédent s'appliquent même si le lieu où est situé le système d'information est différent du lieu où le message de données est réputé être reçu selon l'article suivant.

Article 13.- Sauf convention contraire entre les parties, le message de données est réputé avoir été expédié du lieu où l'expéditeur a son domicile, son siège social et avoir été reçu au lieu où le destinataire a son domicile ou son siège social.

Si l'expéditeur ou le destinataire n'a pas de domicile ou de siège social connu, le lieu retenu est celui de l'établissement qui entretient la relation la plus étroite avec l'opération sous-jacente ou, en l'absence d'opération sous-jacente, le lieu de l'établissement principal.

Si l'expéditeur ou le destinataire n'a pas d'établissement, le lieu retenu est celui de sa résidence habituelle.

Article 14.- Pour les messages de données qui se transmettent sur des supports physiques, comme les disques numériques, les moyens magnétiques, les moyens photo-lithographiques, les supports optiques et autres supports similaires, le moment et le lieu de l'expédition et de la réception sont déterminés par les règles s'appliquant à la transmission de documents sur support papier ou autrement.

DEUXIEME PARTIE : LE COMMERCE ELECTRONIQUE DANS CERTAINS DOMAINES D'ACTIVITÉ

CHAPITRE UNIQUE : LE TRANSPORT DE MARCHANDISES

Article 14.- Sans préjudice des dispositions de la première partie, le présent chapitre s'applique à tout acte relatif à un contrat de transport de marchandises ou entrepris en exécution d'un tel contrat, notamment, mais non exclusivement, les actes suivants.

1. Les actes relatifs à l'embarquement et à la réception des marchandises
 - a) Indication des marques, du nombre, de la quantité ou du poids des marchandises ;
 - b) Déclaration de la nature ou de la valeur des marchandises ;
 - c) Emission d'un reçu des marchandises ;
 - d) Confirmation du chargement des marchandises
2. Les actes relatifs aux conditions du transport
 - a) Notification des conditions du contrat
 - b) Communication d'instructions à un transporteur
3. Les actes relatifs à la livraison des marchandises
 - a) Demande de livraison des marchandises
 - b) Autorisation de remise des marchandises
 - c) Notification de perte ou d'avarie de marchandises
4. Toute autre notification ou déclaration présentée dans le cadre de l'exécution du contrat.
5. Engagement de livrer les marchandises à une personne désignée ou à une personne autorisée à se faire livrer.
6. Octroi, acquisition, remise, transfert, négociation ou abandon des droits sur les marchandises.
7. Acquisition ou transfert de droits et obligations en vertu du contrat.

Article 15.- Sans préjudice des dispositions du troisième paragraphe du présent article, lorsqu'un texte législatif ou réglementaire exige qu'un acte visé à l'article précédent soit exécuté par écrit au moyen d'un document papier, cette exigence est satisfaite si l'acte est exécuté au moyen d'un ou de plusieurs messages de données.

Le paragraphe précédent s'applique que l'exigence qui y est visée ait la forme d'une obligation ou que le texte législatif ou réglementaire prévoie simplement certaines conséquences si l'acte n'est pas exécuté par écrit au moyen d'un document papier.

Quand un droit doit être dévolu à une personne et à aucune autre, ou quand une obligation doit être acquise par une personne et aucune autre, et si un texte législatif ou réglementaire exige à cette fin que le droit ou l'obligation soient transmis à l'intéressé par le transfert ou l'utilisation d'un document papier, cette exigence est satisfaite si le droit ou l'obligation en question sont transmis par un ou plusieurs messages de données, à condition qu'une méthode fiable soit utilisée pour rendre uniques le message ou les messages en question.

Le niveau de fiabilité requis aux fins du paragraphe précédent s'apprécie au regard de l'objet pour lequel le droit ou l'obligation ont été transmis et à la lumière de toutes les circonstances, notamment de tout accord en la matière.

Lorsqu'un ou plusieurs messages de données sont utilisés pour exécuter l'un des actes mentionnés aux alinéas 6 et 7 de l'article 14, aucun document papier utilisé pour exécuter cet acte n'est valide à moins que l'utilisation de messages de données n'ait été abandonnée et remplacée par l'utilisation de documents papier. Tout document papier émis dans ces conditions doit contenir la notification de ce remplacement. Celui-ci est sans effet sur les droits ou les obligations des parties.

Une règle d'ordre public ou une loi de police s'appliquant à un contrat de transport de marchandises s'applique à tout contrat de transport de marchandises qui est constaté par un ou plusieurs messages de données. L'application de telles règles ne pourra être écartée pour la seule raison que le contrat est constaté par de tels messages et non par un document papier.

Article 16.- La présente loi abroge toutes lois ou dispositions de lois, tous décrets ou dispositions de décrets, tous décrets-lois ou dispositions de décrets-lois qui lui sont contraires et sera exécutée à la diligence des Ministres de l'Economie et des Finances, du Commerce et de l'Industrie, et de la Justice, chacun en ce qui le concerne.

Donné à la Chambre des Députés le

Donné au Sénat le

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

<p style="text-align: center;">ANNEXE 4 : AVANT PROJET DE LOI SUR L'ADMINISTRATION ELECTRONIQUE</p>

AVANT PROJET DE LOI
SUR L'ADMINISTRATION ELECTRONIQUE

Le Pouvoir Exécutif

Vu les articles 5, 16, 17, 18, 28, 40, 49, 54, 125, 207, 234 et 236 de la Constitution ;

Vu l'article 1^{er} du Code Civil ;

Vu le décret du 17 mai 2005 sur l'Administration Centrale de l'Etat ;

Vu la loi du ...2010 sur les télécommunications ;

Vu la loi du ...2010 sur la signature électronique, adaptant le droit de la preuve aux technologies de l'information et de la communication et élargissant les compétences du Conseil National des Télécommunications ; et son arrêté d'application ;

Considérant que l'administration électronique se définit par l'usage des technologies de l'information et de la communication par les entités administratives pour améliorer qualitativement les services et informations offerts aux citoyens ; augmenter l'efficacité et l'efficacités de la gestion publique et augmenter de manière substantielle la transparence du secteur public et la participation citoyenne ;

Considérant que la transparence des activités gouvernementales, la probité et la responsabilité des gouvernements dans la gestion de la chose publique constituent des composantes fondamentales de la démocratie ;

Considérant qu'il convient de tirer parti des possibilités offertes par les technologies de l'information et de la communication pour accroître l'efficacité et la transparence du secteur public ;

Considérant que la mise en œuvre de l'administration électronique est un facteur puissant de la modernisation de l'Etat ;

Considérant que la réduction de la fracture numérique constitue une impérieuse obligation pour l'Etat ;

Considérant que le bilinguisme constitue une richesse culturelle qu'il convient de préserver dans le cadre de l'administration électronique dans le but de créer une société plus inclusive et favoriser un accès égal des citoyens à l'administration électronique ;

Sur le rapport du Premier Ministre et après délibération en Conseil des Ministres ;

A Proposé

Et le Pouvoir Législatif

A Voté la Loi Suivante :

TITRE PRELIMINAIRE : DU CHAMP D'APPLICATION ET DES PRINCIPES GENERAUX

Article 1.- Objet de la loi

La présente loi reconnaît le droit de tout administré à s'adresser à l'administration publique par des moyens électroniques. Elle régit les aspects fondamentaux de l'utilisation des technologies de l'information dans l'activité administrative, dans les rapports entre les divers services et entités de l'administration publique, ainsi que dans les rapports entre les administrés et l'administration publique. Elle garantit les droits des administrés, l'égalité de traitement des administrés, la validité et l'efficacité de l'action administrative dans des conditions de sécurité juridique.

L'administration publique utilisera les technologies de l'information ainsi qu'il est prescrit dans la présente loi en s'assurant de la disponibilité de l'accès, de l'intégrité, de l'authenticité, de la confidentialité et de la conservation des données, informations et services traités.

Article 2.- Champ d'application

La présente loi s'applique :

- a) A l'administration publique entendue comme étant l'administration centrale de l'Etat, les services déconcentrés, les collectivités territoriales et les organismes autonomes ;
- b) Aux administrés dans leurs rapports avec l'administration publique ;
- c) Aux rapports à l'intérieur de l'administration publique.

La présente loi ne s'applique pas aux activités de l'administration publique régies par le droit privé.

Article 3.- Objectifs de la loi

Les objectifs de la loi sont de

- a) Permettre l'exercice des droits et l'accomplissement des obligations par des moyens électroniques ;
- b) Permettre l'accès des administrés par des moyens électroniques aux procédures administratives en visant particulièrement l'élimination des barrières qui en limitent l'accès ;
- c) Créer les conditions de confiance dans l'usage des moyens électroniques en établissant les moyens nécessaires à la préservation des droits fondamentaux, particulièrement ceux relatifs à la vie privée et la protection des données personnelles, en garantissant la sécurité des systèmes, des données, des communications et des services électroniques ;
- d) Promouvoir la transparence administrative ainsi que l'amélioration continue des services publics dans la poursuite de l'intérêt général ;
- e) Contribuer à l'amélioration du fonctionnement interne de l'administration publique, en augmentant l'efficacité par l'usage des technologies de l'information, avec toutes les garanties légales dans l'exercice de ses compétences ;
- f) Simplifier les procédures administratives, en accroître la transparence et favoriser une meilleure participation citoyenne ;

- g) Contribuer au développement de la société du savoir dans le cadre de l'administration publique et dans celui de la société en général.

Article 4.- Principes généraux

L'utilisation des technologies de l'information trouve ses limites dans la constitution et la législation en vigueur. Elle respecte les droits fondamentaux des citoyens qui y sont reconnus. Elle s'effectue en fonction des principes suivants :

- a) Le respect de la vie privée, la protection des données à caractère personnel, le respect de l'honneur et de la réputation des administrés.
- b) Le principe de l'égalité des administrés. L'usage de moyens électroniques ne doit en aucun cas créer des discriminations à l'encontre ou en faveur des administrés dans leurs rapports avec l'administration publique, sans préjudice des mesures visant à encourager l'utilisation des moyens électroniques.
- c) Le principe de l'accès à l'information et aux services publics par des moyens électroniques par le biais de systèmes qui en permettent l'obtention de manière sûre et compréhensible ; étant particulièrement garanti l'accès universel indépendamment des supports, canaux et environnements de manière à ce que toutes les personnes puissent de manière égale exercer leurs droits. Un arrêté du Premier Ministre viendra préciser les modes d'accès des personnes handicapées à l'information et aux services publics électroniques.
- d) Le principe de la légalité de l'action administrative. Les entités administratives publieront sur leurs sites électroniques les lois et règlements de toutes sortes régissant leurs compétences, fonctionnement, activités et services.
- e) Le principe de coopération dans l'utilisation des moyens électroniques par l'administration publique dans le but de garantir l'interopérabilité des systèmes et solutions adoptées par chaque entité de l'administration publique. En particulier est garantie la reconnaissance mutuelle des documents électroniques et des moyens d'identification et d'authentification qui se conforment aux dispositions de la présente loi.
- f) Le principe de sécurité dans l'implantation et l'utilisation des moyens électroniques par l'administration publique en vertu duquel s'appliquera au moins le même niveau de garantie et de sécurité que celui requis pour l'utilisation des moyens non électroniques dans le cadre de l'activité administrative.
- g) Le principe de proportionnalité en vertu duquel seront seulement exigées les garanties et mesures de sécurité adaptées à la nature et aux circonstances des diverses formalités et procédures. De même il ne sera requis des administrés que les données strictement nécessaires à la finalité pour laquelle elles sont demandées.
- h) Le principe de responsabilité et de qualité relativement à la véracité et à l'authenticité des informations et services offerts par l'administration publique à travers les moyens électroniques.
- i) Le principe de neutralité technologique et d'adaptabilité au progrès des techniques et systèmes de communications électroniques garantissant un choix indépendant des alternatives technologiques par les administrés et l'administration publique, ainsi que le libre développement des avancées technologiques dans un environnement concurrentiel. A cet effet, l'administration publique utilisera des standards ouverts ainsi que, de manière complémentaire, des standards utilisés de manière généralisée par les administrés.
- j) Le principe de simplification administrative par une réduction substantielle de la durée des procédures administratives, en vue d'une plus grande efficacité de l'activité administrative.

- k) Le principe de transparence et de publicité des procédures administratives, l'usage des moyens électroniques devant faciliter les plus grandes diffusion, publicité et transparence des procédures administratives.

Article 5.- Définitions

A l'effet de la présente loi, on entend par

- a) Activité de services : toute activité économique exercée à son propre compte généralement en échange de rémunération.
- b) Adresse électronique : identifiant d'un équipement ou d'un système électronique à partir duquel on obtient une information dans un réseau de communications.
- c) Administré : toutes personnes physiques ou morales qui entrent en rapport ou sont susceptibles d'entrer en rapport avec l'administration publique.
- d) Application : programme ou ensemble de programmes dont l'objet est la résolution d'un problème par l'usage de l'informatique.
- e) Application de sources ouvertes : l'application distribuée par une licence qui permette la liberté d'exécution, la connaissance du code source, sa modification, son amélioration et la distribution de copies à d'autres usagers.
- f) Canaux : les structures ou moyens de diffusion des contenus et des services, incluant la présence physique, le canal téléphonique ou électronique, ceux qui existent actuellement ou qui pourront exister dans le futur.
- g) Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.
- h) Certificat électronique qualifié : un certificat électronique délivré par un prestataire de services de certification électronique qualifié et répondant aux exigences définies à l'article 6 de l'Arrêté pris pour l'application de la Loi sur la Signature Electronique, Adaptant le Droit de la Preuve aux Technologies de l'Information et Elargissant les Compétences du Conseil National des Télécommunications.
- i) Certification : la certification par des moyens électroniques de l'identité d'une personne ou d'une entité, du contenu de la volonté exprimée dans ses opérations, transactions et documents, de l'intégrité et de l'origine de ces derniers
- j) Données de création de signature électronique : les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique.
- k) Dispositif de création de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique.
- l) Dispositif sécurisé de création de signature électronique : un dispositif de création de signature électronique qui satisfait aux exigences définies à l'article 4 de l'Arrêté pris pour l'application de la Loi sur la Signature Electronique, Adaptant le Droit de la Preuve aux Technologies de l'Information et Elargissant les Compétences du Conseil National des Télécommunications.
- m) Données de vérification de signature électronique : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique.
- n) Dispositif de vérification de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique.
- o) Document électronique : information de toute nature sous forme électronique, archivée sur un support électronique selon un format déterminé et susceptible d'identification et de traitement différencié.

- p) Espaces communs ou guichets uniques : modes ou canaux (bureaux intégrés, assistance téléphonique, page web etc.) auxquels les administrés peuvent se présenter pour accéder aux informations, formalités et services publics déterminés selon accord entre diverses entités administratives.
- q) Interopérabilité : capacité des systèmes d'information, par le biais des procédures auxquelles ils servent de support, à partager des données et à rendre possibles entre eux l'échange d'informations et de connaissances.
- r) Moyen électronique : mécanisme, installation, équipement ou système permettant la production, la sauvegarde ou la transmission de documents, de données et d'informations ; incluant tout réseau de communication ouvert ou restreint comme l'internet, la téléphonie filaire et mobile etc.
- s) Point d'accès électronique : ensemble de pages web groupées en un domaine internet dont l'objectif est d'offrir à l'utilisateur, de manière aisée et intégrée, l'accès à une série de ressources et de services destinés à répondre aux nécessités spécifiques d'un groupe de personnes ou à accéder à l'information et aux services d'une entité administrative.
- t) Prestataire de services : toute personne physique ou morale qui offre ou effectue des activités de services.
- u) Procédure administrative automatisée : la procédure administrative produite par un système d'information adéquatement programmé ne nécessitant pas l'intervention d'une personne physique pour chaque cas particulier. Elle inclut la production de formulaires, d'actes mettant fin à une procédure ainsi que les simples actes de communications.
- v) Sceau horodateur : certificat délivré par un tiers de certification attestant de la date et de l'heure de la réalisation d'une opération ou d'une transaction quelconque par des moyens électroniques
- w) Signature électronique : donnée qui résulte de l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. Elle identifie celui qui l'appose et manifeste le consentement du signataire aux obligations qui découlent de cet acte.
- x) Signature électronique sécurisée : une signature électronique qui est propre au signataire qui est créée par des moyens que le signataire puisse garder sous son contrôle exclusif, qui garantit avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.
- y) Standard ouvert : celui qui réunit les conditions suivantes
 - Qu'il soit public et que son utilisation soit disponible gratuitement ou à un coût qui n'en prohibe pas l'accès,
 - Que son usage et son application ne soit pas subordonné au paiement d'un droit de propriété intellectuelle

TITRE I : DU DROIT DES ADMINISTRÉS
A UTILISER LES MOYENS ELECTRONIQUES
DANS LEUR RAPPORT AVEC L'ADMINISTRATION PUBLIQUE

Article 6.- Droit des administrés

Il est reconnu aux administrés le droit d'utiliser les moyens électroniques dans leurs rapports avec l'administration publique pour l'exercice de leurs droits, l'obtention d'informations, la formulation de

réclamations, la présentation de requêtes, l'expression de consentement, la réalisation de paiements ou de transactions, l'opposition à des décisions ou actes administratifs.

De plus, les administrés ont, relativement à l'utilisation des moyens électroniques dans l'activité administrative, les droits suivants :

- a) Choisir, parmi tous ceux qui sont disponibles sur le moment, le canal par lequel s'établissent les rapports avec l'administration publique.
- b) N'avoir pas à soumettre les données et documents que détient déjà l'administration publique, laquelle utilisera les moyens électroniques pour obtenir ladite information. Toutes les fois où il s'agira de données à caractère personnel, le consentement de la personne intéressée est obligatoire sauf dans les cas relevant de la police judiciaire, de la lutte contre la corruption, l'évasion fiscale, le blanchiment d'avoirs ou le financement du terrorisme ou relevant de la sécurité nationale. Le consentement pourra être émis et obtenu par des moyens électroniques.
- c) L'égalité d'accès électronique aux services de l'administration publique.
- d) Savoir grâce aux moyens électroniques l'état des procédures en cours qui les concernent, sauf dans les cas où la loi ou les règlements restreignent l'accès à cette connaissance.
- e) Obtenir copie électronique des documents électroniques constituant le dossier d'une procédure où ils sont intéressés.
- f) La conservation et l'archivage par l'administration publique sous forme électronique des documents électroniques constitutifs d'une démarche ou d'une procédure.
- g) Obtenir les moyens d'identification électronique nécessaires et utiliser les systèmes de signature électronique admis dans le cadre de l'administration publique.
- h) La garantie de sécurité et de confidentialité des données figurant dans les fichiers, systèmes et applications de l'administration publique.
- i) La qualité des services publics fournis par des moyens électroniques.
- j) Choisir dans leurs rapports avec l'administration publique les applications ou systèmes utilisant des standards ouverts ou, à défaut, deux qui sont utilisés de manière générale par les administrés.

Article 7.- La défense des droits des administrés.

Le Protecteur du Citoyen veillera à la garantie et au respect des droits reconnus aux administrés par la présente loi, sans préjudice des compétences attribuées en ce domaine à d'autres organes ou juridictions.

Le Protecteur du Citoyen adressera annuellement durant le dernier trimestre de l'année fiscale un rapport au Président de la République, au Premier Ministre et aux Présidents de Chambres du Parlement. Ce rapport contiendra une analyse des plaintes et suggestions reçues et une proposition des actions et mesures à adopter pour l'effectivité des droits reconnus aux administrés.

Dans l'exercice de ses fonctions, le Protecteur du Citoyen aura accès à toutes les entités de l'administration publique offrant des services en ligne. Les directeurs généraux des ministères, les directeurs administratifs des services déconcentrés et décentralisés l'assisteront dans l'élaboration du rapport annuel et le maintiendront informé de manière continue des plaintes et suggestions reçues relativement à la fourniture de services publics par des moyens électroniques. Un projet du rapport sera adressé au Conseil Supérieur de l'Administration et de la Fonction Publiques. Sa rédaction définitive n'interviendra qu'après que le Protecteur du Citoyen aura rencontré ledit Conseil.

Article 8.- La garantie des droits des administrés.

