CADRE JURIDIQUE DE LA CYBER-SECURITE DANS L'ESPACE FRANCOPHONE

Étude réalisée par :

Fayçal AJINA

Vice procureur

Sommaire exécutif

La prolifération des textes juridiques relatifs à la cyber sécurité est une réalité commune au sein de l'espace francophone. En effet, l'écart manifeste entre les pays ayant en partage l'usage du français dans le passage au modèle de la société d'information est partiellement comblé au niveau du cadre juridique de la cyber sécurité.

Ce rapport montre que la zone de « non droit » n'existe plus dans l'espace numérique francophone. La juridisation accompagne le développement des technologies de l'information et des communications et se présente pour l'ensemble de la communauté un pilier des politiques de cyber sécurité.

Ce mouvement se caractérise par une harmonie des principes généraux qui se fonde sur l'uniformité des sources du droit de la cyber sécurité. L'influence du droit communautaire est certaine. Elle est le plus souvent véhiculée par le rayonnement de la France sur l'ensemble des pays francophone et l'assistance technique des experts européens dans le cadre des programmes spécifiques de coopération.

Par ailleurs, l'évolution du cadre juridique dans les pays francophones ne cache pas la fosse qui existe au niveau de l'efficacité entre le groupe des pays développés et le groupe des pays en voie de développement. Pour le dernier, les moyens ne se sont pas à la hauteur des politiques adoptées.

Faut-il ajouter que, pour les uns et les autres, le contenu du droit de la cyber sécurité est encore floue, allant du domaine de la défense et de la sécurité à la vie privée en passant par le domaine économique et social.

En plus l'arsenal juridique est composé de textes éparpillés, de nature différente et qui sont, le plus souvent difficilement consultables.

Au vu de ces constatations, le rapport recommande de renforcer les aspects positifs de cette évolution en intégrant la formation juridique dans les cursus de formation générale sur la cyber sécurité et en appuyant l'harmonisation du cadre juridique.

Enfin, le rapport propose quelques solutions pour pallier à certaines insuffisances qui visent particulièrement le renforcement de l'efficacité du cadre juridique par le biais de la coopération bilatérale et multilatérale dans l'espace francophone.

1. INTRODUCTION

1.1 Notion de cyber-sécurité :

La cyber-sécurité n'est pas définie juridiquement. La doctrine n'a pas réussi à proposer une définition qui fait l'unanimité malgré les différentes tentatives pour cerner la notion et en tracer les contours, ainsi que les efforts de standardisation menés par les instances internationales, régionales et certaines expériences nationales.

Cette situation a affecté la signification et la teneur de la notion, qui varient selon les propositions avancées ;elle est encore floue et à contenu variable allant du domaine de la défense et de la sécurité àla vie privée en passant par le domaine économique et social.

Pour les besoins de la présente étude, nous avons choisi de nous référer à la définition proposée par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) français. Dans son document publié en février 2011 et intitulé « *Défense et sécurité des systèmes d'information – Stratégie de la France* », la cyber-sécurité est définie comme « *l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cyber sécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.* »

Ainsi, la notion de cyber-sécurité comprend les trois composantes suivantes :

- les mesures de protection contre les menaces et les attaques ;

- la cyberdéfense définie dans le même document comme étant « *l'ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels* » ;

- la cybercriminalité.

La première et la deuxième composante sont de la même nature et comprennent des mesures qui visent à prévenir les menaces accidentelles et les attaques intentionnelles et à garantir le rétablissement du bon fonctionnement des systèmes d'information et la disponibilité de l'information.

La troisième composante est d'une nature différente ; elle comprend les mesures nécessaires pour incriminer les atteintes aux systèmes d'informations et tous les abus dans l'usage de ces systèmes, ainsi que la détection et la répression de ces infractions.

Cette approche globale est préconisée par le Groupe d'experts gouvernemental à composition non-limitée pour la réalisation d'une étude approfondie sur la cybercriminalité (ci-après, le Groupe), créé en vertu de la Résolution n° 65/230 de l'Assemblé Générale des Nations Unies du 21 décembre 2010. Le Groupe a recommandé dans son étude l'intégration des stratégies contre la cybercriminalité avec une perspective plus large de cyber-sécurité.

1.2 Droit de la cyber sécurité :

Le droit de la cyber-sécurité n'est pas reconnu en tant que branche indépendante de droit ou même en tant que discipline du droit de l'informatique. Il serait, à la lumière de la notion de la cyber-sécurité telle que définie dans le document stratégique susmentionné, l'ensemble des règles juridiques qui visent à prévenir les menaces et les attaques dirigées contre les systèmes d'information et à réprimer celles qui sont commises intentionnellement.

Cette simplification a le mérite de cerner l'objet de notre Rapport mais, elle éclipsele caractère transversal de ce droit, qui rend la recherche et la classification de l'information une tache pénible.

En effet, les règles préventives ou encore les règles de sécurité informatique sont éparpillées dans plusieurs textes appartenant à des branches différentes de droit, et ne cessent de se proliférer dans d'autres textes spécifiques et sectoriels.