L'administration publique devra aménager plusieurs canaux ou moyens en vue de la fourniture de services électroniques, en garantissant l'accès à tous les administrés, indépendamment de leurs particularités personnelles, de leurs moyens, de leurs connaissances. Les administrés adopteront la forme qui leur semble la plus adéquate.

L'Etat garantit à tous les administrés l'accès aux services électroniques offerts par l'administration centrale et les services déconcentrés en utilisant au moins les moyens suivants

- a) Les bureaux d'accueil et d'assistance qui mettront librement et gratuitement à la disposition des administrés les moyens et instruments nécessaires à l'exercice des droits reconnus à l'article 6 de la présente loi. Une assistance pour l'utilisation des équipements devra être incorporée au moyen ou à l'instrument eux-mêmes ou fournie par le personnel de ces bureaux.
- b) Des points d'accès électronique, consistant en des sites portails créés et gérés par les diverses entités de l'administration publique et disponibles aux administrés à travers les réseaux de communication. Particulièrement, il sera créé un Site Portail Général à travers lequel les administrés pourront, dans leurs rapports avec l'administration publique, accéder à toute l'information et à tous les services disponibles. Ce Site Portail Général contiendra la liste des services disponibles aux administrés et l'accès à ces services, dans un souci de coordination avec les autres sites portails de l'administration publique, ainsi qu'un moteur de recherche.
- c) Des services d'assistance téléphonique qui, dans les limites permises par les critères sécurité et possibilités techniques, faciliteront l'accès des administrés aux informations et services électroniques auxquels se réfèrent les paragraphes précédents.

Article 9.- La transmission des données à l'intérieur de l'administration publique.

Pour l'exercice efficace du droit reconnu à l'article 6 alinéa 2 b), chaque entité de l'administration publique devra faciliter l'accès des autres entités aux données qu'elle détient relatives aux personnes intéressées et qui se trouvent sur support électronique. Elle spécifiera les conditions, les protocoles, les critères fonctionnels et techniques nécessaires pour accéder à ces données dans les meilleures conditions de sécurité, d'intégrité, de disponibilité et de respect des informations à caractère personnel.

La disponibilité de ces données est limitée strictement à celles requises des administrés par les autres entités administratives pour les formalités et procédures relevant de leurs compétences légales. L'accès aux données à caractère personnel demeure subordonné aux conditions prescrites à l'article 6 alinéa 2 b) de la présente loi.

TITRE II : DU REGIME JURIDIQUE DE L'ADMINISTRATION ELECTRONIQUE

CHAPITRE I.- DU SITE ELECTRONIQUE

Article 10.- Le site électronique

Le site électronique est l'adresse électronique disponible aux administrés à travers les réseaux de communication dont le titre, la gestion et l'administration incombent à une entité administrative.

L'établissement d'un site électronique confère à son titulaire la responsabilité en ce qui a trait à l'intégrité, la véracité et la mise à jour de l'information et des services auxquels on peut accéder par l'intermédiaire de ce site.

Chaque entité de l'administration publique déterminera les conditions et instruments de création des sites électroniques en respectant les principes de publicité officielle, de responsabilité, de qualité, de sécurité, de disponibilité, d'accessibilité, de neutralité et d'interopérabilité. Dans tous les cas l'identité du titulaire du site devra être garantie, ainsi que la disponibilité des moyens pour la formulation des plaintes, requêtes et suggestions.

Les sites électroniques disposeront de systèmes qui permettent l'établissement de communications sécurisées toutes les fois que ce sera nécessaire.

La publication sur les sites électroniques d'informations, de services et de transactions respectera les principes d'accessibilité et de maniabilité conformément aux normes établies en la matière, fera application de standards ouverts ou à défaut de ceux utilisés de manière généralisée par les administrés.

Article 11.- Publication électronique du Journal Officiel

Toutes les fois où une publication est requise par la loi ou les règlements au Journal Officiel, la publication sur le site électronique du Journal Officiel « Le Moniteur » emportera les mêmes effets que celle effectuée dans l'édition imprimée.

La publication du Journal Officiel « Le Moniteur » sur le site électronique correspondant aura un caractère officiel et authentique, les effets de cette publication étant régis par l'article 1^{er} du code civil et les articles 125 et 125-1 de la constitution.

Article 12.- Publication électronique d'annonces légales.

Toutes les fois où la loi ou un règlement prescrit la publication d'un avis, d'une annonce ou d'un dispositif de jugement quelconques dans un quotidien à grand tirage, cette formalité sera respectée si la publication a lieu sur le site électronique du journal correspondant.

CHAPITRE II.- DE L'IDENTIFICATION ET DE L'AUTHENTIFICATION

Section 1.- Dispositions communes

Article 13.- Formes d'identification et d'authentification.

L'administration publique admettra dans ses rapports par la voie électronique, les systèmes de signature électronique sécurisée conformes à l'Arrêté d'Application de la Loi sur la Signature Electronique.

Les administrés pourront utiliser les systèmes suivants de signature électronique dans leurs rapports avec l'administration publique, compte tenu des exigences de chaque entité administrative :

- a) Les signatures électroniques sécurisées, y compris celles attestées par des certificats électroniques qualifiés ;
- b) D'autres systèmes de signature électronique, comme la fourniture d'une information connue seulement des deux parties ou des systèmes non cryptographiques, selon les termes et conditions déterminés par chaque cas.

Les entités administratives pourront utiliser les systèmes suivants d'identification électronique et d'authentification des documents électroniques qu'elles produisent :

- a) Les signatures électroniques sécurisées attestées par des certificats électroniques qualifiés ou des moyens équivalents permettant l'identification du site électronique et l'établissement à travers lui de communications sécurisées ;
- b) Les systèmes de signature électronique adaptés aux procédures administratives automatisée ;
- c) La signature électronique d'un agent de l'administration publique ;
- d) L'échange électronique de données dans des univers fermés de communication, selon accord spécifique des parties.

Section 2.- Identification des administrés et authentification de leurs démarches

Article 14.- Rôle de l'Office National d'Identification

L'Office National d'Identification a vocation naturelle à être prestataire de services de certification électronique. Il remplira à cet effet toutes les conditions prescrites par l'Arrêté d'Application de la Loi sur la Signature Electronique en vue de sa qualification par le Conseil National des Télécommunications. Une fois qualifié il fournira ses services exclusivement aux personnes physiques titulaires de la Carte d'Identification Nationale qui en feront la demande.

Il étudiera les voies et moyens et mettra en œuvre les ressources financières, techniques et humaines pour l'incorporation de la signature électronique des citoyens dans la Carte d'Identification Nationale.

Article 15.- Utilisation des dispositifs de signature électronique sécurisée.

Les administrés pourront faire usage de la signature électronique sécurisée pour s'identifier et authentifier leurs documents.

La signature électronique sécurisée devra être attestée par un certificat électronique délivré par un prestataire de services de certification électronique qualifié.

Article 16.- Utilisation d'autres systèmes de signature électronique.

Les entités administratives pourront déterminer et justifier, en tenant compte des données et intérêts en cause, les circonstances et conditions d'utilisation par les administrés d'autres systèmes de signature électroniques, comme la fourniture d'une information connue seulement des deux parties ou d'autres systèmes non cryptographiques.

Lorsque ces systèmes sont utilisés pour confirmer un renseignement, une proposition ou un projet de document remis ou produits par une entité administrative, celle-ci s'assurera de l'intégrité et de l'acceptation par les deux parties des documents électroniques concernés.

Lorsque cela s'avèrera nécessaire les entités administratives attesteront de l'existence et du contenu des formalités entreprises par les administrés pour lesquelles il aura été fait usage des moyens d'identification et d'authentification mentionnés dans le présent article.

Section 3.- Identification électronique des entités administratives

Article 17.- Identification des sites électroniques

Les sites électroniques utiliseront, pour s'identifier et garantir une communication sécurisée avec eux, des systèmes de signature électronique sécurisée attestées par des certificats électroniques qualifiés ou un moyen équivalent.

Article 18.- Système de signature électronique pour la procédure administrative automatisée

Pour l'identification et l'authentification de l'exercice de sa compétence lors d'une procédure administrative automatisée, chaque entité administrative pourra déterminer les circonstances d'utilisation des systèmes suivants de signature électronique :

- a) Le sceau électronique de l'entité administrative, attesté par un certificat électronique qualifié ;
- b) Le code sécurisé de vérification lié à l'entité administrative et dans ce cas à la personne signataire du document, permettant à tout moment le contrôle de l'intégrité du document à travers l'accès au site électronique correspondant.

Les certificats électroniques mentionnés à l'alinéa précédent utilisés pour attester des sceaux électroniques des entités administratives contiendront le numéro d'identification nationale et le titre de la fonction occupée par le représentant de cette entité.

La liste des sceaux électroniques utilisés par chaque entité administrative, de même que les caractéristiques des certificats électroniques et des prestataires de service de certification électronique qui les délivrent, seront publiques et accessibles par des moyens électroniques. De plus, chaque entité administrative adoptera les mesures adéquates permettant la vérification de ses sceaux électroniques.

Article 19.- Signature électronique des agents de l'administration publique.

Sans préjudice des dispositions des articles 17 et 18 de la présente loi, l'identification et l'authentification de l'exercice de la compétence d'une entité administrative, lorsque cette dernière utilise des moyens électroniques, s'effectuera à travers la signature électronique de son personnel selon ce qui est dit ci-après.

Chaque entité administrative pourvoira des agents déterminés en dispositifs sécurisés de création signatures électroniques, lesquels identifieront conjointement le titulaire du service envisagé et l'entité administrative à laquelle il appartient.

Article 20.- Echange électronique de données dans des environnements fermés de communications

Les documents électroniques transmis à l'intérieur d'environnements fermés de communications établis entre entités administratives seront réputés authentiques et aptes à identifier les expéditeurs et les destinataires selon les conditions établies dans le présent article.

Lorsque les émetteurs et les destinataires appartiennent à la même entité administrative, celle-ci déterminera les conditions et garanties d'utilisation. Au minimum sera établie la liste des émetteurs et destinataires autorisés et la nature des données susceptibles d'échanges électroniques.

Lorsque les parties à l'échange de données proviennent d'entités administratives différentes, les conditions et garanties mentionnées à l'alinéa précédent feront l'objet d'une convention.

Dans tous les cas la sécurité de l'environnement fermé de communications et la protection des données transmises devra être garantie.

Section 4.- De l'interopérabilité, de l'accréditation et de la représentation des administrés

Article 21.- Interopérabilité de l'identification

Les certificats électroniques émis par des prestataires de services de certification qualifiés seront reconnus valides par l'administration publique.

Les systèmes de signature électronique utilisés et admis par une entité administrative, différents de ceux attestés par un certificat électronique qualifié, pourront être reconnus valides par d'autres entités administratives conformément aux principes de réciprocité et de reconnaissance mutuelle.

Le Conseil Supérieur de l'Administration et de la Fonction Publiques disposera d'une plateforme de vérification de la validité de tous les certificats électroniques émis dans le cadre de l'administration publique. Cette plateforme sera librement accessible à toutes les entités administratives. Chaque entité administrative pourra établir son propre système de vérification de certificats et signatures électroniques émis pour elle et ses agents.

Article 22.- Identification des administrés par un fonctionnaire public

Lorsque pour la réalisation d'une opération quelconque par les moyens électroniques, un administré ne dispose pas d'un des moyens d'identification prévus à l'article 13 de la présente loi, cette identification pourra être effectuée par un agent de l'entité administrative concernée à travers le dispositif sécurisé de création de signature électronique dont il est pourvu.

A cette fin l'administré devra s'identifier et accorder son consentement exprès, étant renseigné qu'il engage sa responsabilité civile et pénale en cas d'inexactitude des renseignements fournis.

Chaque entité administrative maintiendra une liste actualisée des agents habilités à l'identification des administrés prévue dans le présent article.

Article 23.- La délégation de pouvoirs et de signature

Sans préjudice de ce qui est dit à l'article 13 alinéa 3, les agents d'une entité administrative pourront, dans le cadre des transactions et procédures utilisant des moyens électroniques, utiliser la procédure de la délégation telle qu'elle est prévue aux articles 162 à 170 du Décret du 17 mai 2005 sur l'Administration Centrale de l'Etat. Les administrés et les autres entités administratives pourront à tout moment requérir la preuve de cette délégation qui devra leur être fournie.

CHAPITRE III.- DES REGISTRES, COMMUNICATIONS ET NOTIFICATIONS ELECTRONIQUES

Section 1.- Des registres

Article 24.- Les registres électroniques

Les administrations publiques créeront des registres électroniques destinés à la réception et à la remise des requêtes écrites et communications.

Les registres électroniques pourront recevoir :

- a) Des documents électroniques normalisés correspondant aux services, procédures et formalités déterminés lors de la création du registre, et respectant des formats préétablis ;
- b) Toute requête ou communication distincte de celles mentionnées ci-dessus adressée à un agent ou service de l'entité administrative détentricice du registre.

Chaque entité administrative tiendra au moins un registre électronique destiné à la réception de requêtes et de communications de toutes sortes adressées à cette entité administrative. Les entités administratives pourront conclure des conventions de collaboration stipulant l'utilisation des registres d'une entité administrative pour la réception des requêtes et communications destinées à une autre entité administrative.

Une circulaire du Premier Ministre établira les conditions dans lesquelles les registres physiques de diverses entités administratives nommément désignées seront numérisées et automatisées afin de permettre l'interconnexion de ces registres et l'accès par des moyens électroniques aux contenus enregistrés et la délivrance de copies des documents qui y sont contenus.

Article 25.- Création et fonctionnement

La création de registres électroniques sera annoncée au Journal Officiel « Le Moniteur » et dans les média de communication, et le texte du communiqué créant le registre électronique pourra être consulté sur le site électronique permettant l'accès au registre. Il précisera l'organe ou l'entité responsable de sa gestion, ainsi que les dates et heures officielles ainsi que les jours ouvrables.

La liste des requêtes ou communications mentionnées à l'alinéa 2 a) de l'article précédent pouvant figurer sur les registres électroniques figurera sur le site électronique d'accès au registre, ainsi que la possibilité d'admission des documents mentionnés à l'alinéa 2 b) du même article.

Les registres électroniques émettront automatiquement un accusé de réception consistant en une copie authentique de l'écrit, de la requête ou de la communication dont il s'agit, sur laquelle seront portés l'heure et la date de soumission et le numéro d'ordre de l'enregistrement.

Des documents pourront être joints aux écrits, requêtes ou communications pourvu qu'ils se conforment aux normes de format et de sécurité précisés dans les Schémas Nationaux d'Interopérabilité et de Sécurité. Les registres électroniques émettront des accusés de réception de ces documents qui en garantissent l'intégrité et l'acceptation des documents joints.

Article 26.- Calcul des délais

Le calcul des délais applicables tant aux administrés qu'à l'administration publique aura pour point de départ l'heure et la date officielles du site électronique d'accès au registre lors de la soumission des écrits, requêtes, communications ou documents et affichées sur les accusés de réception.

Les registres électroniques devront permettre la soumission des requêtes, écrits et communication tous les jours de l'année et durant les vingt-quatre heures du jour.

Aux fins du calcul des délais, la soumission des documents lors d'un jour férié ou non ouvert sera réputée réalisée la première heure du premier jour ouvrable suivant.

Section 2.- Des communications et notifications électroniques

Article 27.- Les communications électroniques

Les administrés sont libres de choisir le mode de communication qui leur convient dans leurs rapports avec l'administration publique sauf dans les cas où une norme législative exige l'utilisation d'un moyen non électronique. L'option choisie par l'administré ne le lie pas ; il pourra à tout moment opter pour un moyen différent de celui choisi initialement.

L'administration publique utilisera les moyens électroniques de communication dans ses rapports avec les administrés toutes les fois où ceux-ci l'auront requis ou y auront consenti expressément. La requête ou l'assentiment pourront être émis ou obtenus en tout état de cause.

Les communications utilisant des moyens électroniques seront valides et auront force probante à condition que soient garanties l'évidence de l'émission et de la réception, leurs dates, l'intégrité des contenus et l'identification indiscutable des émetteurs et des récepteurs.

Les entités administratives publieront au journal Officiel « Le Moniteur », dans la presse et sur leurs sites électroniques, les moyens électroniques que les administrés pourront utiliser dans leurs rapports avec elles.

Les exigences de sécurité et d'intégrité des communications seront adaptées au caractère des données échangées, en application du principe de proportionnalité et des règles de protection des données à caractère personnel.

Les entités administratives pourront, par avis motivé, exiger que certaines personnes physiques ou morales qui, en raison de leurs capacités financières ou techniques, de leur domaine d'activités professionnelles ou d'autres motifs pertinents disposent d'un accès permanent aux technologies de l'information et de la communication, communiquent avec elles exclusivement en utilisant des moyens électroniques.

Article 28.- La notification par les moyens électroniques

Une notification sera effectuée par un moyen électronique si l'intéressé a exprimé sa préférence pour ce moyen ou y a consenti, sauf ce qui est dit à l'article 27 alinéa 6 précédent. L'expression de cette préférence ou le consentement à l'utilisation de ce moyen pourront être émis ou obtenus en tout état de cause.

Le dispositif de notification indiquera à l'intéressé la date et l'heure de la disponibilité de l'acte ou de la chose objet de la notification ainsi que, celle de la possibilité d'accès à son contenu, et le moment où la notification sera réputée avoir été effectuée à toutes fins utiles.

Si dix jours francs après la date de disponibilité du document, l'intéressé n'y a pas accédé, la notification est réputée avoir été rejetée avec toutes les conséquences de droit, à moins que le destinataire n'établisse l'impossibilité technique ou matérielle d'y accéder.

Durant les diverses étapes de la procédure administrative, l'intéressé pourra requérir de l'entité administrative correspondante que les notifications ultérieures s'effectuent par des moyens non électroniques, sauf ce qui est dit à l'article 27 alinéa 6 précédent.

L'accès électronique aux contenus des procédures administratives produira les mêmes effets juridiques que la notification effectuée physiquement.

CHAPITRE IV.- DES DOCUMENTS ET ARCHIVES ELECTRONIQUES

Article 29.- Les documents administratifs électroniques

L'administration publique pourra valablement émettre par des moyens électroniques des documents administratifs pourvu qu'ils comportent une ou plusieurs signatures électroniques tel que prévu à la section 3 du chapitre II du titre II de la présente loi.

Les documents administratifs seront datés par des moyens électroniques lorsque cette exigence découle de la nature du document.

Article 30.- Copies électroniques.

Les copies réalisées par des moyens électroniques de documents électroniques émanant d'un administré ou de l'administration publique, que le format original soit maintenu ou non, seront considérées conformes à l'original avec les mêmes effets juridiques attachés à l'original, pourvu que le document original soit détenu par l'administration publique et que les renseignements sur la signature électronique ou à défaut sur le sceau horodateur permettent d'en vérifier la concordance avec la copie.

Les copies réalisées par l'administration publique par des moyens électroniques, de documents émis originalement par l'administration publique sur support papier seront réputées conformes à l'original toutes les fois où la concordance avec le document original sera prouvée.

L'administration publique pourra obtenir les images électroniques de documents sous seing privés soumis par les administrés, dotés d'une validité juridique identique, par des procédés de numérisation qui en garantissent l'authenticité, l'intégrité et la conservation du document numérisé. La numérisation pourra s'effectuer de manière automatisée grâce au sceau électronique.

Une fois effectuées dans les conditions prévues au présent article, les copies électroniques des documents émis originellement sur support papier, ceux-ci pourront être détruits.

Les copies réalisées sur support papier de documents administratifs électroniques signés électroniquement seront considérées conformes à l'original à condition que sur la copie papier soit imprimé un code généré électroniquement ou d'autres dispositifs de vérification permettant de vérifier leur conformité à l'original grâce à l'accès aux archives électroniques de l'entité administrative d'où émane le document.

Article 31.- L'archivage électronique de documents

Pourront être archivés électroniquement tous les documents utilisés dans les procédures administratives.

Les documents électroniques contenant des actes administratifs affectant les droits ou les intérêts des administrés seront conservés sur des supports de même nature, dans le même format ou dans un autre, pourvu que soient assurées aux fins de reproduction l'identité et l'intégrité de l'information. Il sera toujours possible de transférer les données sur d'autres formats et supports qui en garantissent l'accès à partir d'applications différentes.

Les moyens ou supports sur lesquels sont archivés les documents devront contenir des mesures de sécurité assurant l'intégrité, l'authenticité, la confidentialité, la qualité, la protection et la conservation des documents archivés. L'identification des utilisateurs et le contrôle de l'accès seront garantis.

Article 32.- Les dossiers électroniques

Le dossier électronique est l'ensemble de documents électroniques relatifs à une procédure administrative, quel que soit le type d'informations contenues.

Le fichier des dossiers électroniques contiendra un index électronique signé de l'entité administrative. Cet index garantit l'intégrité des dossiers électroniques et permettra sa récupération chaque fois que nécessaire. Un même document électronique peut appartenir à des dossiers électroniques différents.

La mise à disposition du dossier électronique aura les mêmes effets que la remise à l'intéressé du dossier papier, sans préjudice du droit de l'administré à en obtenir des copies.

TITRE III : DE LA GESTION ELECTRONIQUE DES PROCEDURES

CHAPITRE I.- DISPOSITIONS COMMUNES

Article 33.- Utilisation des moyens électroniques

La gestion électronique de l'activité administrative s'effectuera en fonction des compétences légales de chaque entité administrative et de l'accomplissement des exigences formelles et matérielles qui les

régissent. En vue de la simplification administrative, sont encouragées l'application des moyens électroniques aux méthodes de travail et aux procédures administratives.

A ces fins, l'Etat veillera à la dotation adéquate des ressources et des moyens matériels pour le personnel administratif qui sera formé en conséquence.

Article 34.- Les critères de gestion électronique.

L'application des moyens électroniques aux procédures et services administratifs sera précédée d'un réexamen et d'une simplification des procédures et services où seront spécialement pris en compte les aspects suivants :

- a) La suppression ou la réduction de la documentation exigée des administrés grâce à son remplacement par des données ou des transmissions de données ;
- b) La prévision de moyens et d'instruments favorisant la participation, la transparence et l'information ;
- c) La réduction des délais et du temps de réponse ;
- d) La rationalisation des communications internes et de la distribution des charges de travail.

CHAPITRE II.- L'UTILISATION DES MOYENS ELECTRONIQUES DANS LE DEROULEMENT DES PROCEDURES

Article 35.- Mise en branle de la procédure par des moyens électroniques

La mise en branle d'une procédure administrative par un administré par des moyens électroniques requerra la disponibilité des modèles correspondants ou des dispositifs électroniques de requête sur le site électronique. Ces modèles et dispositifs devront être accessibles sans autres restrictions technologiques que celles découlant de l'utilisation des standards dans les termes prévus à l'article 4 i) et des critères de communication et de sécurité applicables en fonction des normes et protocoles nationaux et internationaux.

Les intéressés pourront joindre au dossier les copies numérisées des documents, dont la fidélité à l'original sera garantie par l'utilisation de signatures électroniques sécurisées. L'administration publique pourra solliciter de l'archive correspondante la comparaison des copies soumises. En cas d'impossibilité de la comparaison et de manière exceptionnelle, l'administration publique pourra exiger de l'administré la production du document ou de l'information originaux. La soumission de ces copies implique l'autorisation accordée à l'administration publique d'accéder et de traiter les informations personnelles qui y sont contenues.

En vue de faciliter et de promouvoir leur usage, les dispositifs normalisés de requêtes pourront inclure des vérifications automatiques de l'information soumise par rapport à leurs propres données archivées ou à celles archivées par d'autres entités administratives. Dans le même but, les dispositifs normalisés de requête pourront offrir un formulaire complété en tout ou en partie, que l'administré vérifiera ou complétera.

Article 36.- Instruction de la procédure utilisant les moyens électroniques.

Les applications ou systèmes d'information pour l'instruction des procédures par des moyens électroniques garantiront le contrôle du temps et des délais, l'identification des services chargés des procédures ainsi que le cheminement ordonné des données, et favoriseront la simplification et la publicité des procédures.

Les systèmes de communication utilisés pour la gestion électronique des procédures entre les différents services compétents devront respecter les exigences établies dans la présente loi.

Lorsque la participation des administrés est nécessaire à l'instruction de la procédure par des moyens électroniques, il sera fait usage des moyens de communication et de notification prévus aux articles 27 et 28 de la présente loi.

Article 37.- L'information des administrés sur l'état de la procédure.

Lorsque la procédure administrative est prise en charge complètement par des moyens électroniques, le service compétent mettra à la disposition de l'administré un service électronique à accès restreint où il pourra consulter, moyennant une identification appropriée, pour le moins l'état d'avancement de la procédure, sauf en cas de restrictions à l'information imposées par la loi ou les règlements. L'information sur l'état d'avancement de la procédure indiquera les actes posés, l'indication de leur contenu, ainsi que la date de leur réalisation.

Pour les autres procédures, il sera également établi un service électronique d'information qui en indiquera au moins l'état d'avancement et le service responsable.

Article 38.- Clôture des procédures par des moyens électroniques.

La clôture d'une procédure administrative par des moyens électroniques indiquera clairement l'identité du service et de l'agent compétents en utilisant l'un des moyens prévus aux articles 18 et 19 de la présente loi.

Dans les cas prévus par l'entité administrative compétente la clôture de la procédure et la notification y relative pourra se faire de manière informatisée.

Article 39.- Procédure administrative automatisée.

En cas de procédure administrative informatisée, seront préalablement prévus, le ou les services compétents pour la définition des spécifications, la programmation, l'entretien, la supervision, le contrôle de qualité, l'audit du système d'information et de son code source. Il sera également indiqué le service assumant la responsabilité en cas de contestation.

TITRE IV : COOPERATION ENTRE ENTITES ADMINISTRATIVES

POUR LA MISE EN ŒUVRE DE L'ADMINISTRATION ELECTRONIQUE

CHAPITRE I.- CHAMP INSTITUTIONNEL DE COOPERATION EN MATIERE D'ADMINISTRATION ELECTRONIQUE

Article 40.- Rôle du Conseil Supérieur de l'Administration et de la Fonction Publiques.

Le Conseil Supérieur de l'Administration et de la Fonction Publiques est l'organe technique de direction, de supervision et de coopération pour la mise en œuvre de l'administration électronique à tous les niveaux de l'administration publique au sens de l'article 2 alinéa 1 a) de la présente loi.

Il veillera à la réalisation des objectifs et des principes définis par la présente loi en s'assurant particulièrement des fonctions suivantes :

- a) Assurer la compatibilité et l'interopérabilité des systèmes et applications employés par les différentes entités administratives ;
- b) Préparer les plans et programmes conjoints de mise en œuvre de l'administration électronique.

Il pourra, en raison des matières traitées, associer à ses travaux les personnes, organisation ou associations qui en raison de leur objet ou de leurs compétences techniques peuvent apporter une contribution utile à la réalisation des missions du Conseil.

CHAPITRE II.- COOPERATION EN MATIERE D'INTEROPERABILITE DES SYSTEMES ET APPLICATIONS

Article 41.- Interopérabilité des systèmes d'information.

Lorsque les entités administratives utiliseront les systèmes d'informations dans leurs rapports avec les autres entités administratives et les administrés, elles le feront en appliquant les mesures informatiques, technologiques, organisationnelles et sécuritaires qui garantissent un niveau adéquat d'interopérabilité technique, sémantique et organisationnelle et qui évitent la discrimination entre les administrés en raison de leurs choix technologiques.

Article 42.- Schéma National d'Interopérabilité et Schéma National de Sécurité.

Le Schéma National d'Interopérabilité établira, en matière de sécurité, de conservation et de normalisation de l'information, des formats et des applications un ensemble de critères et de recommandations dont devront tenir compte les entités administratives dans leurs décisions en matière de technologie de manière à garantir l'interopérabilité.

Le Schéma National de Sécurité a pour objet d'établir dans le cadre de la présente loi la politique de sécurité dans l'utilisation des moyens électroniques ; il est constitué des principes de base et des conditions minimum requises permettant une protection adéquate de l'information.

Les deux schémas, après consultation des diverses entités administratives et sur proposition du Conseil Supérieur de l'Administration et de la Fonction Publiques, seront adoptés par arrêté du Premier Ministre et seront actualisés de manière permanente.

Dans l'élaboration des deux schémas, il sera tenu compte de la situation technologique des diverses entités administratives ainsi que des services électroniques déjà existants. A cet effet, l'utilisation de standards ouverts sera favorisée et, à leur défaut et de manière complémentaire, celle de standards les plus communément utilisés par les administrés.

Article 43.- Réseau de communications de l'administration publique.

Les diverses entités qui forment l'administration publique haïtienne adopteront les mesures nécessaires pour incorporer les technologies rendant possibles l'interconnexion de leurs réseaux respectifs afin de créer un réseau de communications interconnectant leurs systèmes d'information et permettant l'échange réciproque d'informations et de services.

Article 44.- Réseau intégré d'assistance à l'administré.

Les entités administratives concluront des accords de collaboration ayant pour objet de développer les moyens et instruments de mise en œuvre coordonnée et normalisée d'un réseau d'espaces communs ou de guichets uniques.

CHAPITRE III.- REUTILISATION D'APPLICATIONS ET TRANSFERT DE TECHNOLOGIES

Article 45.- Réutilisation de systèmes et d'applications.

Les entités administratives titulaires de droits de propriété intellectuelle sur des applications développées à leur intention, pourront, sans contrepartie, les mettre à disposition d'autres entités administratives, sans qu'il soit nécessaire de conclure un accord.

Les applications auxquelles se réfère l'alinéa précédent pourront être déclarées de sources ouvertes, lorsqu'il en découle une meilleure transparence dans le fonctionnement de l'administration publique ou une meilleure intégration des administrés à la société du savoir.

Article 46.- Transfert de technologies entre entités administratives.

Le Conseil Supérieur de l'Administration et de la Fonction Publiques conformément aux prescriptions du Schéma National d'Interopérabilité, en vue de favoriser le transfert de technologies, maintiendra un répertoire général actualisé des applications en usage dans l'administration publique en vue de leur réutilisation, fournira une assistance technique pour la libre réutilisation des applications et stimulera le développement d'applications, de formats et de standards communs présentant un intérêt particulier pour le développement de l'administration électronique. L'action dudit Conseil se déroulera dans le cadre des Schémas Nationaux d'Interopérabilité et de Sécurité.

TITRE V : DISPOSITIONS FINALES

Article 47.- Réunions d'organes collégiaux par des moyens électroniques.

Les organes collégiaux, notamment le Conseil des Ministres, les conseils d'administration d'organismes autonomes, pourront se réunir, délibérer et prendre des décisions par des moyens électroniques.

Seront respectées les règles établies par leurs régimes juridiques respectifs relatives à la convocation, à l'accès à l'information, à la communication de l'ordre du jour, à la fréquence des réunions, à la formulation des propositions et à la prise de décision.

Les minutes ou procès-verbaux tant écrits qu'électroniques constateront l'effectivité de la connexion, le nombre et l'identité des participants, les propositions soumises et leur connaissance par tous les participants, les décisions adoptées et leur connaissance par tous les participants.

Article 48.- Plan de mise en œuvre de l'administration électronique.

Les entités administratives promouvoir la formation de leurs agents à l'utilisation des moyens électroniques pour le développement de leurs activités propres.

Particulièrement, les agents recevront une formation spécifique et actualisée sur les conditions de sécurité de l'utilisation des moyens électroniques dans l'activité administrative, la protection des données à caractère personnel, le respect de la propriété intellectuelle et la gestion de l'information.

Dans les six mois suivant la publication de la présente loi, le Conseil Supérieur de l'Administration et de la Fonction Publiques élaborera un plan de mise en œuvre des moyens nécessaires dans le cadre l'administration centrale de l'Etat. Ce plan contiendra les estimations des ressources financières, techniques et humaines nécessaires à l'application de la présente loi, établira les délais d'exécution ainsi que les mécanismes d'évaluation et de contrôle de son application. Il sera homologué par un arrêté du Premier Ministre.

Article 49.- Langues officielles.

La présente loi garantit l'usage des deux langues officielles dans les rapports entre l'administration publique et les administrés par des moyens électroniques.

A cet effet, les sites électroniques des entités administratives permettront l'accès à leurs contenus et services en créole et en français. Leurs contenus, informations et formulaires seront également rédigés en créole et en français.

Les systèmes et applications utilisées dans la gestion électronique des procédures utiliseront l'une des deux langues officielles.

Article 50.- Adaptation de l'administration publique à l'administration électronique.

Dès l'entrée en vigueur de la présente loi, les entités administratives publieront la liste des procédures et services administratifs accessibles aux administrés par des moyens électroniques. Elles veilleront à ce que cette liste soit continuellement mise à jour.

Sur proposition du Conseil Supérieur de l'Administration et de la Fonction Publiques, un arrêté du Premier Ministre établira un calendrier d'adaptation progressive des procédures administratives à

l'utilisation des moyens électroniques. Il tiendra compte du plan de mise en œuvre mentionné à l'article précédent et des Schémas Nationaux d'Interopérabilité et de Sécurité.

Article 51.- Disposition d'abrogation.

La présente loi abroge toutes lois ou dispositions de lois, tous décrets ou dispositions de décrets, tous décrets-lois ou dispositions de décrets-lois qui lui sont contraires et sera exécutée à la diligence du Premier Ministre, du Ministre chargé de l'Économie et des Finances, du Ministre chargé de l'Intérieur et des Collectivités Territoriales, du Ministre chargé de l'Éducation Nationale de la Jeunesse et des Sports, du Ministre chargé de l'Agriculture et du Développement Rural et des Ressources Naturelles, du Ministre chargé de la Justice et de la Sécurité Publique, du Ministre chargé de la Condition Féminine et du Ministre chargé de la Santé Publique et de la Population chacun en ce qui le concerne.

Donné à la Chambre des Députés le

Donné

au

Sénat

le

.....

GTIC
Groupe de Travail sur les Technologies
de l'Information et de la Communication

ANNEXE 5 : TERMES DE REFERENCE

ETUDE DES LOIS SUR L'INFORMATION PUBLIQUE ET L'EXPLOITATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

1. CONTEXTE ET JUSTIFICATION

Les nouvelles technologies de l'information et de la communication sont présentées comme des outils révolutionnant les rapports sociaux. Elles abolissent la distance et le temps. S'ouvrent ainsi de nouvelles perspectives paradoxales des relations du citoyen avec l'administration publique, car grâce aux contacts virtuels la démocratie devient plus concrète. De même, les nouvelles technologiques offrent des moyens plus efficaces et rationnels de gouverner. Certains pressentent l'avènement de Big Brother de George Orwell, mais sans occulter ce risque certain, d'autres choisissent le pari d'appivoiser ces technologies au service du bien commun. D'où les deux acceptions de l'expression « *administration publique en ligne* » : gouvernement en ligne, meilleure gestion informatisée de l'administration publique, d'une part et d'autre part, l'administration en ligne, fourniture de services aux citoyens grâce à l'informatique et à l'internet.^{106,107}

Les nouvelles technologies de l'information induisent une nouvelle manière de commercer. Le commerce électronique n'est plus du tout marginal, les contrats se nouent, les paiements s'effectuent sans que les parties se rencontrent, et surtout sans que leurs échanges ne se matérialisent sur du papier. Cependant le besoin de sécurité juridique impose des mécanismes pour assurer force probante à des documents électroniques en cas de différend.

Pour répondre à ces défis, les législations nationales et organes de l'ONU, particulièrement l'UNIDROIT et la CNUDCI¹⁰⁸ ont produit des normes législatives et réglementaires qui légitiment l'usage

¹⁰⁶ LIRE BENYKHLEF KARIM, L'ADMINISTRATION PUBLIQUE EN LIGNE AU CANADA : PRECISIONS TERMINOLOGIQUES ET ETAT DE LA REFLEXION, *REVUE FRANÇAISE D'ADMINISTRATION PUBLIQUE*, NO. 110, 2004, 267-278

¹⁰⁷ IL EST INTERESSANT DE LIRE A CE PROPOS LA DEFINITION CONTENUE DANS LE E-GOVERNMENT ACT DE 2002 AUX ETATS UNIS (*E-GOVERNMENT ACT, 44 USCS §36 (2003)* SUR L'ADMINISTRATION EN LIGNE : « CELA SIGNIFIE L'USAGE PAR LE GOUVERNEMENT DES APPLICATIONS D'INTERNET BASEES SUR LES RESEAUX ET LES AUTRES TECHNOLOGIES DE L'INFORMATION, COMBINEES AVEC DES PROCESSUS METTANT EN ŒUVRE CES TECHNOLOGIES EN VUE DE RENFORCER L'ACCES A L'INFORMATION ET AUX SOURCES PUBLIQUES ET LEUR DELIVRANCE PAR LE GOUVERNEMENT ET LES DIFFERENTES AGENCES ; ET EN VUE D'AMELIORER LEUR MODE DE FONCTIONNEMENT PAR LA PROMOTION DE L'EFFICACITE, DE L'EFFICIENCE ET DE LA QUALITE ».

¹⁰⁸ COMMISSION DES NATIONS UNIES POUR LE DROIT DU COMMERCE INTERNATIONAL

de l'informatique et de l'internet dans les rapports privés et au sein de l'administration publique. Le GTIC doit, dans le cadre de sa mission, dresser une évaluation du droit haïtien en vue d'aligner notre législation dans le courant moderne. Cette évaluation n'est pas une fin en soi, mais vise à établir les termes de référence des travaux de production normative permettant à notre pays de rattraper son retard.

Un regard sommaire sur le secteur permet de comprendre aisément les principaux freins légaux ou administratifs à son plein épanouissement et par voie de conséquence les besoins en matière de législation dans le développement et l'exploitation des Technologies de l'Information et de la Communication en regard de l'Etat des lieux actuels.

a. Gouvernance globale du secteur :

a. Freins

- i. Législation datant de 1977 obsolète.
- ii. Méconnaissance des nouveaux services
- iii. Contrats octroyés de manière individuelle
- iv. Pas de normes préétablies pour l'octroi des autorisations
- v. Dépendance du régulateur face au pouvoir politique

b. Besoins

- i. Nouvelle législation où reconnaissance des nouveaux services
- ii. Garantie de la Neutralité technologique
- iii. Procédures claires et transparentes en fonctions de normes préétablies et sues de tous
- iv. Régulateur doté de compétences réglementaires et de police
- v. Régulateur plus autonome par rapport au pouvoir politique

b. Gouvernement en ligne

a. Freins

- i. Administration publique aveugle et muette
- ii. A l'intérieur d'un même ministère, pas de système de communication entre l'administration centrale et les services déconcentrés ou départementaux
- iii. Pas de lignes de communication sécurisées et cryptées pour les hauts échelons de l'administration
- iv. Pas d'intranet dans les ministères, entre la primature et les ministères, entre les ministères
- v. Dans les rares administrations où cela existe, pas de normes sur la conservation des données
- vi. Existence de bases de données différentes sur les citoyens (fiscale, immigration, circulation, armes à feu, greffes des tribunaux, assurances véhicules etc.).
- vii. Aucune communication entre les bases de données ce qui nuit à la fonction de renseignement.
- viii. Pas d'outils techniques ou juridiques pour traquer la cybercriminalité

c. Administration en ligne

a. Freins

- i. Prédominance du papier et des formulaires en dupli, tripli ...cata
- ii. Absence d'interactivité entre l'administration et l'administré

- iii. Centralisation géographique des services à la population (passeport, sociétés commerciales, assurances véhicules terrestres etc.)
- iv. Existence de diverses bases de données
- v. Ignorance par la loi des documents électroniques dans l'administration publique
- vi. Effort de la douane pour l'administration en ligne (formulaire et paiement en ligne)

b. Besoins

- i. Disponibilité de formulaires en ligne.
- ii. Possibilité de procédure complètement en ligne
- iii. Disponibilité de modèles d'actes usuels en ligne (baux, sociétés, mandat, vente de véhicule etc.)
- iv. Accès aux services publics essentiels de n'importe quel point du territoire
- v. Choix des pouvoirs publics des domaines d'administration en ligne. Par exemple, santé, douane, CONATEL, Ministère du Commerce, immigration etc.

d. Industrie TIC et Commerce Electronique

a. Freins

- i. Absence de force probante des documents électroniques
- ii. Nécessité du document électronique en autant d'exemplaires que de parties
- iii. Nécessité de la signature manuscrite

b. Besoins

- i. Doter le document électronique de la force probante
- ii. Législation sur le commerce électronique
- iii. Législation sur la signature électronique
- iv. Réglementation des tiers de certification

1. OBJECTIF GLOBAL DE L'ETUDE

L'objectif global de l'étude est d'évaluer l'ensemble du cadre légal haïtien relatif à l'information publique et l'exploitation des Technologies de l'Information et de la Communication à des fins de développement économique et social et de proposer une loi-cadre et les textes d'application appropriés.