Quant au droit de la cybercriminalité,il ne se trouve pas nécessairement dans le Code pénal et leCode de procédure pénale. En effet, s'il ne fait pas l'objet d'une loi spécifique, il est éparpillé dans plusieurs textes juridiques.

La présentation de l'état de la législation par pays va nous montrer le degré de cette difficulté.

2. FICHES PAYS

La recherche de l'information juridique sur la cyber sécurité par pays n'est pas facile pour de multiple raisons. En effet, peu de pays francophones disposent d'un système d'information juridique qui permet une recherche simple de l'information juridique consolidée. Tel est le cas de la France qui diffuse ce type d'information sur son portail « *Légifrance* ». Par contre, la plupart des pays francophones diffusent l'information juridique sur les sites de leurs agences spécialisées ou dans des bases de données administrées par des organisations internationales. Pour les uns et les autres, le chercheur est obligé de déterminer lui-même les critères de sa recherche et ce, en absence de codification des textes relatifs à la cyber sécurité. Le plus souvent, il est obligé de se contenter des informations produites par les administrateurs concernés. A cet égard, il appert que l'information diffusée n'est pas toujours actualisée.

Pour les besoins de cette étude, nous avons choisi de présenter les informations juridiques consolidées à la date de sa réalisation pour donner une idée réelle sur l'état des lieux et montrer l'évolution de l'arsenal juridique de la cyber sécurité dans la zone francophone.

Par ailleurs, si la difficulté de la recherche de l'information juridique consolidée ne nous permet pas d'étendre notre étude sur un éventail large de juridictions francophones, elle ne nous a pas empêché de couvrir la plupart des zones géographiques de la francophonie. Les pays sélectionnés représentent un nombre important de groupe régional et de traditions juridiques différentes.

Ainsi, la France représente la tradition du droit continental de l'Europe occidental, alors que le Canada est le modèle le plus proche de la tradition du « Commun Law » de la zone d'Amérique. Les autres pays ont été choisis pour représenter trois groupes différents de l'Afrique francophone allant de la méditerranée au nord vers l'océan indien au sud en passant par l'ouest subsaharien.

Faut-il signaler toutefois, que la réparation par région n'a pas un intérêt académique significatif. En effet, à l'instar de la communauté internationale, la communauté francophone est divisée en deux groupes ; le groupe des pays développés, situés principalement en Europe occidentale et le Canada et le groupe des pays en voie de développement répartis dans toutes les autres régions de la communauté. La fracture numérique entre ces deux groupes est nette sur tous les aspects liés à l'informatisation y compris, bien évidemment la cyber sécurité.

Ce constat est confirmé par les données présentées dans les fiches pays ci-après.

2.1 France

2.1.1 Présentation générale :

Localisation : Europe Occidentale (France métropolitaine)
Superficie :672 369 Km^2(métropole – outre-mer – autres territoire)
Habitant : 66 millions
Situation économique : 6ème ou 9ème puissance économique dans le mondeselon le mode de calcul du PIB

2.1.2 Cadre juridique :

2.1.2.1 La sécurité informatique :

Structure : Le décret n° 2009-834 du 7 juillet 2009 portant création de l'Agence nationale de la sécurité des systèmes d'information ;
Règles : les principales dispositions se rapportantà la sécurité informatique sont prévues par les textes suivants

- Code de la défense : de l'article L 1332- 1 à l'article L 1332 -6 – 6 ; (sécurité des systèmes d'information)

https://www.legifrance.gouv.fr

- Code des postes et des communications électroniques : article L 32-1 ; (sécurité des réseaux et des communications)

- Loi 78 – 17 du 6 janvier 1978 relative à l'information, aux fichiers et aux libertés (sécurité des données à caractère personnel) https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique(signature électronique et cryptologie)
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (Sécurité des échanges électroniques).

2.1.2.2 La cybercriminalité :

Incrimination

Code pénal :
  - Le non-respect des règles relatives au traitement des données à caractère personnel : de l'article 226-16 à l'article 226-17
  - Pornographie infantile : article 227-23
  - Atteintes aux systèmes automatisés de traitement des données ; de l'article 323-1 à l'article 323-8

Code monétaire et financier :
  - Falsification d'un instrument de payement : Les articles L 133-4 et L163-3

Code de la propriété intellectuelle :
  - Protection des logiciels : R335-2

Procédure :

Code de procédure pénale :
  - Constatation des infractions et enquête
  - Collecte des preuves électroniques
  - Coopération internationale

Code des postes et des communications électroniques
  - Conservation des données
  - Interception des communications

2.1.3 Aperçu général :

L'arsenal juridique français est relativement ancien mais il n'a pas cessé d'évoluer et de s'élargir pour couvrir tous les aspects liés à l'usage des systèmes d'information. Sommairement il se distingue par les caractéristiques suivantes :

- Un arsenal juridique fortement encadré par :
  - Un droit communautaire imposant
  - Une stratégie nationale évolutive

- Un arsenal juridique global : qui couvre tous les aspects de la cyber-sécurité tel que définie dans le document stratégique ;
- Un arsenal juridique souple : l'essentiel des règles relatives à la sécurité informatique sont versées dans des textes situés en bas de la hiérarchie des normes juridiques et qui peuvent être produites et ajustées rapidement. Les lois susmentionnées contiennent des règles générales qui sont déclinées d'une façon détaillée dans des textes réglementaires mais surtout dans la forme de règlement ou des instructions interministérielles ou même de référentiel
- Un arsenal juridique composé de textes éparpillés qui rend la visibilité et la consultation difficile malgré l'utilisation de la technique de codification à droit constant.