2. OBJECTIFS SPECIFIQUES

Au regard de cet objectif global, les objectifs spécifiques suivants sont définis :

- Procéder à l'évaluation des besoins du secteur des Technologies de l'Information relatifs à un cadre normatif, légal et institutionnel eu égard aux domaines suivants : gouvernance du secteur, gouvernement en ligne, administration en ligne
- Rédiger le cadre légal et les textes d'application qui s'imposent et adapter les textes légaux existant au nouveau cadre proposé.

3. RESULTATS ATTENDUS

Les résultats attendus de l'étude sont :

1. Une proposition de loi-cadre sur l'information publique et l'exploitation des Technologies de l'Information et de la Communication pour le développement économique et social, le gouvernement et l'administration en ligne.
2. Une proposition de cadre institutionnel incluant :
 - a. Une actualisation de la loi créant et organisant l'instance de régulation,
 - b. Une loi créant ou définissant l'instance publique en charge des missions d'exploitation du secteur par l'Etat Haïtien
3. Une proposition de lois d'application pour la promotion de l'industrie des TIC, du commerce électronique et des activités d'externalisation liées aux TIC en Haïti incluant notamment :
 - a. Une adaptation à l'environnement haïtien de la loi-type de la CNUDCI sur le commerce électronique
 - b. L'adoption par le Parlement de la loi sur la signature électronique. Ce texte est déjà prêt
 - c. Un Arrêté d'application et cahier de charges pour tiers de certification
 - d. Les Conditions de reconnaissance d'organismes de certification étrangers (ceci est nécessaire dans le cadre du commerce international)
 - e. Le renouvellement du principe de la neutralité technologique et les conditions dans lesquelles ce principe doit être ignoré
4. Une proposition de loi de protection du citoyen dans l'espace cybernétique incluant notamment :
 - a. Une définition des infractions cybernétiques,
 - b. Les conditions d'accès des autorités publiques, policières et/ou judiciaires aux données détenues par les FAI,
 - c. La licéité et les limites de la cryptographie dans les rapports privés,
 - d. La création d'une autorité chargée de la sauvegarde des données personnelles ou le renforcement de l'Office de Protection du Citoyen
 - e. Les conditions de communication ou de divulgation des données personnelles conservées par les instances publiques ou privées
 - f. Etendue de l'obligation de confidentialité à la charge des tiers de certification
 - g. L'accès du citoyen aux données conservées à son sujet
5. Une proposition de cadre d'organisation d'un système de « gouvernement en ligne » incluant notamment :
 - a. L'Interopérabilité et l'interconnexion des bases de données de certains services publics (sécurité publique, et renseignement)
 - b. La validité des visioconférences (réunion de cabinet, décisions et instructions données lors de ces réunions)
 - c. L'authenticité de l'identification des intervenants (p. ex. biométrie) tout en préservant le principe de neutralité technologique
 - d. La conservation des données et des échanges
 - e. L'accès du public et du parlement aux archives informatiques.
6. Une proposition de cadre d'organisation d'un système « d'administration en ligne » incluant notamment :
 - a. L'établissement de la preuve des documents électroniques en matière administrative
 - b. La signature et le paiement électroniques en matière administrative et la protection des données personnelles,

- c. Un système d'identification des Haïtiens pouvant facilement être mis à jour et utilisé dans les rapports entre l'administration en ligne et les citoyens
7. Un inventaire exhaustif des lois d'application nécessaires à une bonne exploitation des TIC pour le développement économique et social et le fonctionnement en ligne du gouvernement et des services de l'administration publique

4. METHODOLOGIE

La méthodologie proposée pour la réalisation de l'étude consiste à faire un état des lieux à travers :

- une recherche documentaire dans les administrations publiques
- une recherche empirique à partir de visites de terrain, d'observations et d'entretiens ciblés avec des personnes ressources et, les prestataires et les bénéficiaires des services et soins de santé.

Activités spécifiques

Aux fins de l'étude, le contractant devra :

- constituer et animer sa propre équipe de compétences
- consulter toute la littérature déjà consacrée aux questions de l'étude
- collecter par des entretiens ou tout autre moyen jugé approprié l'ensemble des données nécessaires pour atteindre les objectifs et résultats de l'étude
- produire dans les délais indiqués les rapports initial, intermédiaire et final dont les dates de livraison seront déterminées en concertation avec le consultant.

Entrevues ou réunions programmées et à planifier

- Réunions avec les directeurs et autres responsables des institutions publiques
- Réunions avec des "focus groups" de représentants du secteur privé et des opérateurs, industriels, des télécommunications et des banques, et ceux de la Société civile, pour mieux cerner leurs attentes ;
- Rencontres éventuelles avec d'autres interlocuteurs à identifier.

5 - PRODUIT FINAL

L'Étude sera sanctionnée par un Rapport d'analyse s'articulant autour des principaux domaines d'activités définis plus haut accompagnant l'ensemble des textes de lois prévus plus haut.

L'Étude s'ouvrira par un résumé synthétique des résultats essentiels et le rappel de l'approche méthodologique et des procédures adoptées

6. COMITE DE SUIVI

Le suivi de la réalisation de l'Étude sera assuré par le comité exécutif du GTIC qui sera étroitement assisté par le comité légal du GTIC.

Ce comité technique aura pour tâche d'orienter techniquement l'Équipe en charge de l'étude, de valider les outils et l'approche méthodologiques proposés ainsi que le Rapport d'analyse

7 - PROFIL DU CONSULTANT

Les consultants doivent remplir les conditions suivantes :

- une bonne connaissance de l'environnement juridique haïtien dans le domaine des Technologies de l'Information et de la Communication,
- une bonne expérience en matière de conduite d'études et de recherches.
- une bonne connaissance du secteur des TIC en Haïti et dans le monde.

Le consultant présentera une offre technique et financière pour la conduite et la réalisation de l'étude tout en précisant les compétences dont il dispose, ainsi qu'un chronogramme indiquant les différentes étapes de l'étude. Les rapports d'étapes feront l'objet de présentation devant le comité légal et le comité exécutif du GTIC.

8 - CHAMP DE L'ETUDE

L'étude s'étend aux besoins de l'ensemble du pays dans toutes les activités liées ou connexes au secteur des TIC ou de la gestion de l'information publique. Cependant il convient de noter qu'elle doit prendre en compte certaines spécificités telles que les zones rurales et urbaines, les groupes cibles tels que les jeunes, les femmes, les hommes, les enfants, les personnes à besoin spéciaux.

9 - DUREE DE L'ETUDE

L'étude durera cinq (5) mois au maximum à compter de la date de signature du contrat avec le consultant.

Un premier rapport d'étape sera donné au plus tard à la fin de novembre 2009. Un atelier de restitution du rapport d'étape se tiendra en décembre 2009. Le dépôt du rapport final en dix (10) exemplaires et en version électronique est prévu pour janvier 2010.

10- COMMANDITAIRE ET RESPONSABLE DE L'ETUDE

Cette étude a été commanditée par la Commission Présidentielle appelée « Groupe de Travail sur les Technologies de l'Information et de la Communication » ou GTIC.

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

ANNEXE 6 :
RAPPORT DE L'ATELIER SUR LES LOIS CONCERNANT LA
SIGNATURE ELECTRONIQUE ET LES ECHANGES
ELECTRONIQUES
(17 décembre 2009)

Introduction

La signature électronique est un concept nouveau pour Haïti. Il convient essentiellement de réguler les principes qui la sous-tendent. Ces principes doivent cependant respecter les normes internationales en la matière et s'adapter à la situation particulière du pays. Les lois soumises par le Président de la République sur la signature électronique et les échanges électroniques sont donc, à ce propos, dépouillées, décortiquées, analysées au cours d'un atelier organisé par le Groupe de Travail sur les Technologies de l'Information et de la Communication (GTIC) et animé par le Group Croissance, le jeudi 17 décembre 2009, à la salle Ramier de l'Hôtel Montana.

Les points qui ont constitué le menu du programme sont les suivants :

- objectifs poursuivis par le GTIC dans le cadre de l'atelier ;
- Définition d'un cadre légal pour les Technologies de l'information et de la communication (TIC) ;
- exposé des trois textes de lois ;
- rapport des groupes de travail.

Il est à souligner que le nombre des participants présents à cette rencontre a dépassé les attentes des organisateurs, étant donné « l'aridité » du sujet – pour reprendre le terme d'un des intervenants – ponctué de nombreux termes techniques, comme *e-commerce*, *e-information*, etc. Le thème a été toutefois abordé franchement et simplement. En tout premier lieu, M. Kesner Pharel du Group Croissance a présenté les objectifs visés dans l'organisation d'un tel atelier.

1. Objectifs du GTIC

Pour souligner l'importance de lois devant régir ce type d'échange transactionnel sous l'obédience d'un régulateur, l'exemple avancé par M. Pharel est celui d'un match de football. Comment, en effet, faire jouer deux équipes sans arbitre ? En général, l'arbitre est celui (ou celle) que l'on remarque le moins sur le terrain de jeu. Il n'en demeure pas moins un élément central et décisif dans le déroulement du jeu. D'où la nécessité de lois cadre mais surtout d'une instance devant veiller à leur exécution mais surtout à leur respect.

Ceci dit, le premier objectif visé est de porter les participants à réfléchir autour des textes de loi présentés dans le cadre de cet atelier – en l'occurrence ceux sur la signature électronique et les échanges électroniques –, à les analyser pour en déterminer les forces et les faiblesses et à faire des propositions sur la manière de les améliorer. Il conviendra ensuite d'envisager comme intégrer normalement Haïti dans le mouvement global des échanges électroniques¹⁰⁹.

Les objectifs étant définis, la présentation des différents partenaires associés à cet atelier de travail et de la thématique s'imposait...

2. Cadre légal pour les TIC

Cette tâche incombait à M. Patrick Attié, coordonnateur du GTIC qui s'est d'abord fait le devoir de présenter au nom du comité des remerciements aux différents partenaires associés au projet ainsi que diverses personnalités ayant contribué à la réalisation de l'atelier.

M. Attié a en outre souligné que la signature électronique est indissociable du commerce électronique. Il faut donc la mise à jour du cadre légal en vue de son application... Il a plaidé en faveur de suivis et de recommandations pour un modèle d'application moderne et adapté. Ce cadre légal permettra l'intégration effective du pays dans le monde du commerce électronique. Il concernera, entre autres, la gouvernance publique, les processus intra-gouvernementaux et la mise en place d'un partenariat avec l'université... Certains éléments sont essentiels à ce propos, notamment : environnement physique approprié, élaboration de termes de références, association avec des partenaires tant locaux qu'étrangers... Il est en fin de compte proposé au pays un nouvel écosystème pour la création d'emplois à tous les niveaux.

¹⁰⁹ ON NOTERA LA GENERALISATION DU TERME « ECHANGES ELECTRONIQUES », SOULIGNEE PAR LES INTERVENANTS EN LIEU ET PLACE DE « COMMERCE ELECTRONIQUE », CE DERNIER N'ETANT QU'UN ASPECT DES ECHANGES ELECTRONIQUES.

Il faudra déterminer, en analysant le projet de législation, son utilité économique et sociale, l'identification des éléments susceptibles de faire fonctionner le système ainsi que l'équité dans l'accès aux services proposés.

3. Présentation des textes de loi

« Considérez un vendeur de café dans un petit village du pays. Au lieu de laisser son produit à un spéculateur comme, de fait, cela se passe habituellement, il fait appel à son fils afin de consulter le prix du café sur le marché mondial avec son portable et, ainsi, traiter directement en ligne avec l'acheteur qui se trouve à l'étranger... »

À travers cet exemple, M^e Bernard Gousse a introduit le principe de l'échange électronique mais surtout les avantages et les transformations qui en découlent. Une autre illustration des avantages de ce genre d'activité concerne l'étudiant qui s'inscrit, paie ses études, soumet ses devoirs en ligne... M^e Gousse a cité le cas, il y a trois ans, d'un étudiant qui a pu, en France, soutenir sa thèse de doctorat en ligne et recevoir son diplôme...

D'un autre côté, l'intervenant a montré les conséquences fâcheuses qui peuvent dériver d'une absence d'interconnexion entre, par exemple, deux villes du pays – comme c'est d'ailleurs le cas – au regard de base de données qui peut être disponible dans une région quelconque sans que l'on puisse accéder dans telle autre région. Ainsi peut-il en être d'un malfaiteur qui s'enfuit de sa ville natale – disons Jérémie – pour viol mais qui, arrivé au Cap-Haïtien, se porterait candidat à des élections locales.

Sur le plan international, a poursuivi M^e Gousse, il est démontré par exemple qu'aux États-Unis d'Amérique le « lundi cybernétique » (*Cyber Monday*) qui a suivi le « vendredi noir » (*Black Friday*) a engendré davantage de transactions que ce dernier. D'où la nécessité, pour les juristes, d'encourager ces genres de transactions en les plaçant dans un cadre légal et sécurisé. Ainsi, on trouve-t-on une législation sur le commerce électronique dans les pays de l'Amérique, notamment en République Dominicaine, notre plus direct concurrent en matière d'échanges commerciaux mais aussi dans de nombreux autres pays,

Faire donc en sorte que les Haïtiens communiquent sur le plan commercial serait un excellent moyen de désenclaver le pays qui s'apprête à intégrer le Marché et l'Économie Unique de la Caraïbe¹¹⁰. « Il y va du développement économique du pays », selon M^e Gousse.

Tout ce qui précède prouve combien il est important que le pays se mette au pas en matière d'échanges électroniques et adapte en conséquence sa législation particulièrement celle relative à la preuve en vue de sécuriser les engagements pris sur la toile, soutient M. Gousse.

¹¹⁰ EN ANGLAIS CARIBBEAN SINGLE MARKET AND ECONOMY (CSME)

3.1. L'effet de signature

Une double fonction s'applique à toute signature apposée au bas d'un document. Elle permet en effet d'identifier la personne qui signe et d'avoir en même temps une preuve de son consentement à l'échange en question.

« Sans adoption de textes, le pays sera un 'PMA numérique' »

M^e Bernard Gousse a expliqué que certaines exigences sont difficilement observables dans le contexte électronique. Ainsi, il est impossible d'obtenir la signature manuscrite d'une personne consentante, lors d'un échange électronique. L'exemple d'une banque de commerciale offrant des services en ligne condamnée par la justice de restituer, à tort ou à raison, une importante somme d'argent à un client – en dépit de preuves d'échanges électroniques fournies par cette banque avec ledit client –, montre bien la précarité des échanges en ligne, eu égard au droit civil.

Il faut en conséquence établir des dispositions de loi pour les échanges qui s'effectuent en ligne. Une obligation dont nombre d'États sont conscients, en initiant des principes régulateurs de ces échanges. Ce qui n'est pas encore le cas chez nous. Or, sans adoption de textes, a soutenu M^e Gousse, le pays sera un « PMA numérique ».

M^e Gousse a soulevé à ce propos deux importantes questions, à savoir :

- a) Comment faire ?
- b) Qu'est-ce qui a été fait ?

À la première question, il est suggéré de s'inspirer pour la législation haïtienne des meilleures pratiques internationales pour la sécurité juridique, la neutralité technologique et la garantie de la conservation et des échanges des données, la garantie de l'identité des échangeurs ainsi qu'une garantie de confidentialité.

En ce qui a trait aux modèles déjà existants dans le domaine, il faut chercher sur le plan international. Il existe le modèle européen, le modèle américain, mais surtout la loi type de la CNUDCI sur le commerce électronique dont s'inspire la grande majorité des législations en la matière. A noter également que la question de la signature électronique et de la force probante des documents électroniques est fait l'objet de l'attention des législateurs. En République Dominicaine toutefois, une même loi traite de la signature électronique, et du commerce électronique. Pour Haïti, il est proposé de modifier les règles sur le droit de la preuve dans le Code civil en vue d'établir l'équivalence entre le document électronique et celui sur support papier, et de définir les exigences devant être remplies par la signature électronique pour qu'elle remplisse les mêmes fonctions que la signature manuscrite ; c'est-à-dire que la signature garantisse à la fois l'identité de l'auteur du document et l'intégrité du document produit par rapport à celui qui a été signé. Un projet d'arrêté vient préciser davantage les exigences applicables pour la qualification des prestataires de services de certification électronique, exigences à la fois techniques et juridiques ainsi que les conditions d'admissibilité des certificats émanant de prestataires situés en dehors d'Haïti.

3.2. Un cadre régulateur

À ce propos, il y a nécessité de faire appel à des prestataires de service en certification électronique. Mais il faudrait une autorité d'État pour contrôler le fonctionnement desdits prestataires de service. Et l'intervenant d'indiquer qu'il faudrait peut-être opter pour un organisme déjà existant plutôt que d'en créer un nouveau. L'organisme d'État le plus apte à remplir cette fonction, moyennant un élargissement de ses compétences, est donc le Conseil National des Télécommunications (Conatel).

Avant la répartition en groupes de travail, l'assistance invitée à réagir notamment par des questions et/ou commentaires ne s'est pas fait prier, qui partageant ses préoccupations quant à l'instance de contrôle suggérée¹¹¹, qui évoquant le problème de la vérification des signatures numériques représentées dans les passeports haïtiens, qui se demandant jusqu'à quel niveau on pourra penser à la matérialisation de certains actes au niveau de la commercialisation, et qui se questionnant sur le type de média à utiliser pour des échanges électroniques...

Maître Bernard Gousse a montré, en cela aidé par d'autres, que la création d'un service spécial en tant que régulateur dans le cadre des échanges électroniques serait trop coûteuse et qu'il vaudrait mieux exploiter les avantages offerts par une institution susceptible de remplir ce rôle, en redéfinissant son cadre de fonctionnement. Le rôle du Conatel serait toutefois confiné à des activités de contrôle de la légalité des prestataires de service de certification électronique et de leur respect des normes établies dans ce cadre. En ce qui a trait au facsimilé de signature retrouvé dans les passeports, suite à question émanant de l'assistance, M^e Gousse a reconnu en effet qu'il peut être imité par n'importe qui a accès à la machine. Ce document n'offre donc aucune sécurité quant à l'authenticité des signatures de celui qui délivre et celui qui en est le détenteur à moins que le Service d'Emigration et d'Immigration présente la garantie que l'accès à la machine est strictement contrôlé. Cette question a permis de préfigurer la présentation qui aura lieu bientôt relativement au projet de législation sur la gouvernance et l'administration en ligne.

4. Rapports de groupes

La tâche des groupes en atelier a été grandement facilitée par la préparation préalable, par les organisateurs et organisatrices, d'une fiche de rapport (voir Annexe II) permettant de progresser dans les réflexions autour de points essentiels prédéterminés en rapport aux thèmes débattus. Quatre

¹¹¹ DANS LE CAS PAR EXEMPLE D'UN PROGRAMME D'ÉDUCATION A DISTANCE, LES FINALITES SONT PLUTOT LIEES A LA FORMATION INTELLECTUELLE ET NON AUX MOYENS ELECTRONIQUES, AUQUEL CAS LA REGULATION INCOMBERAIT PLUTOT AU MINISTERE DE L'ÉDUCATION NATIONALE...

groupes de travail ont été constitués suivant les instructions de M. Pharel, avec la désignation d'un facilitateur pour chacun des groupes, dont les réflexions sont ensuite présentées en plénière par un rapporteur désigné au sein des groupes respectifs.

Les membres de chaque groupe devaient réfléchir sur différents thèmes, notamment :

- le cadre institutionnel devant jouer un rôle de régulateur pour les échanges électroniques ;
- les prestataires de services de certification ;
- la sécurité des échanges ;
- les appréhensions, contraintes et craintes majeures relatives à la mise en place d'un tel système ;
- les opportunités identifiées dans différents secteurs pour améliorer les textes.

La méthodologie à suivre dans le cadre de ces réflexions consistait à déterminer les priorités, à proposer les actions à entreprendre et à identifier des acteurs et des partenaires clés devant contribuer au bon fonctionnement du système.

4.1. Cadre institutionnel en tant que régulateur

En dépit de certaines réserves formulées quant à la capacité du Conatel à assumer cette fonction de régulateur, il reste entendu qu'en redéfinissant le rôle de cette institution et en en modifiant la loi organique, l'on pourra faire l'économie d'une nouvelle instance avec tous les coûts et le temps que sa mise sur pied entraînerait. Du nombre des actions possibles, dans ce cas, on trouve un agencement de la légalisation sur la vie privée et l'élargissement du cadre de l'institution régulatrice. D'autres acteurs pourraient être associés à ce nouveau système, dont l'ONI et une institution privée, entre autres.

4.2. Prestataires de service de certification électronique

L'emphase est mise ici sur le principe de la concurrence d'où une pluralité de prestataires est préférable à un éventuel monopole étatique. Toutefois, pour maintenir une certaine uniformisation du service certains ont suggéré de centraliser la base de données nécessaires à ce type d'activité. Il est proposé d'étendre le champ d'activités de l'Office national d'identification (ONI) et d'en faire un prestataire de service central.

4.3. Sécurité des échanges

Ce point soulève un certain nombre de questionnements relatifs aux sujets engagés dans un échange électronique. Comment, par exemple, trouver une équivalence pour une personne aveugle ou analphabète qui se fait accompagner ? La question de la sécurité se pose également d'un double point

de vue physique et logistique. Elle revêt alors plusieurs aspects, notamment, sur les plans normatif, technique et administratif. Il faudra, en termes d'action, s'assurer de la fiabilité des différents réseaux mis à profit et régler le problème de l'infrastructure au sein des diverses institutions concernées. Une loi contre la cybercriminalité est incontournable pour une meilleure garantie de la sécurité des échanges. Parmi les acteurs et/ou partenaires clés susceptibles d'assurer un système sécurisé, on retrouve l'ULCC, l'UCREF le MEN, entre autres.

4.4. Appréhensions et contraintes

Le problème d'infrastructure ainsi qu'un manque de vulgarisation du système, entre autres, peuvent s'ériger en obstacles majeurs à son bon fonctionnement. Beaucoup reste donc à faire pour une instrumentalisation au niveau des tribunaux, dans le cadre de la recherche de l'authenticité d'une pièce, pour la hiérarchisation de la mise en place des textes d'application, le mécanisme de mise à jour des données, etc. Il est essentiel de passer par l'éducation, la formation et élaborer des documents cadres sur la question de la communication via ordinateurs. Une réduction des taxes en acquisition technologique s'impose également, en vue d'éviter des coûts onéreux pour un service de certification électronique.

4.5. Pour améliorer les textes de loi

Une traduction créole du document pourrait en faciliter la compréhension. Il faut également donner des définitions plus précises aux termes purement techniques.

5. En guise de conclusion

Il était prévu au départ que M^e Gousse interviendrait également à la suite des rapports des groupes. Un choix judicieux à la lumière des clarifications apportées sur certains points. Tel est, par exemple, le cas de la proposition de l'ONI en tant que prestataire de service par excellence. S'il est reconnu que l'ONI peut remplir au même titre que d'autres la fonction de prestataire de service de certification, il ne peut remplir un rôle central. Car, en plus des citoyens haïtiens, d'autres personnes de nationalités différentes, ainsi que des personnes morales, auront besoin d'une certification électronique, ce qui va bien au-delà des attributions de l'ONI. Il est à préciser que les textes de loi prévoient de la concurrence au niveau de la prestation de services.

Pour ce qui a trait à la traduction des textes de loi en créole, M^e Gousse a estimé, à juste titre, que la meilleure démarche serait que le document soit de préférence écrit, parallèlement au texte français, en créole en faisant intervenir à la fois des spécialistes des questions juridico-légales et linguistiques.

La question de la cybercriminalité est assez préoccupante au point d'être inscrite dans l'agenda du GTIC quant à sa mission de travailler sur divers textes de loi. Toutefois, a estimé M^e Gousse, il ne suffit pas de voter des textes. Il faut essentiellement penser à la formation des cadres, des magistrats,

disposer de ressources humaines et techniques, ce qui constitue le vrai critère d'application des textes.

Quant à la question de la responsabilité des prestataires de services de certification, elle est de toute façon prévue dans les projets de lois et d'arrêté analysés, des sanctions administratives à l'encontre des prestataires, le Conatel étant à même de révoquer n'importe quelle qualification. Quant aux sanctions civiles, elles peuvent être puisées dans le droit commun de la responsabilité. Par ailleurs, certaines exigences techniques ne peuvent être que fonctionnelles pour respecter le principe de neutralité technologique. Aujourd'hui on utilise l'algorithme comme signature électronique mais il est fort possible que cela soit autre chose à l'avenir : identification par l'empreinte digitale, le timbre vocal ou l'iris.

Pour la question de la hiérarchie entre la preuve sur support papier et la preuve virtuelle, l'équivalence est déjà établie un peu partout dans le monde. Au système de la justice de déterminer laquelle de ces deux preuves est la plus fiable en fonction des circonstances, au cas par cas.

L'on ne mentionnera pas le terme conclusion à proprement parler, dans la mesure où cette séance autour de la signature électronique et des échanges électroniques n'est que le début d'un travail de réflexion auquel les responsables du GTIC accordent une importance capitale. En effet, un forum électronique est créé à cet effet sur le site internet du GTIC pour recueillir les commentaires et suggestions des uns et des autres autour de la signature et des échanges électroniques. En outre, une réunion de suivi est prévue, en vue de s'assurer de la prise en compte des recommandations faites autour de la question lors de l'atelier.

Liste des participants

1	ACHILLE	Thony	AGD
2	ADOLPHE	Hulzer	CNMP
3	AIME	Alberte	Group Croissance
4	ANDRE	Nick	Rapporteur
5	ATTIE	Patrick	GTIC
6	BOYER	Dominique	FONKOZE
7	BRUNO	Stéphane	GTIC
8	BRUTUS	Hugue Herold	MCN
9	CANAL	Frantz	TNH
10	CASSION	Henry	GTIC
11	CHARLESTON	Giles	FONKOZE
12	CHILOSI	Paolo	GTIC
13	COQ	Michelet Staël	MISCO-PRO
14	DE BEES	Pierre	GWC
15	DIEUDONNE	Richard	ESCALDI
16	DOLMA	Anita	Avocate
17	DOMOND	Gregory	Journaliste
18	DUBOIS	Jean Baden	GTIC
19	EDMOND	José	MCN
20	EDWARD	Ruth	PNUD
21	ELYSEE	Jaunasse	GTIC
22	ETIENNE	Tayana	GTIC
23	FILS-AIME	Madelain	OMRH
24	FOURON	Kettly	Franco
25	FRANCK	Marie-Antoine	Unibank
26	FRERRE	Ernest	Aquinter
27	GOUSSE	Bernard	GTIC
28	GREATHOUSE	Greta	USAID / HIFIVE
29	HOGARTH	Marilyn	Cabinet Sales
30	JEAN-BAPTISTE	Schiller	GTIC
31	JEAN-DAVID	Rodney	CONATEL
32	JOLIVERT	Jean Kellens	AIC
33	JOSAPHAT		MCI
34	LABAZE	Alzimé	Radio
35	LABBE	Paula	Group Croissance
36	LAFORTUNE	Max Stanley	Avocate
37	LAMBERT	Jean Osselin	Immigration
38	LAMOTHE	Guy	CFI
39	LAMOTHE	Marline	USAID
40	LOUIS	Gregory	LEVIER/DID
41	MAIGNAN	Jean-Marie	CONATEL
42	MC KENZY	Louis Denis	TBD
43	MENARD	Giovanna	GTIC
44	MILLET	Jean	Unibank
45	MOISE	Jeff	DPC
46	MYRTHIL	Gilbert	ONI
47	NOEL	Raymond	GTIC
48	OLIUS	Gary	BID
49	PEREIRA	Ralph	GTIC
50	PHAREL	Kesner	GTIC
51	PIERRE-LOUIS	Frantz	MCI
52	RICHARD	Dieudonné	TBD

53	ROSEMOND	Edgard	USAID
54	SALES	Jean Frédéric	Cabinet Sales
55	SALNAVE	Bertrand	Capital Bank
56	SAM	Marlène	GTIC
57	TERNIER	Paul Edouard	Cabinet Sales
58	TIPPENHAUER	Hans	Fondation Espoir
59	VERCH	Michaël	CompHaiti
60	VILGRAIN	Philippe	Unibank

Fiche de rapport pour les travaux en groupes

Secrétaire/Rapporteur :		Facilitateur :
Noms participants/Institutions :		
Thème(s) retenu(s) : (a) Cadre institutionnel/Régulateur ; (b) Prestataires de services de certification ; (c) Sécurité des échanges ; (d) Appréhensions, contraintes et craintes majeures ; (e) Opportunités identifiées dans les secteurs respectifs pour améliorer les textes.		
Problème Prioritaire 1	Action 1	Acteurs et partenaires clés
Problème Prioritaire 2	Action 2	Acteurs et partenaires clés
Problème Prioritaire 3	Action 3	Acteurs et partenaires clés
Problème Prioritaire 4	Action 4	Acteurs et partenaires clés
Problème Prioritaire 5	Action 5	Acteurs et partenaires clés
Délai et modalités de mise en œuvre et coordination des recommandations, s'il y en a :		
Au moins un volontaire du groupe à assister a une réunion de suivi ?		

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

**ANNEXE 7 :
Rapport de Mission – Dr Ivar Tallo, eGA, avril – mai 2009,
Port-au-Prince**

Report: how to start the e-governance process in Haiti

By Ivar Tallo

CONTENTS

Executive summary:.....	126
Basic framework.....	127
UNPAN evaluation model.....	127
Situation.....	128
Political process.....	128
Policy process:.....	130
Immediate recommendations:.....	131
Project proposals:.....	131
Training for a group of key officials.....	131
Taking the development past central government to the local level.....	131
Creating the e-cabinet.....	132
Mobile based warning system – crisis communication system.....	132
Covering the country with wireless.....	133
Creating basic engagement of schools with ICTs.....	133
Creating population registry.....	133
Creating an e-gov unit.....	134
Creating an Haitian ICT conference.....	134
Government finances on-line.....	134
Providing legislation on-line free of charge.....	134
Introducing transparency legislation.....	134
Other recommendations.....	135
Possible time-line.....	136

"A TOUCH OF E-MAGIC TO SPICE UP THE TRADITIONAL VOO-DOO"

EXECUTIVE SUMMARY:

The following paper is the result of a 5 day mission to Haiti in April/May 2009. The primary objective was to provide practical advice to the government on the question of using ICTD and e-governance for the modernization of Haiti.

The overall situation is not easy and one would first need to answer the question whether it is possible and desirable in this situation to try to put stress on the ICTs when the grave questions of poverty have not been solved. However, ICTs can play a very positive role for the development of a country and it could be seen like fishing rod and hooks handed to a sizeable proportion of population instead of feeding them with fish. Some of the recent data in Haiti tends to confirm this as witnessed by the rapid growth of mobile phone users or relatively high number of internet users compared to the general income levels.

The overall strategy for the government in this situation is clear, it has to create a momentum of change and use the deployment of ICTs as one of the means to convey the message to the whole population that the old days are over and that a major change is in the air. In fact, none of the donors can provide serious positive development impact (aside providing for general security) alone, this has to be done first and foremost by the country and its own institutions.

Because of the characteristics of the overall situation, it seems that the three basic steps that have to be taken are a) creating the connectivity; b) creating digital resources; and c) creating legal framework. All the process should be managed openly and flexibly as this corresponds to the prevailing practices and conditions where one needs to use multiple sources of funding and be very inventive to stretch the available resources.

To help this process on the way, the current paper provides an open list of projects that under the circumstances would best fit the development matrix for the e-governance in Haiti. The way to advance them is to assign the task of coordination of the fundraising and initial deployment to someone with sufficient authority and access to necessary decision makers.

BASIC FRAMEWORK:

While the introduction of the e-governance as part of a political modernization of a country will be by necessity a unique process in any given country, there is sufficient experience around to suggest basic prerequisites and stages of a successful policy process.

To avoid confusion in terminology, e-governance would refer to the use of information and communication technologies (ICTs) in the overall drive to modernize the public administration and improve good governance.

We can divide the overall process into three interrelated tasks:

- 1) creating connectivity of people and offices;
- 2) creating digital resources;
- 3) providing "e" services

These services are usually viewed in three distinctive categories:

- 1) government to government G to G
- 2) government to citizen G to C
- 3) Government to business G to B

The main mistake (often done but also easily avoided) is to concentrate on the first category of services and develop e-government as a support service of the government itself apart and separate from the people and businesses. The second mistake is from the other end, governments concentrate on second category of services as they tend to be most talked about without having clear customers and preparing the infrastructure first.

In fact, the most logical approach for Haiti would be to concentrate on the first and the third category of services as businesses have more means to use the modern ICTs and running the government more efficiently is a clear and unambiguous goal as opposed to creating services that the country would not have means to administer.

UNPAN EVALUATION MODEL:

When measuring the e-government readiness, the most used model is that of the United Nations Public Administration Network (UNPAN) e-readiness index that is based on the web index or a similar EU used scheme of stages for e-government where ...

The first stage is just basic provision of information by public authorities over web interface, presence of integrated web portal for government etc;

The second stage of the development presupposes the extended information offering in forms of downloadable forms etc with clear benefits to users,

The third stage is that of first transactions between the public authorities in one side and citizens and businesses on the other. Usually its prerequisite is presence of some form of e-identity, meaning there has to be also a legal framework for using digital signatures;

The fourth stage is generally called transactional stage that would presuppose the interconnection of the various databases and information systems with the possibility of automated queries that allow providing complex e-services.

SITUATION:

Haiti is in 165 place out of 183 countries compared in the e-Government Readiness index 2008 that is compiled by the United Nations Public Administration Network (UNPAN). To break the result down to three basic categories of Web measure Index, Infrastructure index and Human Capital index shows considerable weakness in all underlying data.

According to the ITU data from 2007, Internet use is at 8.5% and mobile phone use at 5.87 % and land line at 1.7 persons for every 100 people. Though the number of mobile users is growing rapidly, it is clear from the basic data that Haiti suffers weakness in all main ICT infrastructure measurements.

In the Web measure index the total score of 19 ranks Haiti's developments among the lowest 20 countries ranked globally. This corresponds roughly to the Haiti's ranking in terms of GDP (taking into account the PPP) in 2008 and confirms the overall impression of a desperately underdeveloped country.

This means that to start building information society and the development of e-government in Haiti would need to be a delicate balancing act between the need for the robust development in a number of sectors and high competition for the scarce resources.

The positive news is that while the government policy toward building information society has been lacking previously, there is a clear interest from the top leadership of the country to move forward as witnessed by the creation of the Presidential Commission on e-Government and initiatives of the Prime Minister.

It is also interesting to note that internet use compared to overall economic situation is quite high which suggests that first steps to improve the situation could be relatively easy to undertake as there is some preparedness of the popular culture to use the new technologies.

Also, as different scenarios to take the first steps have been tried out extensively in variety of conditions over the last ten years, Haiti as a latecomer has an advantage to compose a suitable and proven ICTD strategy.

POLITICAL PROCESS:

The main task for the political process is to create and sustain momentum for the development of information society as a general strategy for taking the country into XXI century. The setting of goals itself has to be ambitious for this also conveys the message of the intentions of a country and its political elites.

On the practical level, the political leadership has to define the people/structural units responsible and provide them with authority to proceed and access to the leadership to solve serious practical obstacles.

Having a direct and immediate interest from the very top of government/local government/organization whether private or public is considered the most important ingredient for the successful change management in governance.

The reason for this is both obvious - as political will is formulated in the top - and not so obvious, because a successful introduction of e-governance is only in part technical task and more something that would be better characterized as a process of change management.

Obviously, neither the head of the country nor the head of the government has to be permanently occupied by the e-governance. However, there are three basic rules that would be advisable to follow:

- 1) Openly expressed interest and support to the process of introduction of e-governance. During my mission to Haiti I heard from a number of different people both from the public and private sector that they were not sure whether the government is serious in pursuing these goals of modernization and consequently, they are holding back making an extra effort to support the e-governance process. This is unfortunate as to overcome the low starting position, Haiti would need a concentrated effort by both public and private sectors to jumpstart the modernization process.
The best way to show this support is to create over time a number of "events" where leaders of the country would give keynote addresses that receive a wide audience via exposure in mass media.
- 2) Access to the top leadership. As the change management means dealing with unexpected, one cannot formalize the process without endangering the dynamism. Comparative experience shows (but does not guarantee) that placing a trusted advisor/administrative unit at the center of executive (e-gov envoy/e-gov czar) would considerably ease the required coordination activities and help to overcome the non-technical challenges to the process. The same basic principle is valid in the organizational level and has been promoted by a number of international organizations (e.g. World Bank) for the last 3-4 years, calling the creation of CIO (chief Information Officer) posts for Ministries etc and keeping the appointed persons as part of management teams.
- 3) Show support by a personal example. It is a surprisingly effective way to convey the need for change within the political elite and for the youth to show the use of what the leadership is preaching, i.e. deploying new forms of communication (send invitations to colleagues via e-mail, create a blog and ask a close junior staff member to add entries and keep an eye on it etc).

Seeing e-governance build-up through political terms is clearly the task for politicians. Usually there are three types of considerations to be taken into account/to be used.

1. Political: political functions can be either projecting a modernizer imago for the population or cleaning up and also progressive imago for donors. As the use of new technologies does project an image of an innovator, it is a good way of conveying the sublime message of the change. There could be a difficulty of calibrating the message for one's own population vis-a-vie donor community but in case of demonstrable changes the dissatisfaction seems to fade rather quickly.
2. Administrative: administration of people and things entails a lot of information gathering, exchange and analysis. The ICTs can help on almost with every imaginable function and no modern administration can seriously be considered without the use of the ICTs. It is more of a question whether there is a list of priority areas within the administrative changes and comparative experience suggests that to be the case.
3. Economic: the initial driver has not really fulfilled its promise as the savings are usually used up elsewhere in the larger system. The positive side of this is that the fear of many civil servants about the jobs is also unfounded as when something can be done by machines rather than humans, there is a new

job somewhere else in the administration that needs to be filled as the use of new technologies creates new demands.

In addition to these considerations, it is important to keep in mind that political support for the e-gov process can be continued only if there is a clear shared understanding why it is necessary and also doable. This would mean that considerable effort should be directed not to the development of the ICT in Haiti per se but to the positive public relations effort about modernizing Haiti via ICTs that could go under the title a "touch of e-magic to the traditional voo-doo".

In political level it is also important to show early successes which are rather hard to come by as usually the general resource base needs to be built up first before it is possible to start providing e-services. However, there are a number of low hanging fruits that should be included into the government plan and picked up in the development road. These services are generally characterized by the low implementation costs and high visibility. In Haitian context the most suitable would be some combination of mobile phone based warning system (see the general parameters for the project in p. 10)

POLICY PROCESS:

Policy process is usually seen as rational well defined process of formulating the dreams in measurable policy goals and matching them with means and creating administrative structures to monitor and support the overall coordination and implementation activities.

The situation in Haiti deviates from a textbook case in a developed country in a number of important ways. First, the policy planning function has not been well developed. Second, the resources are extremely scarce. Third, there is a large multifaceted donor activity in the country. This all creates additional instability that has to be taken into account.

Thus, it is very difficult to propose a clear firm multiannual strategy to build up information society in Haiti. Due to the uncertainty of funding and character of the political situation as well as prevailing administrative practices, it makes sense to confirm on government level the overall values and goals and then institute an open planning strategy where government would support key projects that for one reason or another are considered crucial for the development of the e-government in Haiti.

The framework for the strategy in outline is fairly simple - one has to create the basic conditions for change. In case of building information society and e-government, this consists of three steps:

- 1) Creating connectivity
- 2) Creating digital resources
- 3) Creating legal framework

The strategy government approves would need to describe administrative resources and procedures that would be used in pursuing this strategy. These will of course depend on political agreements reached but as a rule, there should be a central government unit, responsible for the overall coordination and (at least in key ministries) CIO system, so that e-gov development would be worked into the Public Administration system during the public administration reform/development process.

As there is a lot of different things to do and coordinate, it would make sense to try to package them into larger chunks with clearly defined responsibility. One of the examples could be to try to give the responsibility for connectivity to a large national project and allow it to live independent live away from everyday politics.