2.2 Canada

2.2.1 Présentation générale :

Localisation : Amérique du nord

Superficie : 9 984 670 km²

Habitant :35,86 millions d'habitants

Situation économique :11ème puissance économique dans le monde (PIB)

2.2.2 Cadre juridique :

2.2.2.1 La sécurité informatique :

Structure :

- Centre canadien de réponses aux incidents cybernétique (CCRIC) ; centre qui relève du ministère de la sécurité publique au gouvernement fédéral
- Centre de la sécurité des télécommunications Canada (CSTC) ; centre qui relève du ministère de la défense

Règles : les principales dispositions se rapportantà la sécurité informatique sont prévues par loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications (L.C.2010, ch. 23)
http://laws-lois.justice.gc.ca/fra/lois/E-1.6/index.html

Deux règlements sont pris en application de cette loi :

- Règlement sur la protection du commerce électronique (CRTC) (DORS/2012-36)
- Règlement sur la protection du commerce électronique (DORS/2013-221)

2.2.2.1 La cybercriminalité :

Incrimination

Code criminel :

- Atteintes la confidentialité, intégrité et disponibilité des données et des systèmes :les articles326, 327, 334, les articles de 183 à 190, les articles de 193 à 194 et l'article 430;
- Fraude, falsification et usurpation d'identité : les articles 342 et 342-1, 402-1, 402-2 et 403 ;
- Accès illégal, interception des communications et abus du dispositif informatique : les articles 342-1 et 342-2 et les articles 191 et 192
- Atteintes à l'intégrité physique par un système d'information : article 372 ;
- Voyeurisme : article 162 ;
- Pornographie infantile : les articles 163-1, 164, 164-1, 164-2, 164-3, 171-1, 172, 172-1 et 172 ;

Procédure :

Code criminel :

- Constatation des infractions et enquête
- Collecte des preuves électroniques
- Loi sur l'extradition (L.C. 1999, ch. 18)
- Loi sur l'entraide juridique en matière criminelle (L.R.C. (1985), ch. 30 (4e suppl.))

2.2.3 Aperçu général :

Le système juridique canadien est particulier à deux niveaux :

- Un système hybride influencé par le système de Common law et le système du droit continental
- Un système fédératif qui observe un partage complexe entre les compétences juridiques des Etats provinces et de l'Etat fédéral

Malgré ces particularités le droit canadien de cyber-sécurité est fortement influencé par le droit européen surtout dans son aspect relatif à la lutte contre la cybercriminalité. Quant aux aspects liés à la sécurité informatique leschamps d'intérêts du droit canadien sont similaires à ceux des pays développés et qui ont un degré très élevé d'informatisation et de connectivité.

- Défense et sécurité : la cyber sécurité est un axe essentiel de la politique de défense non militaire et de sécurité publique dans l'objectif est de préserver l'intégrité du cyber espace et de sauvegarder la souveraineté sur les infrastructures et les données ;
- Sauvegarde des intérêts économiques de l'Etat en participant à la protection des infrastructures critiques et en aidant les canadiens en général, et les entreprises économiques, en particulier, à se protéger.
- Protection de la vie privée en assurant par une intervention juridique très affichée la confidentialité des renseignements personnels

Le législateur canadien est soucieux de créer une synergie entre ces intérêts qui sont omniprésents dans la plupart des textes qu'il décrète.

La volonté d'appliquer la loi est exprimée par :

- Un leadership de haut niveau qui assure une coordination nationale et internationale
- Une vision assez claire versée dans un document de politique générale qui intègre les efforts de tous les intervenants au niveau fédéral et provincial et le secteur privé ;
- Des mesures efficaces pour l'application de la loi (exemple : unité spéciale d'enquête à la gendarmerie royale du canada)

2.3 Tunisie

2.3.1 Présentation générale :

Localisation : Afrique du nord

Superficie : 163.610 km²

Habitant :11,1 millions

Situation économique : Rang 84 parPIB nominale

2.3.2 Cadre juridique :

2.3.2.1 La sécurité informatique :

Structure : Agence Nationale de Sécurité Informatique crée en vertu de la loi n° 5 - 2004 du 3 février 2004Loi n° 5 - 2004 du 3 février 2004

Règles :

- Loi n° 2004-5 du 3 février 2004 fixant les règles générales de protection des systèmes informatiques et des réseaux.
- Loi organique Loi organique n° 2004-63 du 27 juillet 2004portant la protection des données à caractère personnel.
- Loi n° 2000-83 du 9 août 2000, relative aux échanges et au commerce électroniques (certification et signature électronique)
- Code des télécommunications (2001) : article 9 (homologation et cryptage)
- Loi n° 2005-51 du 27 juin 2005 relative au transfert électronique de fonds

2.3.2.2 Cybercriminalité

Incrimination

Code pénale :

- Accès illégal, atteinte à l'intégrité des données et entrave au bon fonctionnement des systèmes : article 199 bis
- Falsification informatique : articles 199 ter et 172

Procédure

- Code de procédure pénale : règles de droit commun de poursuite, instruction et jugement
- Décret n° 2013-4506 du 6 novembre 2013, relatif à la création de l'agence technique des télécommunications et fixant son

organisation administrative, financière et les modalités de son fonctionnement : Article 2 : L'agence technique des télécommunications assure l'appui technique aux investigations judiciaires dans les crimes des systèmes d'information et de la communication, elle est à cet effet chargée des missions suivantes :

- la réception et le traitement des ordres d'investigation et de constatation des crimes des systèmes d'information et de la communication issus du pouvoir judiciaire conformément à la législation en vigueur.
- la coordination avec les différents opérateurs de réseaux publics de télécommunications et opérateurs de réseaux d'accès et tous les fournisseurs de services de télécommunications concernés, dans tout ce qui relève de ses missions conformément à la législation en vigueur.
- l'exploitation des systèmes nationaux de contrôle du trafic des télécommunications dans le cadre du respect des traités internationales relatifs aux droits de l'Homme et des cadres législatifs relatifs à la protection des données personnelles.

2.3.3 Aperçu général :

L'essentiel des textes relatifs à la cyber sécurité ont vu le jour entre 1999 et 2005. Ce mouvement législatif a accompagné la libération du secteur des technologies de l'information et des communications et a constitué un socle pour créer des structures dynamiques et développer une expertise technique assez riche. Cependant les limites de ce cadre juridique sont de plus en plus ressenties et pèsent lourdement sur l'ensemble des acteurs et de l'économie du pays.

En effet les différents textes sont relativement anciens par rapport à l'état de la technologie et du savoir et souffrent de plusieurs lacunes.

L'absence d'une vision stratégique globale et intégrée se traduit par les incohérences textuelles et la faiblesse de réactivité du système.

Les projets en cours pour améliorer le cadre juridique de cyber sécurité traine à voir le jour à cause de la situation transitoire du pays.

2.4 Sénégal

2.4.1 Présentation **générale :**

Localisation : Afrique occidentale

Superficie : 196 722 km2

Habitant : 13 ,508millions

Situation économique : Rang120 par PIB nominale

2.4.2 Cadre juridique :

2.4.2.1 La sécurité informatique :

Structure : Service technique central des chiffres et de la sécurité des systèmes d'information crée en vertu du décret n° 2007-909 du 31 juillet 2007 portant organisation de la présidence de la république.

Règles :

- Décret n° 2007-909 du 31 juillet 2007 portant organisation de la présidence de la république et fixant les missions du service technique central des chiffres et de la sécurité des systèmes d'information.
- Loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques
- Loi n° 2008-10 du 25 janvier 2008 portant loi d'orientation sur la Société de l'Information (LOSI)
- Loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel
- Loi n° 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal.
- Loi n° 2011-01 du 24 février 2011 portant Code des télécommunications

2.4.2.2 Cybercriminalité

Loi n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité

Incrimination

Code pénale :

Infractions liées aux technologies de l'information et de la communication : les articles 431-7 à 431-65

- Atteintes aux systèmes informatiques.
- Atteintes aux données informatisées
- Abus du dispositif
- Infractions se rapportant au contenu
- Infractions liées aux activités des prestataires techniques de services de communication au public par voie électronique
- Infractions liées à la publicité par voie électronique
- Atteintes aux biens
- Infractions commises par tous moyens de diffusion publique
- **Atteintes à la défense nationale**

Procédure.

Code de procédure pénale :

La procédure en matière d'infractions commises au moyen des technologies de l'information et de la communication :lesarticles 677-34 à 677-42

- Conservation rapide de données informatisées archivées
- Perquisition et de la saisie informatique
- Interception des données informatisées
- Preuve électronique en matière pénale

2.4.3 Aperçu général :

L'année 2008 a marqué le système juridique de cyber sécurité en Sénégal. La promulgation simultanée de plusieurs textes touchants le cyber espace suppose que l'action était réfléchie et coordonnée. En effet les lois sur les transactions électroniques, la protection des données à caractère personnel, la lutte contre la cybercriminalité, la cryptologie et le code des télécommunications ont été précédé par une loi d'orientation générale sur la société d'information qui encadre l'ensemble du corpus et trace la vision du pays pour le secteur.

Par ailleurs le Sénégal a largement bénéficié des meilleures pratiques internationales et régionales pour se faire doter d'un cadre juridique moderne et largement suffisant pour répondre au besoin du développement du secteur des technologies de l'information et des communications.