As the creation of national digital resources has usually proceeded “needs based”, there tend to be a lot of legacy systems in different countries whereas this is not necessarily the case in Haiti as local databases apart from the voter register and population registry are clearly rather rudimentary. That could invite a chance to work on this issue and compose a separate project for the creation of digital resources (property, land, economic activity etc).

In the given time frame, the policy level undertakings should be directed for the creation of the preconditions for further development rather than achieving clear measurable e-goals.

IMMEDIATE RECOMMENDATIONS:

PROJECT PROPOSALS:

As it is very difficult to propose a clear firm multiannual strategy to build up information society in Haiti due to the uncertainty of funding and character of the political situation as well as prevailing administrative practices, it makes sense to confirm on government level the overall values and goals and then institute an open planning strategy where government would support key projects that for one reason or another are considered crucial for the development of the e-government in Haiti.

Thus, it seems suitable to provide here a list of discrete projects that could be proposed to various donors for the support. The following is a short description of these projects and it has to develop further through developing the actual ToRs for them. Also, the list should not be considered closed, as one could add elements to it when there is a specific donor interest that could be suitably accommodated.

These projects could be promoted and coordinated through the ICT office for the Central Government, initially even as a job for someone in the PMs office.

Training for a group of key officials

For an all encompassing initiative, it cannot be either hobby or paid activity of one or another person but instead, it has to be led by a group of like minded people, sharing the common vision of change, coming from different institutions and sectors in the country. It would make sense to compose such a group from key officials and provide them formal intensive training with the clear goal of both know-how transfer as well as creating a shared purpose and preliminary action plan when going home.

Taking the development past central government to the local level

Local governments are closer to the people as they are actually providing services to the population. Quite often they are the first impression of “government” to the people and at the same time they are a necessary link between people and central government activities as well. Thus, it is necessary to start the e-gov developments in local governments parallel to the one in the central government.

There is a good example and generic resource that has been commissioned by the LGI (lgi.osi.hu) that can be localized and initial training of trainers done in the country. The main aim for this is to convey the necessity of change and a very practical steps of how to do it to the leaders of local governments. The training would concentrate not on technical questions (there is always enough technical competency to create basic information systems) but how a reform minded mayor can start the process in his/her local government.

Creating the e-cabinet

One of the most visible show of change and at the same time a good way to review the administrative practices in the top decision making is to create an e-cabinet, i.e. a paperless cabinet sessions. For a small country in the modern world with active international exchange and necessity of travel, it will also allow for continued top political decision making independently of the actual location of one or another cabinet member.

The basic requirement for the success of an e-cabinet project would be a clear and unambiguous support from the key members of the cabinet. Having this transmitted to the key staff at the PMs office, one could designate a member of the PM support team to put together a tender document for the e-cabinet and solicit support for it from the donors. This should be relatively easy to find as the outcome of this project would be higher efficiency and more transparency in decision making that is of almost universal interest of donor community.

Vendors for this project could be international but they would need to have a local company in the consortium that would later help to run and most probably develop the solution further. The role of the international partner is, first of all, to help to break the barriers of "customary" that would be too much to ask from the local vendor.

The possible price tag for such a project would be around 500.000 dollars, depending on the scope of functionalities, reach of the system and inclusion of hardware for the tender (it might make sense to have a separate tender just to procure the hardware). The time-frame for the execution of such project (without calculating the tender setup requirements that can vary from donor to donor) could be anywhere between 3 and 6 months.

Mobile based warning system – crisis communication system

One of the ways to demonstrate the usefulness of new technologies and harness support to government action in this area is to create a mobile phone based warning system for natural disasters as floods, hurricanes, earthquakes etc.

There are basically two ways to solve this problem, either by sending sms to all registred users or to send it to all recipients in the area of base tower. Both approaches have their pluses and minuses. The overall process, however, is clearly beneficial on both policy terms and political terms and it is also relatively easy to set up and cheap to execute.

I would recommend the following approach, first procure a pilot project to cover the capital (or any other comparably populated area for a quick impact) and depending on the success of this, scale it up (or try something else, if it didn't work to satisfaction). The cost for pilot could be depending on the approach taken to find it and the political support in the negotiations with mobile operators between 80k and 120k in US dollars and would include an assessment mission and working prototype. The time frame for the

deployment (after the conclusion of procurement) could be set to 3-4 months. The price for the system for the country and its running costs could be set as one of the outcome for the pilot.

For the execution I would again recommend a consortium of local and international vendors, i.e. with international vendors bringing in know-how and that would later stay with the local company. One of the companies I consulted for this recommendation was Mobi Solutions&Fortumo (www.mobisolutions.com)

Covering the country with wireless

Creating access is the very precondition for the development of information society. With today's wireless technologies, one need not to spend heavily on infrastructure for this as shown in Macedonia Connects, a USAID project that covered the Former Yugoslav Republic of Macedonia with wireless access within less than 1 year with a price tag of 5 million dollars. I would recommend for Haiti a similar approach and if possible, maybe also to use the same competence (i.e. USAID project executed by AED or at least the same team outside this institutional framework).

This project for Haiti could be developed in stages but it would be important to provide access to schools and local governments in such a centralized way. The price tag for the total project could be the outcome of an assessment mission together with the required changes in the telecom laws to execute such a project.

Creating basic engagement of schools with ICTs

People are creatures of habit and many nations have proverb to the tune that what has not been studied while young, will not be used as grown ups. Thus, it is extremely important to provide at least an awareness of the information and communication technologies at an early age and a possibility to study the use of them at schools since, if students grow up without that knowledge, they will reproduce the non-ICT literate workforce.

Usually countries have different ICT and education engagement programs that are quite widely supported by public and also private donors. It might be relatively easy to find donated hardware for schools and just to direct someone from the education ministry to work on this could pay back very quickly. This, however, should be done in parallel for finding possibilities for school connectivity and developing some teacher competence in using the new technologies.

Creating population registry

Population registry is one of the basic digital resources for the country. As Haiti has been developing the population registry already and as this is connected to a number of on-going projects and even the key people involved seem to have different understanding of the state of development, I would recommend to clarify the issue and the further steps in a conference that would gather different stakeholders.

As an additional step to an on-going development work, I would recommend to explore the possibility of developing mobile based digital ID as a cheaper alternative to other possible digital ID solutions, especially in the situation where majority of adult population already possesses a plastic ID card and to issue new ones with digital ID could be simply too expensive.

Creating an e-gov unit

The not so original recommendation but necessary activity nevertheless: development of information society and construction of the e-government needs systemic work and coordination and control. In order to carry out these tasks, it is not sufficient to have ad hoc committees and/or a group of enthusiasts who do this next to their daily jobs. Thus the necessity to create a regular government unit for e-governance. This unit should be placed in the center of government as this is the best place for coordination in the situation where there is a little regular funding and a lot of donor activities.

The next step should be to create a CIO positions in the key ministries that would supply digital resources not only to their own institutions but for the government at large, i.e. ministries of Justice, Interior, Economy. These activities should be financed from the regular budget, however, there are donors who would consider supporting the set-up of central e-gov unit as a long term high impact project.

Creating an Haitian ICT conference

ICT/eGov conference is necessary to take the resolve of change out from the offices to the society and to the international community. First conference could be directed at popularizing the e-gov strategy for Haiti. It could become an annual occurrence for renewing the e-gov agenda and raising awareness for the central topics of the day.

This activity as a rule is initially easily funded by donor community. The task should be initially given to a small working group and the logistics could be contracted out. However, it is important to ensure both the high level participation and extensive media exposure.

Government finances on-line

Usually one of the first information systems that any country establishes is to track the finances (various aspects of finances could become different projects, i.e. customs, tax collection, tracking international aid, overall expenditure). As a rule, these projects are packaged according to relevant international standards, the ToRs are easy to customize and it is relatively easy to procure as there are a number of international vendors specializing on these services.

Providing legislation on-line free of charge

This project is really a “low hanging fruit” as all the laws are in digital form in any case. Usually the hardest part of executing this project is to fight back the influential law offices that have created a paid version of this resource and would be afraid of losing business (which bzw is not true). A technical solution for the laws could be either procured or simply asked as a favor from governments that have it. The project could be situated either in the Cabinet office or in the ministry of Justice and its execution should not take more than 6 months. It is important, though, not to limit oneself with simple full text publishing but have a search functions, different time versions etc. They are easy to do and very helpful for a layman use.

Introducing transparency legislation

To regulate the information flows is one of the crucial tasks of the modern government. In this particular context this regulation is necessary for quick benefit for the population to understand why e-government is a good way of modernization. First e-services are everywhere basically information services, i.e. provision of information. It does not make sense to legislate every piece of information separately as some more traditional countries have attempted to do. Instead, the developed world has since middle of 1990s created public information laws that regulate increasingly also the “active provision of information” by the governments, i.e. what information should one find in government homepages.

By itself this project belongs clearly to the public law department of the Ministry of Justice/Public Administration but it can be run from the prime minister’s office as well (as it is done in Georgia with the help of the local Open Society Foundation there). The time frame from the beginning to the end of such project could be from 1 to 1.5 years, depending on the legislative process in the country. The price tag for Georgian project was 200.000 US\$ but it included some capacity building for the central government IT unit.

OTHER RECOMMENDATIONS:

There are a number of truisms that can be evoked in a particular country context in a particular time frame that time does not allow at the moment to develop into full recommendations. However, the following ones should be mentioned and deployed in Haitian context as much as possible:

- Utilization of free resources (open source software, products developed by international NGOs like Gov2U, Open City Portal etc.)
- Targeted negotiations for donated hardware and special license agreements with big software companies.
- Use local solutions as much as possible as they have shown being adopted to the local (meager) conditions and a change in the conditions could very quickly improve the overall situation.
- Use local companies as much as possible as this would mean the build-up of local expertise that would remain even if donor support would end.

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

ANNEXE 8 :
Rapport de Mission – RedGEALC, Uruguay
Préparé par M Raymond Noël, GTIC

RAPPORT DE PARTICIPATION A LA RÉUNION DE RedGEALC

« *Le Gouvernement Electronique au service de la gouvernance démocratique et de la compétitivité* »

Montevideo, Uruguay,

5-6 mars 2009

I. Présentation générale de la Réunion

Les 5 et 6 mars 2009, s'est tenue au local de la Mercosur à Montevideo, sous le patronage de l'OEA et de la République Orientale de l'Uruguay, la réunion annuelle du Réseau de Leaders de Gouvernement Electronique de l'Amérique Latine et de la Caraïbe (RedGEALC).

Elle était appelée à permettre aux ministres, hautes autorités et responsables d'e-Gouvernement dans chacun des 32 états de l'Amérique latine et de la Caraïbe membres de l'OEA, aux responsables d'organisations internationales et d'autres institutions contribuant à l'avancement de l'e-Gouvernement dans la région :

- 1) d'analyser la situation de l'e-Gouvernement dans les pays de la région
- 2) de définir les mécanismes de support nécessaires pour surmonter les contraintes au progrès de l'e-Gouvernement
- 3) de découvrir les meilleures expériences de la région en termes d'efficacité dans le secteur public et le m-Gouvernement (Mobile-Government)
- 4) de lancer de nouvelles initiatives d'appui au développement de l'e-Gouvernement dans l'Amérique latine et de la Caraïbe (e-Government Monitor, Mécanismes d'échange d'applications d'e-Gouvernement (e-Govex), Centre d'Excellence en e-Gouvernement)

II. Déroulement de la Réunion

La réunion a donné lieu à :

- 1) deux discours de cadrage :
 - a. du Secrétaire général de l'OEA, Jose Miguel Insulza
 - b. du vice-Président de l'Uruguay, Rodolfo Nin Novoa
- 2) des interventions à caractère général comme celles :
 - a. de l'ex-Président de Costa-Rica, Jose Maria Figueres : *La fonction Gouverner dans la société de la connaissance*
 - b. du Directeur Exécutif du Programme Leadership for a Networked World de Harvard Kennedy School of Government, Zachary Turnin : *La feuille de route du gouvernement électronique*
- 3) des présentations / partages d'expérience comme celles :
 - a. du Directeur Exécutif de l'AGESIC, Jose Clastornik : *Les avancées de l'Uruguay en matière d'e-Gouvernement*
 - b. du Directeur des Moyens Electroniques dans la campagne d'Obama, Joe Rospars : *Comment arriver au renforcement de la citoyenneté à travers les TIC ?*
- 4) un atelier d'échanges avec des membres d'organisations et d'initiatives internationales contribuant au développement de l'e-Gouvernement dans la région (SEDI/OEA, ICA/CDRI, BID, Banque Mondiale, CEPAL, CARIDAD, CAF, AHCIET)
- 5) des débats sur le contenu de la Déclaration de la Réunion de Montevideo
- 6) un atelier de travail sur le Plan d'Action RedGEALC 2009-2010.

III. Résultats

La rencontre a permis des échanges intéressants sur des enjeux et défis pour les pays de l'Amérique latine et de la Caraïbe à s'engager dans la voie du gouvernement électronique.

Les TIC et / ou l'e-Gouvernement sont tour à tour présentés comme des outils pouvant :

- accélérer le processus de modernisation du secteur public (Insulza)
- accroître la conscience citoyenne (Insulza)
- accélérer la transformation du service au sens large (Turnin)
- réduire les conflits intergénérationnels (Turnin)
- faciliter l'application des principes de transparence, d'authenticité et de participation (Rospars)
- contribuer à la croissance économique (Clastornik)
- aider au développement de la citoyenneté (Clastornik)

Les défis ne sont pas moins importants. Le développement de l'e-Gouvernement devra entres autres :

- compter sur la collaboration (Turnin) et l'implication de la société civile, du secteur privé à côté du Gouvernement (Noboa)
- identifier un leader (Turnin)
- développer un cadre légal adapté (Clastornik)
- faire du projet d'e-Gouvernement non un projet technologique mais un projet politique (Comas)
- personnaliser les services (Turnin)
- gagner la confiance des gens (Rospars)
- maintenir l'innovation au-delà de l'extinction du financement (Turnin).

D'autres points ont été soulevés tels

- le besoin d’harmonisation des cadres réglementaires régionaux
- l’accès universel
- de nouveaux mécanismes de financement comme le Fonds de capacité institutionnelle, le fonds de coopération horizontale (FOCOH).

La délégation haïtienne (le Directeur des Communications du MTPTC, Jean-Marie Maignan et moi) a mis l’accent dans ses prises de parole sur les efforts à engager par le Réseau RedGEALC en vue d’une part du renforcement de la coopération régionale en matière d’e-Gouvernement et d’autre part de l’assouplissement des procédures de déblocage des fonds des organisations internationales pour réduire le délai trop long entre l’expression du besoin et la disponibilité du financement et atténuer les risques d’inadaptation technologique.

Vraisemblablement, en 2009-2010, le RedGEALC compte intensifier les actions d’inventaire et de monitoring des initiatives existantes, avec accent particulier sur le M-Gouvernement.

Le Costa-Rica s’est proposé et est retenu pour héberger la prochaine réunion du RedGEALC en 2010.

II. Contacts particuliers

En marge de la réunion, j’ai pu aménager des entretiens avec quelques acteurs pouvant éventuellement contribuer au travail du GTIC, dont Silvana Rubino-Hallman Spécialiste en Modernisation de l’Etat de la BID, Juan Navas Sabater de la Banque Mondiale, et Christine Deslopes de Passport Canada.

Entretien avec Silvana Rubino-Hallman

Comme son supérieur hiérarchique Xavier Comas (xavierc@iadb.org) avec lequel j’ai eu des échanges informels lors du dîner de jeudi soir, Silvana (srubino@iadb.org) paraît bien informée du dossier Modernisation de l’Etat en Haïti. En plusieurs occasions, ils font référence au document Programme global de Modernisation de l’Etat et du volet e-Gouvernance qui y est inclus. Elle a certaines idées sur la structure et la portée d’un programme d’e-Gouvernement en Haïti, en référence à des initiatives menées au Brésil et au Chili et dans les limites des informations reçues d’Haïti.

Silvana précise l’intérêt de la BID pour ce dossier et pense qu’une mission exploratoire en Haïti, qui serait conduite par elle ou un (e) collaborateur (trice), est possible toutes les fois qu’il y a une requête via la représentation locale.

Entretien avec Juan-Navas Sabater

Avec lui, j’ai débattu du projet de Caribbean Infrastructure Initiative envisagé par la Banque Mondiale dans la lignée de Africa Infrastructure Initiative déjà opérationnel. Selon Juan (insabater@worldbank.org), le dossier est encore au stade de projet. Il vise à connecter des pays de la Caraïbe par un câble sous-marin et à développer la connectivité rurale sur cette plateforme. Les premiers pays ciblés sont ceux qui ont des problèmes plus sérieux d’accès : Haïti, Surinam. Il sera aussi considéré dans le cadre de ce projet la mise en place d’une liaison physique terrestre entre Haïti et la République Dominicaine.

Sitôt le dossier constitué, la Banque va travailler à mobiliser le financement nécessaire pour sa concrétisation.

Grâce à un financement du gouvernement japonais, un consultant vient d’être engagé pour réaliser l’étude en question. Il doit rentrer dans une dizaine de jours en Haïti. La proposition d’une réunion de travail avec le GTIC est bien accueillie.

Entretien avec Christine Desloges

Christine (cdesloge@pptc.gc.ca) a été la coordonnatrice du programme Gouvernement en ligne du Canada. Elle m'a fait part de la stratégie qui a été mise en place et de certains préalables.

Le partage de cette expérience pourrait être très intéressant pour le GTIC. La question de sa disponibilité à cette fin n'a pas été abordée. Mais elle m'a promis de m'envoyer les documents électroniques.

III. Conclusion

En guise de conclusion, je remercie le Secrétariat Général de la Présidence pour la célérité avec laquelle le traitement de la requête a été fait et pour l'opportunité qu'il m'a donnée de participer à cette importante réunion au nom du GTIC.

J'espère que le GTIC pourra mobiliser les ressources suffisantes pour faire le suivi de cette participation avec efficacité.

Liste des sigles et acronymes

AGESIC	:	Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento
AHCIET	:	Asociación Hispanoamericana de Centros de Investigación y de Empresas de Telecomunicaciones
BID	:	Banque Interaméricaine de Développement
CAF	:	Corporación Andina de Fomento
CARICAD	:	Caribbean Centre for Development Administration
CEPAL	:	Commission Economique pour l'Amérique Latine
CRDI	:	Centre de Recherches pour le Développement International
GTIC	:	Groupe de Travail sur les TIC
ICA	:	Institut pour la Connectivité des Amériques
Mercosur	:	Mercado Común del Sur
MTPTC	:	Ministère des Travaux Publics, Transports et Communications
OEA	:	Organisation des Etats Américains
RedGEALC	:	Réseau de Leaders de Gouvernement Electronique de l'Amérique Latine et de la Caraïbe
SEDI	:	Servicio de Desarrollo Integral
TIC	:	Technologies de l'Information et de la Communication

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

ANNEXE 9 :
Mission Exploratoire BID, Mme Silvana Rubino-Hallman,
Port-au-Prince 10-14 août 2010

La mission du Dr. Silvana Rubino-Hallman, spécialiste en réforme institutionnelle notamment par l'utilisation des TIC dans la transformation de l'administration publique, s'est déroulée du lundi 10 au jeudi 14 août 2009.

La programmation préparée par le GTIC incluait une dizaine de rencontres individuelles et d'entretiens plus larges, avec des organismes publics et privés de secteurs-clé. Cette mission a été précédée d'une rencontre lors de la conférence annuelle du Red GLEAC, suivie de deux vidéo conférences. Ces interactions entre la BID et le GTIC ont servi à établir le bien-fondé de cette mission, à en définir le mandat, prévoir son contenu, et à arrêter la répartition des tâches entre la Représentation et le GTIC en vue d'une coordination optimale.

1.- Lundi 10 août - 18:00 heures - GTIC

M. Gary OLIUS
M. Patrick ATTIE
Mme Tayana ETIENNE
M. Schiller JEAN-BAPTISTE
M. Raymond NOEL
Mme Marlène SAM

Une première séance de travail a eu lieu, à l'hôtel où est descendue Madame Rubino, peu après son arrivée à Port-au-Prince, le lundi 10 août, à 18 :00 Heures. Y étaient présents, outre M. Gary OLIUS, de la BID, Patrick ATTIE, Coordonnateur du GTIC et trois autres membres de la Commission, Mme. Tayana ETIENNE, M. Raymond NOEL, Schiller JEAN-BAPTISTE et Mme. Marlène SAM, Consultante.