2.5 cote d'ivoire

2.5.1 Présentation générale :

Localisation : Afrique subsaharienne

Superficie : 322.463 km²

Habitant : 22,7 millions d'habitants

Situation économique : Rang95 par PIB nominale

2.5.2 Cadre juridique :

2.5.2.1 La sécurité informatique :

Structure : CI-CERT centre spécialisé de l'autorité de régulation des télécommunications crée en vertu de l'ordonnance n° 2012-293 du 21 mars 2012 relative aux Télécommunications et aux technologies de l'Information et de la communication

Règles :

- Ordonnance n° 2012-293 du 21 mars 2012 relative aux Télécommunications et aux technologies de l'Information et de la communication
- Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel
- Loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques

2.5.2.2 Cybercriminalité

Incrimination

Loi n° 2013-451 relative à la lutte contre la cybercriminalité

- o Infractions spécifiques aux technologies de l'information et de communication
- o Atteintes à la propriété intellectuelle
- o Agissements illicite sur les réseaux de communicationélectronique
- o Responsabilité des prestataires techniques de services en ligne

- Adaptation des infractions classiques aux technologies de l'information et de communication

Procédure.

Loi n° 2013-451 relative à la lutte contre la cybercriminalité

- Procédure pénale en matière de cybercriminalité : les articles de 71 à 78

2.5.3 Aperçu général :

D'après la banque mondiale « depuis quatre ans, la Côte d'Ivoire connaît un succès économique impressionnant, illustré par une croissance rapide du PIB qui a fait reculer la pauvreté ». Les indicateurs économiques montrent que tous les secteurs ont profité d'une demande globale vigoureuse et d'une poussée de l'investissement autant privé que public.

Ceci étant, cette émergence économique est accompagnée par un mouvement de modernisation juridique qui a touché la cyber sécurité. Les textes fondateurs se rapportant à ce secteur sont parus en 2012 et 2013 et ont profité lors de leur élaboration d'une assistance technique internationale qui a fait bénéficier le pays des bonnes pratiques internationales.

La jeunesse de l'expérience juridique ivoirienne n'a pas caché un apport particulier intéressant qui consiste à regrouper les prérogatives essentielles en matière de cyber sécurité chez l'autorité de régulation des télécommunications.

En effet, l'ARTCI initialement chargée de la régulation des télécoms, s'est vu confier des missions nouvelles par le législateur. A ce titre, elle est l'autorité de protection des données à caractère personnel (article 46 de la loi 2013-450), l'autorité chargées à veiller à la sécurité des réseaux et des systèmes d'information (article 50 de la loi 2013-546)et enfin l'autorité compétente d'investigation et de recherche en matière de cybercriminalité (article 71 de la loi sur la cybercriminalité).

Cette concentrationdes compétences peut être utile pour améliorer l'efficacité du système.

2.6 Madagascar

2.6.1 **Présentation générale :**

Localisation : Etat insulaire de l'océan indien au sud-est de l'Afrique

Superficie : 587 000 km^2

Habitant :24,24 millions d'habitants

Situation économique : Rang135 par PIB nominal

2.6.2 **Cadre juridique :**

2.6.2.1 La sécurité informatique :

Structure :

- Ministère des technologies d'information et de communication

Règles :

- Loi n°2014-026 du 5 novembre 2014 fixant les principes généraux relatifs à la dématérialisation des procédures administratives
- Loi n°2014-025 du 5 novembre 2014 sur la signature électronique
- Loi n° 2014 – 038 Sur la protection des données à caractère personnel du 16 décembre 2014

2.6.2.2 Cybercriminalité

Incrimination

Loi n°2014-006 sur la lutte contre la cybercriminalité du 19 juin 2014

- Délits relatifs aux systèmes d'information
- Les atteintes aux personnes par le biais d'un système d'information

Procédure.

Loi n°2014-006 sur la lutte contre la cybercriminalité du 19 juin 2014

- Des opérateurs et prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications ou de communications électroniques

2.6.3 Aperçu général :

Madagascar est parmi les pays le plus pauvre au monde. En pleine période de transition politique, le nouveau parlement, issue d'un long processus de conciliation nationale, n'a pas tardé a adopté en 2014 une série de textes qui touchent directement la sphère de la cyber-sécurité. Ces lois ont profité à l'instar des lois parues à la même époque dans plusieurs pays de l'Afrique d'une expertise internationale.

Le contexte de ces lois est bien différent à plusieurs égards. L'absence d'une structure spécialisée dans la sécurité des systèmes d'information est une illustration de la précocité de l'expérience. Le Madagascar se contente actuellement de recevoir une assistance à distance à partir de la France. Le décalage entre le texte et le contexte est très net, laissant des doutes sur l'efficacité et l'efficience du système juridique.

3. ANALYSE GENERALE

Les pays francophones sont divisés en deux catégories : les Etats développés, d'une part, et les pays en voie de développement d'autre part.Cette réalité est vérifiée sur tous les plans. La fracture numérique est très nette entre les deux catégories malgré les efforts soutenus de certains pays pour accélérer le passage à la société d'information. Sur le plan juridique, les différences au niveau de l'expérience, du champ de couverture ainsi que l'abondance des règles sont remarquables. La France et leCanada possèdent des textes anciens qui ne cessent de se développer et de se renforcer par d'autres textes pour couvrir des domaines multiples en se collant au mouvement de l'informatisation et de la connectivité. Les autres pays ont une expérience récente et lacunaire dans l'ensemble, à des degrés variables.

Mis à part ce décalage, le bilan des cas étudiés est encourageant ; il fait ressortir les remarques suivantes :

3.1 Le droit envahit le cyber espace

Malgré les divergences entre les pays ayant en partage l'usage du français, ils se rassemblent par la prolifération de textes juridiques qui visent à encadrer le cyber espace. D'ailleurs ce mouvement est universel puisqu'il répond aux besoins de l'Homme à réguler ses relations indépendamment de la nature de l'environnement dans lequel se nouent et se gèrent ses relations.

En effet, du moment où le cyber espace est devenu un levier des échanges sociaux et économiques, le droit est naturellement invité à conquérir cet espace pour imposer l'ordre, facteur indispensable de stabilité et de progrès.

Certes, la juridisation se fait à des vitesses variables selon le niveau d'intégration des technologies d'information et de communication, mais elle tend à se généraliser progressivement pour atteindre le même niveau d'informatisation et de connectivité.

Ainsi, la zone du non-droit (selon le vocabulaire de Jean Carbonnier) n'existe plus dans l'espace francophone, témoignant d'une transformation radicale des Etats vers le modèle de sociétés d'information. Cette transformation est très visible dans les pays du nord, dits développés, et elle est de plus en plus constatée dans les pays en voie de développement et, en particulier,les pays de l'Afrique qui enregistrent chaque année des chiffres intéressants de développement.

La forme de la juridisation diffère selon les traditions de chaque Etat, mais l'influence du droit continental est évidente vu les liens historiques et culturels avec la France.

L'intervention des législateurs se fait par le biais de lois spéciales ou des lois modifiant des textes anciens pour intégrer des nouvelles dispositions en relation avec la cyber sécurité.

La loi n'est pas la seule forme utilisée par les pays francophones. Les règlements trouvent leur place dans le corpus juridique. Cette souplesse est plus visible dans les pays du nord qui ont une capacité d'adaptation et une plus grande réactivité. Les autorités françaises interviennent le plus souvent par des instructions interministérielles et des règlements qui sont décrétés rapidement.

Parfois, cette souplesse est absente,surtout dans les pays qui passent par une transition politique et pour les matières qui exigent le respect du principe de la légalité. Les changements successifs des pouvoirs publics bloquent le processus législatif et freinent le développement du cadre légal et son adaptation à la réalité économique et sociale.Le cas du projet de loi sur la cybercriminalité en Tunisieest significatif. Ce projet a été présenté pour la première fois en 2010, mais il n'a pas été adopté par le pouvoir législatif jusqu'à présent.

Faut-il signaler à cet égard que la diversité des formes des textes juridiques contribue au manque de lisibilité du cadre juridique. La recherche de l'information juridique pertinente est difficile, surtout pour les pays qui ne possèdent pas un système de traitement automatique dédié à ce type d'information.

3.2 Uniformité des sources du droit de la cyber-sécurité

3.2.1 La convergence vers le droit communautaire

La lecture des textes promulgués récemment dans plusieurs pays de l'Afrique montre les ressemblances certaines entre ses textes.

Le droit communautaire en matière de cyber-sécurité est une source formelle directe du droit national des pays européens, mais qui continue à rayonner en dehors de l'espace européen et de servir de modèle ou de source matérielle pour les nouvelles législations extra-communautaires.

En effet, les conventions du conseil de l'Europe sont ouvertes à l'adhésion des pays non européens ; c'est le cas par exemple de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite Traité 108. L'Ile Maurice est membre à la Convention, le Maroc et la Tunisie ont déposé une demande d'adhésion. C'est aussi le cas de la Convention sur la cybercriminalité dite Convention de Budapest de 2001. Le Canada, L'Ile Maurice et la République Dominicaine sont membres à la convention, le Maroc et le Sénégal ont, quant à eux, déposé des demandes d'adhésion.Pour ces pays, le droit communautaire est une source directe de leurs droits.

Les autres Etats sont largement influencés par ce droit pour les raisons suivantes :

- La France est un partenaire privilégié des pays francophones. Son droit est une source d'inspiration et un modèle à suivre au point que certains pays se contentent de transposer littéralement des dispositions entières de ce droit.
- La coopération étroite entre certains pays francophones appartenant au même groupe régional facilite l'harmonisation des législations et l'échange des expériences et des informations juridiques ;
- Le recours à l'assistance technique et le bénéfice de programmes d'appui similaires, financés par des instances ou des Etats européens.