Cette première prise de contact a été l'occasion de souhaiter la bienvenue à Mme Rubino, dont la venue résulte d'une mission à laquelle le GTIC a pu être représentée, peu de mois auparavant, avec l'appui de la BID, et de lui rappeler les deux volets de la courte et intense mission qu'elle débutait, à savoir :

- a) Achever la définition du projet d'e-Gouvernement
- b) Finaliser le projet d'assistance technique de la BID au GTIC.

Le GTIC, explique M. Patrick Attié, Coordonnateur, est dans une phase où il collecte des données pour remplir son double mandat fixé par arrêté présidentiel : préparer un plan stratégique pour le développement des technologies de l'information et de la communication et la gouvernance électronique.

Pour ce qui a trait à la modernisation de l'administration publique, l'e-Gouvernement, plusieurs pistes sont explorées, et un cadrage est indispensable. Les priorités exprimées par l'Exécutif sont :

- 1) Mise en place d'un système d'identification des citoyens
- 2) Cadastre / Aménagement du territoire
- 3) Cadre légal pour la gestion de l'information électronique
- 4) Lutte contre la corruption
- 5) Transparence.

Bien entendu, le problème du financement se pose, de même que celui de la coordination des interventions. Pour compléter cette liste de priorités et principes énoncés par les pouvoirs politiques, il convient de mentionner que, tout récemment, la Commission de Travail sur la Compétitivité a proposé des secteurs économiques prioritaires : l'agriculture (filiales des fleurs, fruits, tubercules, et élevage...); les BPO et l'industrie textile et le tourisme.

Les objectifs primordiaux à poursuivre sont la création d'emplois et la création de richesse. Les TIC sont un secteur porteur transversal.

A cela s'ajoute bien entendu, le souci de mettre en place un cadre institutionnel capable d'impulser et d'accompagner ce changement pour permettre l'accès aux services sur tout le territoire national et la mise en place des infrastructures indispensables. Ainsi que la décentralisation des activités, de l'administration, et l'aménagement des infrastructures (téléphoniques et dorsale) pour permettre un accès, une couverture nationale de services...Le Président se préoccupe, pour sa part, d'une structure capable d'assurer le suivi des recommandations formulées.

Les points suivants font l'objet d'échanges :

- La nécessité d'une décision stratégique pour dégager une vision et des priorités clairement énoncées.
- Le cadre institutionnel existant et les modèles alternatifs à adapter.
- L'importance d'identifier une approche pour procéder, de proposer une « Feuille de Route » assortie de phases définies.
- La nécessité de quantifier avec précision les besoins en termes de coûts et de Ressources humaines.
- La multiplicité d'initiatives indépendantes les unes des autres, en l'absence d'une plateforme d'interopérabilité qui intégrerait les services de l'Etat aux citoyens.
- La double intervention de l'Etat en tant que gestionnaire et d'exploitant.
- La nécessité de finaliser le contenu de l'appui au GTIC, compte tenu des contraintes de temps.
- L'importance d'une ferme détermination de la part des pouvoirs politiques pour avancer.
- La nécessité de faire connaître les avantages liés aux TIC à la Fonction Publique.
- L'importance d'atteindre rapidement des objectifs liés à des résultats visibles démontrant clairement l'impact des améliorations en cours de mise en œuvre.
- Le projet de la BID concernant l'ONI (une enveloppe de 12 Millions de Dollars).
- Le mandat du GTIC : définir les orientations, les lignes directrices et les sources de financement et les partenariats stratégiques potentiels pour l'exécution du Plan National.
- La disposition de la BID à accompagner le GOH dans les projets identifiés et jugés prioritaires par le Gouvernement.
- La volonté du GTIC de « délivrer » d'ici décembre, et lancer 1 ou 2 « chantiers », en particulier le cadre légal sur la gestion de l'information électronique, préalable à toute réforme du secteur.

Appui technique et financier pour répondre aux attentes de l'Exécutif en respectant les délais impartis. Finaliser l'analyse pour proposer une approche et un système à la fois efficaces et réalistes, parce qu'adaptés. Consulter les acteurs.

En cette occasion, il est mis en exergue que la BID a aussi pour vocation de renforcer les capacités des pays membres et qu'elle manifeste son intention :

1. d'accompagner le GTIC ;
2. d'avancer rapidement dans l'élaboration du projet d'appui
3. d'impliquer le GTIC dans le cadre du projet envisagé avec l'ONI.
4. de prévoir des ateliers de sensibilisation pour les Parlementaires, les Fonctionnaires
5. d'envisager le recrutement d'un Consultant pour l'élaboration de la « Feuille de Route »
6. d'inclure un plan d'implantation de la décentralisation des services administratifs
7. d'identifier des sources de financement tels que les Fonds Chinois, Japonais ou encore Opérations Spéciales.

M. Gary OLIUS indique les délais qui seront nécessaires pour l'approbation interne à la Banque : 30 - 40 jours, à compter de la soumission du document de projet qui sera préparé avec l'aide de Silvana Rubino.

Le GTIC remercie la BID de sa sollicitude et rappelle combien l'approche qui sera proposée pour les TIC, secteur transversal et de support aux autres activités socio-économiques, peut servir d'exemple pour d'autres domaines d'intervention.

Questionnée sur ses attentes exactes à l'égard des divers interlocuteurs qu'elle est amenée à rencontrer dans les deux jours à venir, Mme Rubino précise qu'elle souhaite cerner les services attendus ou souhaités de la part de l'Etat ; connaître leurs visions respectives sur ce qu'il convient de faire ; leur compréhension du « Doing Business » ; leur opinion vis-à-vis des besoins, en particulier, en ressources humaines ; leurs réflexions sur les filières envisageables...

Mesdames Tayana ETIENNE et Marlène SAM sont chargées de se relayer pour accompagner Mme Rubino.

2.- Mardi 11, 8 :00 Heures – Chambre Franco, Pétionville : Focus Secteur privé

M. Philippe MATHIEU, Membre du groupe Compétitivité, Entrepreneur agricole
 M. Wilkair FEGOND, VISION 2000, animateur d'une émission PASSWORD
 M. Patrick Attié, ESIH, Vice-Président de la Chambre Franco
 M. Schiller Jean-Baptiste
 Marlène Sam

Peu furent les présences en raison de la tenue d'une autre importante rencontre du secteur privé à l'initiative de la Chambre de Commerce, le jour même.

M. Philippe Mathieu, représentant du Groupe de Travail sur la Compétitivité put amplement faire part de l'expérience et du déroulement des travaux du groupe qui vient de soumettre son rapport. Il rappelle la tenue de plusieurs rencontres avec divers acteurs, de leur souci concernant la méthodologie, du sens « transversal » donné à la compétitivité, et d'adopter une présentation efficace, en particulier, pour les décideurs.

Les sondages menés ont fait ressortir que la méfiance vis-à-vis de l'Etat est moindre que celle vis-à-vis du secteur privé. En ce qui concerne les TIC, il évoque que la question sémantique est primordiale : il faut définir ce que sont ces nouvelles technologies ; d'établir le potentiel qu'elles recèlent en matière de création d'emplois, d'amélioration des services et comme nouveau secteur... Il

manifeste son intérêt réel pour s'informer d'avantage, au cours de cette rencontre, des perspectives et enjeux liés aux TIC.

Mme Rubino brosse, l'historique et l'évolution du concept, ses succès et les diverses écoles de pensée et souligne le potentiel incroyable qu'il renferme, lequel ne se limite pas à la gestion de l'Etat, mais s'étend à la transparence dans son fonctionnement ; la coordination améliorée des organismes publics, des relations public/privé ; la diminution du coût des transactions des citoyens avec l'Etat ; l'accroissement des recettes ; en d'autres termes, elles peuvent favoriser une nette amélioration de l'organisation de l'Etat.

Les TIC permettent de faire les choses différemment, les compétences d'avant sont agencées d'une autre manière ; les choses sont « intégrées », d'où le besoin d'informations intégrées.

Pour l'e-Gouvernement, chaque pays s'emploie à définir ses priorités politiques, culturelles, sociales et économiques, et conçoit ainsi un cadre adapté, en tenant compte des fonctions essentielles remplies ou attendues de l'Etat, et utilise les TIC pour appuyer son intervention.

Ceci signifie la création d'une plateforme technologique ayant, en règle générale, pour double finalité : a)- l'accroissement des services aux citoyens, l'utilisation plus efficace de ces services ; qui ont un caractère plus « personnalisé », accompagné d'une baisse des coûts et pour l'Etat et pour le citoyen ; et b)- de meilleures informations et données sur ce qui se passe, ce dont on a besoin et, aussi, sur l'impact de l'action menée par le Gouvernement...ce qui améliore et facilite l'efficacité de la prise de décision.

Elle cite en exemple l'expérience des Bahamas.

Les thèmes suivants sont ensuite abordés :

- Le décalage existant entre un modèle idéal et la réalité.
- Les avantages et opportunités qu'une telle politique engendrera.
- La nécessité de disposer de données fiables, principalement sur les grands agrégats, et sur l'évolution des facteurs (notamment pour le secteur agricole).
- Les différentes étapes ou phases de mise en œuvre d'un plan d'e-Gouvernement.
- L'appropriation par les différents groupes et secteurs existants en vue de reconstruire une relation de confiance.
- L'absence de circulation de l'information sur les projets et réalisations en cours actuellement, notamment en-dehors de la zone métropolitaine. Il y a une réelle méconnaissance à déplorer. Ainsi, il semble que le Sud ait un programme de développement plus intégré, contrairement au Nord du pays.
- Les coûts et taux exorbitants pratiqués en Haïti, en particulier, en matière de crédit, auxquels sont confrontés les particuliers tout comme les entreprises.
- Un paradoxe : la douane est la première source de revenus de l'Etat, c.a.d. les taxes prélevées sur les importations.

Bien faire ressortir pour les acteurs le sens et les enjeux liés aux TIC pour le développement et la compétitivité d'Haïti. Appuyer l'Etat dans la mise en œuvre.

3.- Mardi 10 août 10 :00 Heures – Ministère de l'Economie et des Finances (MEF)

Messieurs Félix, Avrilus et deux autres collaborateurs – Annullé

Cette rencontre à laquelle devait participer la représentante a.i. de la BID, Madame Sarah ROMAIN, a été annulée, à la demande du MEF, en raison des manifestations quelque peu violentes qui se déroulaient dans cette zone. Elle n'a pas pu être reprogrammée.

4.- Mardi 10 août 13 :00 Heures – Office National d'Identification (ONI)

M. Ronald COVIL, Directeur Général

Le GTIC n'a pas pu être représenté à cette réunion. Mme Rubino remercie M.Covil de son accueil et lui explique les objectifs de sa mission. M. Covil remercie Mme Rubino de sa visite et présente la situation de l'ONI, spécialement les obstacles qui existent maintenant. La procédure pour collecter l'information en provenance des bureaux de l'ONI en-dehors de Port-au-Prince pose beaucoup de problèmes. Le citoyen présente ses documents au bureau décentralisé et l'opérateur saisit l'information sur un ordinateur qui n'est pas connecté aux ordinateurs centraux. L'information concernant toutes les demandes/applications est regroupée sur un CD qui est envoyé au bureau central de l'ONI par la poste, une fois par mois. Cette procédure comporte des faiblesses du point de vue sécurité, non seulement pendant la transmission de l'information mais au tout début du processus.

Mme Rubino a manifesté l'urgence de mettre en œuvre un réseau qui connecte tous les bureaux de l'ONI (au nombre de 141). Un système ayant ces caractéristiques pourrait résoudre les problèmes de sécurité, réduire le temps d'attente du citoyen pour recevoir sa carte d'identité. En plus, si un réseau peut être mis en place, ce serait possible de l'utiliser pour l'état civil tout en permettant l'interconnexion des deux procédures.

M.Covil a dit qu'une plateforme technologique avec ces caractéristiques est justement le type de solution dont l'ONI a besoin. Mme Rubino se mettra en contact avec ses collègues de la Banque qui sont en train de travailler dans la nouvelle opération du Registre Civil.

La réunion s'est conclue avec la promesse de garder le contact pour explorer les possibilités d'envisager l'inclusion d'une composante additionnelle dans l'opération avec le GTIC pour développer la conception de ce réseau technologique pour l'ONI.

5.- Mardi 10 août 15 :30 Heures – Ministère du Commerce et de l'Industrie (MCI)

Mme Marie-Josée GARNIER, Ministre
M. Pierre André DUNBAR, Directeur Général
M. Patrick Attié
Marlène Sam

M. Attié remercie la Ministre de son accueil et expose les objectifs de la mission de Mme Rubino. Les TIC représentent un pilier pour la croissance économique, au service des entreprises, et là intervient le facteur temps. Certains problèmes se posent : celui du cadre légal adapté à cette évolution technologique.

La Ministre remercie le GTIC. Le sujet l'intéresse au plus haut point. Le MCI a un projet de réaliser un forum, en octobre, au cours duquel il compte organiser une table ronde sur les TIC. Le MCI s'intéresse aux TIC à deux titres : comme outils, et aussi, comme industrie.

Mais pour le Ministère, le Directeur Général a déjà identifié des domaines et services liés aux TIC :

- a)- stockage des informations (registres commerciaux, exportations ; et autres...);
- b)- gestion du courrier, afin de réduire les délais et pour assurer un meilleur suivi des dossiers ;
- c)- outil de prise décision : les TIC peuvent être aussi un précieux outil, indispensable, en se basant sur un système d'information et de données fiables, aussi bien sur le plan comptable (entrées/sorties), que dans d'autres domaines ; et

d)- faciliter la collecte et la diffusion de données, en interconnexion (plateforme) avec d'autres agences de l'Etat...ce qui permettrait de pallier au manque de Ressources Humaines qualifiées, éventuellement.

Le MCI est préoccupé d'assurer la sécurité, la centralisation, le stockage, le partage et le traitement des données statistiques diverses et est favorable à une centralisation, là où c'est envisageable et possible, du processus dans le respect des spécificités de chaque administration.

Le MCI attend avec impatience l'évolution et lui suivi de ce dossier ainsi que les recommandations qui seront formulées par le GTIC sur l'utilisation des TIC et l'e-Gouvernement.

Aider le MCI et les administrations publiques à exploiter et utiliser les TIC pour améliorer leur gestion, coordonner leurs interventions, et aussi pour favoriser la prise de décision, la communication, la collecte et la diffusion de l'information.

6.- Mardi 10 août 16 :30 Heures – Société Civile – Chambre Franco

Mme Marie Louise AUGUSTIN, Directrice Exécutive – Alliance pour la Gestion des Risques & la Continuité des Activités - AGERCA

M. Rosny DESROCHES, Directeur Exécutif – Initiative de la Société Civile – ISC

M. Jérôme DOMOND, COMCEL / VOILA – AGERCA

En introduction, M. Attié rappelle les attentes de l'Exécutif, la prochaine mission du GTIC en Estonie, les efforts pour favoriser la définition d'un projet de loi sur l'utilisation de l'information publique et un cadre légal pour le secteur TIC. Il invite les participants à faire connaître ce que les TIC, à leur avis, peuvent signifier ou apporter aux citoyens, à la société civile.

M. Domond remet à Mme Rubino un article, dont il est l'auteur, portant sur les TIC. L'AGERCA demande ce que le GTIC peut faire pour que le câble de fibre optique puisse être exploité.

Le représentant de l'ISC, qui regroupe depuis 2000 une trentaine d'organisations des secteurs associatifs, du patronat, syndicats, écologiques, éducatifs, églises,...explique l'utilisation faite par l'Initiative :

- Lors des récentes élections, utilisation du portable pour collecter les rapports des observateurs et des permanences à travers le pays, fort du constat qu'ils possédaient tous un téléphone portable ;
- Lors des dernières élections, utilisation d'un site créé par un jeune. Plus de 170.000 visiteurs lors du jour des élections, le 21 juin dernier ;
- Lors des mouvements de 2003, le GNB, les portables ont beaucoup servi à la mobilisation des citoyens.
- Proposition d'utiliser les TIC pour surveiller la mise en œuvre du Budget National, outil de planification, de contrôle, avec l'aide de la Banque Mondiale.

Fort de cette expérience, l'ISC considère qu'il faut deux éléments fondamentaux pour garantir le succès d'un plan d'e-Gouvernement : a)- la volonté politique et b)- des moyens techniques adaptés.

Les autres thèmes successivement abordés sont :

- Une meilleure coordination des interventions de la communauté internationale. Quelle est, en effet, la Table Sectorielle chargée de s'occuper des TIC ?

- Le lancement de chantiers précis, c'est-à-dire d'un passage à l'action, peut servir à mesurer l'existence d'une volonté politique, même si cette dernière est manifeste par l'intermédiaire de la création du GTIC.
- Les TIC peuvent servir à accroître le contrôle de la part des citoyens et développer, par là même, la volonté politique.
- L'expérience d'utilisation des téléphones portables pour lancer des appels, des demandes d'aide pour les sinistrés. A noter qu'il y aurait une clause faisant obligation aux entreprises de télécommunications d'aider en cas d'urgence.
- L'effet multiplicateur de l'utilisation des TIC enregistré en Uruguay dans le cadre du projet « One laptop per child », surtout en milieu rural.
- AGERCA travaille pour inclure un module ou un cours sur la gestion des risques de catastrophes naturelles, climatiques, sismiques et autres, dans le cursus scolaire.

La société civile a pleinement pris conscience des opportunités qu'offrent les TIC.

7.- Mercredi 13 :00 Heures – Université d'Etat d'Haïti (UEH)

M. Pierre Henri VERNET, Recteur
 Gary Olius
 Tayana ETIENNE
 Raymond NOEL
 Patrick Attié
 Marlène Sam

Le Recteur fait part du projet de campus numérique qui permettra une décentralisation de l'université qui veut garantir une formation académique de qualité, en dépit de lacunes en ressources humaines, infrastructures, bâtiments, laboratoire et équipements. Elle est à la recherche de partenariats nationaux et internationaux qui lui permettraient de développer ses capacités internes en se connectant à des réseaux.

Il rappelle que la mission de l'institution universitaire est d'apporter une expertise à la communauté : Etat, entreprises et société. Elle est prête à expérimenter de modèles afin d'en piloter l'exécution, l'implantation. Elle doit fournir les ressources et, dans ce domaine, a un rôle-clé. Il faut renforcer son potentiel.

Interrogé sur l'existence, au sein de l'UEH, de programmes de gestion administrative spécifique pour les futurs fonctionnaires publics, il indique qu'existe l'ENAF (Ecole Nationale de l'Administration Financière) et l'ENAPP, en cours de formation, pour l'Administration et les Politiques Publiques.

Les échanges se poursuivent, ensuite, sur :

- L'existence de formations spécifiques sur la gestion des TIC au sein du secteur public, de ressources humaines qualifiées ayant la capacité de concevoir et de gérer l'architecture des

administrations publiques dans le cadre de mise en place de l'e-Gouvernement, comparable à celle destinée aux Chief Information Officers (CIO), des Etats-Unis.

- La nécessité d'identifier des créneaux de recherche sur des applications débouchant sur des filières spécifiques.
- La petite enveloppe réservée à l'Enseignement universitaire dans le cadre de la coopération internationale ou l'absence de référence au R&D dans le DSNCRP.
- La BID rappelle qu'elle est très impliquée dans le domaine de la Recherche et Développement.
- Le manque d'interaction, dans la culture haïtienne, entre l'Université et les institutions étatiques, dans la recherche de solutions aux défis nationaux, alors qu'elle pourrait procéder, par exemple, à l'analyse des données collectées.
- La tendance à mettre en place des observatoires que l'Université serait à même d'héberger, d'alimenter, etc...
- L'Université a conscience de devoir être plus proactive car il y a, au sein du DSNCRP, des piliers qui ne sauraient être atteints en l'absence d'une coopération Etat / Université.
- Le besoin de cerner le rôle de l'Université dans le processus de développement et de l'exploitation des TIC en Haïti.

En conclusion, il est convenu qu'il serait judicieux de mener une étude pour identifier les compétences, de définir, voire de quantifier, les profils des ressources humaines à former pour accompagner la mise en œuvre d'un plan national d'e-Gouvernance. Il faudrait, par la même occasion, identifier ses besoins en assistance technique pour y participer et y contribuer.

Des TDR allant dans ce sens vont être élaborés et une requête adressée à la BID par le Recteur, est-il convenu.

La décentralisation de l'Université peut coïncider avec l'implantation d'un plan d'e-Gouvernance auquel l'institution pourrait contribuer en renforçant sa capacité à préparant les compétences adaptées.

8.- Centre National de l'Information Géo-Spatiale (CNIGS)

Mme Gina PORCENA MENEUS, Directrice Générale
 M. Robert PIARD, Coordonnateur Technique
 M. Gary Olius
 M. Patrick Attié
 Marlène Sam

La Directrice et son collaborateur accueillent chaleureusement la délégation, sur une demande faite peu auparavant. La Directrice fait un bref exposé sur l'historique de cet organisme autonome du Ministère de la Planification et de la Coopération Externe (MPCE), fondé en 2006. Il gère et alimente une base de données d'images satellites pour constituer un référentiel de base qui puisse permettre qu'elles servent à la prise de décision et aboutir à une meilleure gestion du territoire. Le CNIGS bénéficie d'un financement de l'Union Européenne et a développé des partenariats autour d'applications thématiques. Par exemple, avec le CNSA. Il s'emploie à monter une plateforme de système d'informations géographiques.

Le CNIGS s'efforce d'utiliser, dans la mesure du possible, des applications adaptables et compatibles avec ceux qui existent déjà sur place, ce qui permettra de « superposer » des couches en vue d'optimiser la prise de décision. Par exemple, a)- exploiter les données du recensement en possession de l'IHSI ; b)- compléter avec les 7.408 photos datant de 2002, les anciennes cartes de l'ONACA (Cadastre) datant de 2002.

Le CNIGS est l'unique effort géo spatial de ce niveau de sophistication et de professionnalisme en Haïti. Il ambitionne de constituer un nouveau référentiel 2010 (1^{er} janvier au 30 mars). Il s'agit d'une opération qui coûtera approximativement 500.000.000 dollars américains auxquels s'ajouteront environ 200.000 Dollars pour le traitement et le renouvellement, tous les cinq ans, des données.

Sont discutés, ensuite :

- L'élaboration d'une cartographie des zones inondables, en vue de compléter une programme d'alerte précoce.
- La demande de plus en plus forte pour les données numériques.
- Une collaboration en cours avec la Mairie du Cap-Haïtien.
- Les efforts consentis en matière de formation : entre 2005 et 2009, le CIGS a formé 34 personnes au sein des ministères et organismes partenaires. Le CNIGS compte 70 employés dont environ 55 techniciens.
- Le CIGNS signe un protocole d'entente avec les bénéficiaires de bourses de formation, par lesquels ces derniers s'engagent, une fois formé, à travailler cinq ans pour l'État, ou sinon, à rembourser les dépenses qu'il aura encouru pour sa spécialisation.
- Le CINGIS se soucie au plus haut degré de mettre en commun ou d'harmoniser le niveau de connaissance, pour posséder des interlocuteurs compétents pour servir d'interfaces dans l'institution partenaire ; les équipements, logiciels et matériels, pour mieux coordonner les échanges et mettre en commun l'information. De fait, il s'aligne, en termes de délais de réalisation, pour rester en diapason avec les institutions partenaires, garantie du succès du projet commun.
- Le CINGIS est en relation et/ou en étroite collaboration avec des institutions sœurs et autres sources de données de l'étranger.

Il est convenu qu'à l'occasion de sa prochaine mission, Mme Rubino effectuera une vite compète des installations du CNIGS.

En allant voir, grâce aux TIC, ce qui se fait et a été tenté ailleurs, Haïti peut faire des bonds !

On peut faire soi-même, de son côté, et vite...mais pour s'assurer du succès et du suivi, c'est mieux de le faire plus lentement, en un an, un an et demi...Il faut savoir attendre !

9.- Mercredi 15:30 heures – Bureau du Premier Ministre

Mme Michelle PIERRE-OUIS, Premier Ministre
 M. Thierry CHERIZARD, Conseiller
 M. Gary Olius
 M. Patrick Attié
 M. Raymond Noël
 Mme Tayana Etienne
 M. Schiller Jean-Baptiste
 M. Jaunasse Elysée
 Marlène Sam

Le Coordonnateur du GTIC remercie le Premier Ministre d'avoir accordé au GTIC cet entretien motivé par la mission exploratoire qu'accomplit Mme Rubino, spécialiste de la BID, dans le cadre de la définition d'un appui au groupe. Il lui cède la parole.

Madame Rubino retrace, brièvement, les grandes lignes d'un projet qui se dessine à l'issue des rencontres qui ont déjà eu lieu : la mise en place d'une plateforme technologique pour l'ensemble du gouvernement, l'élaboration d'une Feuille de Route pour la mise en œuvre d'un plan d'e-Gouvernance, qui devra inclure des indications sur les caractéristiques du système, son coût, les délais de réalisation, les résultats escomptés en 2010, et à moyen / long terme. Il y aura, aussi, des investissements considérables en infrastructures à faire pour effectuer ce bond. Ce plan stratégique des investissements devrait être assorti de propositions de financements à Moyen / Long terme.

La rencontre avec le Chef du Gouvernement représente, pour ce, une occasion d'avoir ses réactions vis-à-vis de ces pistes et de recueillir des conseils.

Le Premier Ministre remercie la BID pour son appui au GTIC. Elle poursuit en faisant référence à la présentation du rapport d'étape que le GTIC a faite au Palais, le matin-même, et dit combien elle demeure impressionnée par le travail accompli. Elle souligne comme il est important, vu ce momentum, de travailler conjointement. Le point de départ a été la déclaration du Président dans laquelle il disait souhaiter l'avènement d'un nouveau mode de gouvernement, d'une nouvelle gestion de l'Etat....

Avec les TIC, Haïti peut faire des sauts qualitatifs car on n'a plus le temps de cheminer.

Le GTIC a fait l'inventaire de tout ce qu'il faut : le plan stratégique, les infrastructures, le cadre légal adapté...Il faut commencer à établir les bases. Le GTIC est composé de pionniers, de constants défenseurs des TIC. L'engagement du Président, du Premier Ministre est total. Cet effort a tout le support du Gouvernement qu'il faut.

Madame Rubino fait part du projet d'organisation d'ateliers sur les TIC et l'e-Gouvernement destinés aux parlementaires, aux membres du Gouvernement, les hauts fonctionnaires et cadres.

Sont abordés ensuite, les thèmes suivants :

- Quelques éléments du contenu du Plan stratégique, la proposition de système, et le plan d'implantation.
- Le volet Identification et le projet-pilote de la BID avec l'ONI.
- L'importance accordée par le Premier Ministre au domaine de l'identification, car trop d'haïtiens n'existent pas légalement, et que d'autre part, les décideurs politiques ont besoin d'un système fiable qui permette de planifier.
- Le Premier Ministre interroge Mme Rubino sur la problématique des résistances à ce changement. L'expérience prouve qu'en présence d'une volonté politique et d'une direction précises, elles disparaissent. De fait, la mise en œuvre d'une telle politique est plus facile dans un cadre intégré.
- Le signal fort que cette identification représentera pour les citoyens.
- Les modèles existants pouvant servir d'inspiration.
- La sécurisation de certains champs.
- L'importance accordée par la BID à la définition des priorités et à leur expression de la part du Gouvernement, surtout au niveau du Budget.
- La complémentarité et la durabilité des structures.
- Les aspects institutionnels, économiques et sociaux des TIC et les liens qui existent entre eux.
- La matérialisation des partenariats public/privé.

On n'a pas le temps de cheminer.

Il y a un alignement des planètes.

10.- Mercredi 17 :00 heures – Secteur Télécommunications - GAMA, Delmas

M. Mathias PIERRE, PDG GAMA, Président AHTIC, Vice-Président de la Chambre de Commerce & d'Industrie d'Haïti - CCIH

M. Claude APAID, Alpha Communications Network (A C N), AHTIC

M. Reynold GUERRIER, Multilink, AHTIC

M. Napoléon, Etudiant, AHTIC

Gary OLIUS

Marlène Sam

En ce qui concerne le cadre légal :

La loi sur les télécommunications a été faite et refaite. L'AHTIC et les autres acteurs ont formulé des recommandations, qui ont été prises en compte. Il y a maintenant un consensus et il ne reste que le vote de ce texte. Ce contexte permet d'avancer plus rapidement.

Il faut prévoir un accompagnement du Parlement pour qu'il comprenne mieux les enjeux.

En ce qui concerne l'e-Gouvernement :

- Renforcer les infrastructures : il faut que la dorsale soit une opportunité de partenariat public-privé (PPP).
- Le câble de fibre optique est en train d'être posé à Pétionville.
- Il ne faut pas voir l'Etat en compétition avec les concessionnaires. L'Etat est aussi un opérateur, un investisseur. Il y a des provisions claires dans la nouvelle proposition de loi.
- Haïti peut s'inspirer de modèles de privatisations effectuées ailleurs, dans la région : République Dominicaine, Uruguay...
- Comment faire profiter à toute la communauté de cette autoroute ?
- Il faut que l'Etat central soit connecté aux collectivités pour une décentralisation des services.
- Construire aussi en tenant compte de l'existence de la dorsale mise en place par les opérateurs de téléphonie mobile.

11.- Mercredi 18:00 Heures – Secteur Bancaire et Financier – Chambre Franco

M. Maxime D. CHARLES, Directeur Scotia Bank, Président de l'APB

M. Claude PIERRE-LOUIS, Directeur Général SOGEBANK

Mme Greta GREATHOUSE, Directrice, HIFIVE / USAID

Mme Anne HASTINGS, FONKOZE

Mme. Michelle REMY, Directrice Opérations CAPITAL BANK

Marlène Sam

Après un rapide préambule sur l'objet de la mission, les participants abordent les points suivants :

1. L'importance acquise par les paiements électroniques.
2. Les problèmes liés au coût des ces transactions.
3. L'absence du cadre légal, même si la signature électronique est utilisée sur la base d'un accord entre le client et sa banque.
4. L'obligation faite aux agences de payer par l'intermédiaire de la Banque centrale.
5. L'existence d'un système embryonnaire d'e-payment.

6. Le système interbancaire (SPE).
7. Les progrès dans les discussions et rencontres avec le Parlement, mais le projet de loi n'est pas encore voté.
8. L'attitude positive des institutions internationales telles que le FMI pour accroître la lutte contre le blanchiment d'argent.
9. Les contraintes auxquelles les banques sont confrontées énormes en raison des limites au niveau de l'identification des individus.
10. Les gains de temps qui résulteraient, par exemple, dans l'enregistrement des sociétés et la création d'entreprises (allers et venues entre CFI, MCI, DGI, Presses Nationales,...), si ces paiements étaient autorisés.
11. Les banques sont prêtes et impatientes de se lancer dans les transactions électroniques et le Mobile banking. Certaines banques proposent déjà le Online service à leurs clients.
12. Les ATM existent, depuis des années, en Haïti, même si le nombre est limité : Sogebank en a plus d'une trentaine, à Port-au-Prince et au Cap ; Unibank en a 6 ; Scotia en compte 4.
13. Les banques reconnaissent qu'il y a une grande compétition entre elles, et pensent que les coûts d'exploitation seraient réduits par l'arrivée de ces nouveaux produits.
14. Les banques soulignent la nature et la composition de l'actionnariat (150, 70 actionnaires, tout au plus...) des institutions bancaires, même les plus grandes, lesquelles ont un impact sur leur gestion et leur expansion.
15. Le taux de pénétration bancaire est limité (20% de comptes courants ?) ...mais il est fonction du faible pouvoir d'achat de la population.
16. Le Mobile banking peut être une solution, et c'est imminent. Cependant, doivent être d'abord résolus les problèmes de sécurité des transactions ; les problèmes d'ordre juridique et il faut, aussi, pouvoir être en mesure d'éviter d'encourager le blanchiment d'argent.
17. Les institutions de micro finance pensent qu'il faudrait accroître le nombre de services de la part de l'administration publique pour favoriser l'e-Gouvernement.
18. Il faudrait, aussi, que l'assiette fiscale augmente.
19. Pour l'instant, c'est la Diaspora qui finance grandement la forte pénétration de la téléphonie mobile.
20. Une question est posée : les haïtiens sont-ils prêts ? La réponse est fournie par les résultats d'un récent sondage mené par une des institutions représentées :
21. Question : a.- Utilisez-vous des SMS : 40% Oui
b.- Avez-vous accès à un portable ? 80% Oui
c.- Recevez-vous des transferts de l'étranger ? 60 % Oui
22. En ce qui a trait au milieu rural : l'exemple des caisses populaires, fédérées, LE LEVIER, et qui ont créé leur réseau interconnecté et qui utilisent des cartes d'identité biométriques est cité.

En conclusion, il est convenu que le secteur bancaire et financier souhaite vivement revoir la Consultante lors de sa prochaine mission, pour discuter de l'état d'avancement du dossier e-Gouvernement et des perspectives de création d'une plateforme technologique pour l'administration publique.

Emotion is paramount in Haiti...

En Conclusion :

Madame Rubino a pu rencontrer, au cours de deux journées et demie, grâce à la coordination du Comité Exécutif GTIC et à M. Gary Olius, de la Représentation de la BID en Haïti, vingt-huit interlocuteurs représentant divers secteurs de la vie nationale, au cours de dix (10) entretiens individuels ou en groupe, d'une durée d'une heure au minimum.

Elle s'est entretenue avec le Premier Ministre et le Ministre du Commerce et de l'Industrie. Toutefois, il convient de noter l'impossibilité dans laquelle les organisateurs ont été de pouvoir lui faire rencontrer les cadres supérieurs du Ministère de l'Économie et des Finances, contrairement à ce qui avait été planifié. La rencontre a dû être annulée en raison de manifestations en centre ville et n'a pu être reprogrammée immédiatement, compte tenu des autres engagements.

Les entretiens et rencontres qui ont eu lieu ont tenté de lui permettre de mieux apprécier ou mesurer directement :

- L'étendue et la nature des attentes exactes du GTIC en vue de la réalisation de son double mandat de planification stratégique et de recommandations pratiques pour la mise en œuvre d'un plan d'e-gouvernement.
- de l'existence d'une volonté claire et fermement énoncée de la part de l'Exécutif, de progresser rapidement sur ce dossier.
- de l'intérêt généralement bienveillant, quoique diversifié (très variable selon leur maîtrise du sujet et des problématiques TIC), que les acteurs manifestent pour une planification stratégique voire une politique plus volontariste vis-à-vis de l'utilisation, le développement et de l'exploitation des TIC en Haïti.
- de leur connaissance et de leur convergence de vues sur les contraintes majeures liées à cet effort : le cadre légal, les infrastructures, les coûts, l'absence de coordination / vision / communication, le manque de ressources humaines qualifiées...
- de la capacité de plusieurs secteurs à saisir, accompagner, soutenir ou amplifier les chances et les opportunités offertes par les TIC : l'État ; les administrations chargées de collecter des données fiables pour la prise de décision ; la société civile, en vue de la mobilisation des citoyens à travers le pays, aussi bien en cas de catastrophes naturelles que dans le cadre du renforcement du processus démocratique ; les opérateurs de télécommunications ; l'université ; les entreprises du secteur privé bancaire ou autre...
- de la nécessité d'intensifier une meilleure promotion des enjeux, opportunités et avantages liés ou inhérents aux TIC, pour les secteurs socio-économiques moins directement « en contact », impliqués et concernés, aujourd'hui, par leur utilisation ou par leur exploitation.
- de leur prise de conscience ou de leur conviction que l'identification des citoyens représente une urgence – car elle serait un bond en avant considérable – par quasiment tous les secteurs : étatique, bancaire, financier, société civile,...
- des initiatives, ressources insoupçonnées, potentielles ; et
- d'appréhender d'autres éléments du contexte et du cadre existants sur lesquels capitaliser ou avec lesquelles coopérer ultérieurement.

GTIC

Groupe de Travail sur les Technologies
de l'Information et de la Communication

**ANNEXE 10 :
LES MEMBRES DU GTIC****Patrick Attié** (Coordonnateur)

Ingénieur en Génie Electronique Co-fondateur de l'Ecole Supérieure d'Infotronique d'Haïti (ESIH)
et du laboratoire Présence et Innovation (LPI, Réalité Virtuelle).

Stéphane Bruno (membre du Comité Exécutif)

Consultant en technologies de l'information et de la communication, Vice-Président de
l'Association Haïtienne pour le développement des TIC (AHTIC).

Henry Cassion

Entrepreneur et consultant, spécialiste en macroéconomie des économies ouvertes et en
économie internationale, maîtrise des méthodes statistiques et des techniques d'analyse de
données, PDG de Turbonet S.A.

Paolo Chilosi

Directeur de la Société Multilink, fournisseur d'accès Internet.

Charles Clermont

Titulaire d'un diplôme d'ingénieur de l'Institut National des Sciences Appliquées de Toulouse,
Vice-Président de la SOHFIDES, entrepreneur et créateur d'entreprises.

Jean Baden Dubois

Directeur de l'Unité responsable de la technologie à la BRH.

Jean Jaunasse Elysée (membre du Comité Exécutif)

Ingénieur, spécialisé en Télécommunications, Coordonnateur du RDDH et consultant spécialiste
en Télécommunications et en gouvernance.

Tayana Etienne (membre du Comité Exécutif)

Coordonnatrice du Master en Base de Données et Systèmes (MBDS) de la Faculté des Sciences
et Directrice Générale de la société Solutions.

Didier Fils-Aimé

Président du conseil d'administration de Hainet.

Régine Godefroy

Spécialiste en logistique et Directrice Générale de la société de services en ligne ecard

Bernard Gousse

Titulaire d'un Doctorat en droit de l'Université d'Aix-Marseille III, cofondateur et associé du Cabinet Pasquet, Gousse et Associés, ancien Ministre de la Justice, a aidé à la mise en place de la Chambre de Conciliation et d'Arbitrage de la Chambre de Commerce et d'Industrie d'Haïti.

Jean Vernet Henry

Ingénieur Agronome de formation et Recteur de l'Université d'Etat d'Haïti (UEH).

Schiller Jean Baptiste

Consultant indépendant pour les questions d'innovation technologiques en Haïti, l'un des premiers acteurs de l'introduction de l'Internet en Haïti et Coordonnateur de l'Organisation du Salon de l'Innovation 2008.

Jacky Lumarque

Recteur de l'Université Quisqueya (UNIQ) et Coordonnateur du Groupe de Travail sur l'Education (GTEF).

Nesmy Manigat

Directeur exécutif de la branche de l'ONG Aide et Action localisée en République Dominicaine, a travaillé pour Groupe Croissance.

Giovanna Ménard

Avocate de Formation, Directrice du département légal de Digicel.

Raymond Noel (membre du Comité Exécutif)

Ingénieur, Consultant spécialiste de l'accès en milieu rural et de la gouvernance, ancien Coordonnateur du projet AHSI-PNUD, fondateur de l'Observatoire Haïtien pour les TIC (OHPTIC), ancien membre du Conseil de Direction de la Faculté des Sciences (FDS).

Ralph Pereira

PDG de CompHaiti et ancien président de l'AHTIC, membre de la Chambre de Commerce et d'Industrie d'Haïti (CCIH).

Kesner Pharel

Détenteur d'une Maîtrise en Administration sportive de l'Université de Lyon, d'une Maîtrise en Administration Publique de la prestigieuse Université américaine de Harvard, il est depuis 1994 le PDG du Groupe Croissance.

Mathias Pierre

Ingénieur, entrepreneur , Président de l'Association Haïtienne pour le développement des TIC (AHTIC), membre du conseil d'administration de plusieurs associations du secteur privé comme la AmCham, CHDC et Vice-Président de la Chambre de Commerce et d'Industrie de l'Ouest (CCIO), PDG du Groupe GaMa regroupant GaMa Consulting S.A. et GaMa Entreprises S.A.

Geneviève Poitevien

Médecin, Interniste et cardiologue; doyenne de la Faculté de Médecine de l'Université Quisqueya (UNIQ), trésorière adjointe de l'Association Médicale Haïtienne, membre fondateur du Collège Haïtien de Cardiologie et de l'Association des Femmes Professionnelles en Haïti.