L'harmonisation sur la base du droit communautaire est renforcée par l'influence exercée sur le droit africain. La convention de l'Union Africaine sur la cyber-sécurité et la protection des données à caractère personnel, adoptée le 27 juin 2014 à Malabo, est une reproduction fidèle des dispositions pertinentes des traités européens. La convention Arabe de Lutte Contre les Infractions Liées à la Technologie de l'Information de 2010 n'a pas échappé à cette règle.

3.2.2 La divergence sur l'instrument international

La francophonie est à l'instar de la communauté internationale divisée en deux groupes à propos de la nécessité d'un instrument juridique international de lutte contre la cybercriminalité. Les Etats-parties à la convention de Budapest soutiennent la reconnaissance de l'universalité de la convention et ne partagent pas l'idée d'établir un autre instrument international pour uniformiser les mesures juridiques de lutte contre ce phénomène et faciliter la coopération internationale en la matière. L'adhésion des Etats-Unis d'Amérique, du Canada, du Japon et de l'Australie à la Convention a donné un élan important pour cette idée.

A l'opposé, les Etats appartenant au Groupe 77,dont notamment la plupart des pays francophone de l'Afrique, et la Chine considèrent que la Convention est régionale, d'où la nécessité d'adopter un instrument international sous l'égide des Nations-Unies.

Cette opposition frontale sur le plan politique n'a pas pris d'ampleur sur le plan juridique.

En effet, certains pays francophones ont dépassé cette polémique en adhérant ou en demandant l'adhésion à la Convention.

Pour les autres, leur refus de signer la Convention ne les a pas empêchés d'en transposer les dispositions dans leurs droits nationaux.

En plus, le Groupe d'experts crée par l'Assemblé Générale des Nation-Unies pour élaborer une étude sur la cybercriminalité, n'a pas proposé à ce jour un projet différent.

La Convention est ainsi une source directe pour les uns et une source d'inspiration pour les autres.

3.3 Le caractère transversal du droit de la cyber-sécurité :

Le cadre juridique de la cyber-sécurité est composé de plusieurs textes juxtaposés. Chaque texte porte sur un aspect particulier de la matière et aucune expérience n'a essayé de codifier ce droit. L'étude nous montre que ce droit est constitué autour d'un ensemble de dispositions qui en constituent le noyau dur et des règles qui ne cessent de se multiplier, soit sous forme de textes spéciaux, soit sous forme de dispositions particulières dans des textes sectoriels.

3.3.1. **Le noyau de ce droit se compose des textes portant sur les aspects suivants :**

1- La sécurité technique des systèmes d'information :

Les pays du nord possèdent une réglementation développée portant essentiellement sur les conditions techniques de l'exploitation des systèmes d'information et les obligations des responsables de la sécurité de ses systèmes. Parmi les pays du sud, l'expérience de la Tunisie est remarquable à cet égard par l'instauration de l'audit périodique obligatoire. Cette catégorie contient aussi les règles de la cyber-défense qui visent à garantir la sécurité des infrastructures jugées essentielles ou critiques.

La place qu'occupent ces règles diffère d'un pays à l'autre mais, en général, deux attitudes sont observées :

- La sécurité technique des systèmes relève du domaine de la défense et de la sécurité publique ; c'est le cas pour les pays développés ;
- La sécurité technique des systèmes relève du service public des technologies d'information et de communication, placé soit sous

l'autorité d'un ministère technique, soit sous l'autorité suprême du pouvoir exécutif.

2- **La protection des données à caractère personnel :**

Dans tous les cas étudiés, la cyber-sécurité vise à garantir le respect de la vie privée et des données à caractère personnel lors du traitement automatisé de ces données. Les fondements des principes directeurs de cette protection sont les instruments internationaux relatifs au respect des droits de l'Homme et des libertés individuelles et qui sont le plus souvent reproduites dans les constitutions.

3- **La cryptologie :**

Les règles relatives à la technique du cryptage sont les plus anciennes et constituent pour certains pays le socle du cadre institutionnel et juridique. Les services techniques des chiffres sont généralement les précurseurs des CERTs.

En plus, la cryptologie est fortement militarisée vu le besoin des armées et des corps paramilitaires pour préserver le secret de leurs données et de leurs communications.

Le commerce électronique a donné un nouvel élan à cette technique, qui assure actuellement la sécurisation des échanges électroniques.

La réglementation relative au cryptage couvre la chaine de la mise à disposition de ce service et en, particulier, l'homologation du dispositif et la fourniture des services.

4- **La signature électronique :**

Tous les pays concernés par cette étude reconnaissent la valeur juridique du document électronique et de la signature électronique, outils indispensables des échanges électroniques et en particulier du commerce électronique.

Par ailleurs, cette reconnaissance ne vise pas uniquement la concurrence du document écrit, elle est considérée, aussi, comme étant une technique efficace pour renforcer la sécurité des échanges. En effet, si le cryptage est la technique des professionnels, la signature et orientée vers le grand public pour assurer un minimum de sécurité.

La signature électronique nécessite la mise en place d'un système de certification et l'organisation institutionnelle et juridique des activités liées à la fourniture de cette technique.

5- La cybercriminalité :

Le droit pénal constitue la clef de voûte du droit de la cyber-sécurité. Il permet de combattre les actes malicieux qui enfreignent la réglementation sur le cyberespace.

Le droit pénal contient des dispositions substantielles qui déterminent les actes incriminés et les sanctions. Les infractions en matière de cybercriminalité sont réparties en quatre catégories :

- Les atteintes ciblant les systèmes d'information objet d'infraction : il s'agit des atteintes à l'intégrité, la confidentialité et la disponibilité des systèmes et des données ;
- Les systèmes d'information, moyen d'infraction : il s'agit des infractions informatiques et de toutes autres infractions commises par l'utilisation d'un dispositif informatique ;
- Les systèmes d'information, support d'un contenu illégal : la pornographie infantile est l'infraction type de cette catégorie ;
- Les atteintes aux droits de la propriété intellectuelle.

Les lois sur la cybercriminalité dans les pays francophones sont largement conformes à cette typologie, mais le contenu des dispositions diffère d'un pays à l'autre. Les importants écarts sont constatés dans les deux dernières catégories et nécessitent un effort soutenu d'harmonisation.

Par ailleurs, le droit pénal contient des dispositions relatives à la procédure. Les pays francophones n'ont pas traité ce volet de la même manière. En général, on constate une économie d'effort dans la mise en place d'un système efficace d'application de la loi répressive. Certains pays ont négligé cet aspect malgré son importance capitale dans la lutte contre la cybercriminalité. Par contre, la procédure est au centre des politiques pénales des pays développés. Pour cet aspect, les moyens déterminent la politique.

Les règles procédurales se rapportent aux trois aspects suivants :

- La collecte des preuves électroniques : les procédures spécifiques sont applicables aux infractions cybernétiques et à toutes les autres infractions ;
- La compétence juridictionnelle : les infractions cybernétiques sont le plus souvent transnationales et requièrent la reconnaissance du principe de la compétence universelle pour assurer l'efficacité de la répression. Cependant, peu de pays sont libérés de leur système

classique d'attribution de la compétence juridictionnelle internationale ;

- La coopération internationale : la lutte contre la cybercriminalité exige des Etats une volonté réelle de s'affranchir des voies ordinaires de coopération internationale et la mise en place d'un réseau opérationnel permanent pour répondre instantanément aux demandes de coopération. Le cadre juridique actuel de la coopération est loin d'atteindre cet objectif.

3.3.2 Le cadre légal de la cyber-sécurité est en évolution constante,

Empruntant le rythme de l'informatisation. Plusieurs textes ont paru pour réguler des nouveaux aspects de la cyber-sécurité. En plus, cette thématique est devenue un centre d'intérêt dans la plupart des textes juridiques sectoriels.

La réglementation des échanges avec l'administration publique, des archives et des postes et des communications intègre de plus en plus la sphère du cyber-sécurité.

Les textes relatifs aux activités financières et des banques, du transport des énergies contiennent des dispositions sur la sécurité informatique.

La normalisation des règles de sécurité informatique appliquées à des secteurs spécifiques constitue un enrichissement du cadre légal et un facteur de développement important.

3.3.3 Le droit de la cyber-sécurité est composé de plusieurs textes juridiques éparpillés.

La lisibilité de ce droit n'est plus certaine. Deux techniques ont été utilisées par les pays francophones pour surmonter cette situation :

- l'encadrement des textes par un document de politique générale qui trace les orientations du pays et sa vision globale pour le secteur en intégrant le cadre juridique en tant qu'axe de cette politique. Cette démarche facilite la compréhension des textes, mais elle n'aide pas à rechercher l'information pertinente ;
- l'unification institutionnelle des différents aspects de la cyber-sécurité ; l'exemple a été donné par le Côte d'ivoire qui a chargé l'autorité du régulation des communications des différentes prérogatives liées à la sécurité des réseaux, des données et des système d'information.

4. Recommandations :

1- Etablir un cursus de formation juridique en matière de cyber-sécurité pour les différents acteurs ;

2- Harmonisation du cadre juridique dans l'espace francophone :
   - Surmonter la polémique sur l'instrument international de lutte contre la cybercriminalité en proposant une loi modèle sur la base des bonnes pratiques internationales, avec un Guide pour son implémentation, mettant en valeur les principes de base auxquels il n'est pas recommandé de déroger ;
   - Proposer un projet de codification du droit de la cyber-sécurité qui contient essentiellement l'architecture générale de ce droit en vue d'une meilleure lisibilité du cadre juridique et afin de garantir l'harmonisation entre les textes ;

3- Créer une base de données sur des informations juridiques en matière de cyber-sécurité ;

4- Créer un mécanisme de coopération entre les pays francophones en matière d'investigation et d'enquête ;

5- Proposer une convention d'entraide judiciaire pour la zone francophone, adaptée aux besoins de la lutte contre la cybercriminalité ;

6- Encourager la coopération juridique bilatérale et multilatérale dans le cadre de groupes régionaux pour promouvoir les échanges des informations et des expériences et la formation.