Centre de recherches pour le développement international

IDRC CRDI

Exploration sur la cybercriminalité et la sécurité en Afrique : État des lieux et priorités de recherche

Synthèse des rapports nationaux

Pr Abdoullah CISSE

Juriste, Expert légiste
Coordonnateur scientifique

Janvier 2011

Table des matières

Avant-propos

I. Contexte et justification de l'étude exploratoire

Le développement contemporain des Technologies de l'Information et de la Communication (TIC) constitue un enjeu majeur pour le développement économique en Afrique. Cependant, il a été à l'origine de l'apparition du phénomène de la cybercriminalité dont les caractéristiques particulières ont entraîné l'inadaptation des systèmes répressifs de la plupart des États africains, dont les réponses traditionnelles conçues pour un environnement matérialisé et national, se sont révélées inappropriées pour saisir ce nouveau phénomène criminel, immatériel et mondial de l'ère numérique.

Face à l'actualité de la cybercriminalité qui constitue une véritable menace pour la sécurité des réseaux informatiques, la sécurité des cybercitoyens et cyberconsommateurs dont la protection reste très précaire ainsi que pour le développement de la société de l'information et de l'économie du savoir en Afrique, il est nécessaire de fixer les grandes orientations de la stratégie de prévention et de répression de la cybercriminalité en Afrique en se basant sur les résultats de la recherche scientifique. Il faudra penser à des stratégies innovantes de politique criminelle combinant les réponses étatiques, sociétales et techniques et qui tiennent compte des capacités et des ressources des Etats africains tout en s'inspirant des bonnes pratiques recensées à l'échelle internationale et des lignes directrices de l'Union Internationale des Télécommunications sur la cybersécurité pour les pays en développement.

Dès lors il devient à la fois opportun et judicieux à partir d'un état des lieux, de définir les priorités de recherche et de susciter des études approfondies qui pourront contribuer à une meilleure connaissance du phénomène et partant à stopper ou atténuer son ampleur. La cybercriminalité n'épargne aucun continent du fait de la nature du cyberespace et de l'effet conjugué de la mondialisation. Cette ampleur est accentuée en Afrique du fait de la fracture numérique : « l'hypo connexion » des régions du Sud et l'ignorance des usagers vont de pair avec l'absence d'un dispositif approprié de lutte contre la cybercriminalité et transforme les États en paradis pénal pour les cyberdélinquants qui y trouvent des proies faciles et l'utilisent comme base de travail pour porter atteinte aux réseaux internationaux.

La cybercriminalité est une maladie de la société de l'information qui préjudicie aux intérêts des consommateurs et des commerçants dans le commerce électronique. En outre, elle constitue une menace très sérieuse à la stabilité de l'ensemble du système financier international étant donné le risque systémique lié notamment aux opérations de blanchiment de l'argent électronique et au financement du terrorisme. Enfin, la cybercriminalité est une menace grave pour les libertés notamment lorsqu'elle s'attaque aux bases de données à caractère personnel ou aux catégories vulnérables (pédopornographie, proxénétisme, traite des enfants et des femmes etc.)

Le CRDI a financé une recherche exploratoire sur “la cybercriminalité et la sécurité en Afrique” pour établir un état des lieux qui puisse fonder une définition scientifique des priorités de recherche pour l’Afrique.
Huit pays représentatifs des cinq régions d’Afrique ont été étudiés et les études nationales font l’objet de la présente synthèse. L’examen et la validation des rapports se feront dans le cadre d’un Atelier de restitution.

II. Objectifs

Ayant à l'esprit que le traitement de la cybercriminalité participe à la sécurisation du cyberespace par la protection qu’il assure aux ordinateurs, aux systèmes d’information, aux enfants et aux transactions commerciales et financières numériques sans compter la protection des données à caractère personnel, l'exploration a permis d’une part, de dresser l’état des lieux du phénomène et d'analyser les questions juridiques et réglementaires qui entravent l’existence, l’effectivité et l’efficacité d’un traitement approprié de la cybercriminalité et fournir les bases d’une harmonisation de la politique cybercriminelle en Afrique et, d’autre part, d’identifier les priorités d’une recherche panafricaine sur le thème de la cybercriminalité et de la sécurité en Afrique.

La présente étude sur la cybercriminalité avait pour objectif d’explorer :

- en politique criminelle, les différentes facettes du traitement différentiel des cybercrimes en examinant le degré de complémentarité entre les réponses pénales étatiques (judiciaires et administratives, les réponses sociétales (éducation, sensibilisation, prévention spéciale) et les réponses techniques (sécurisation des systèmes d’information et des ordinateurs, dispositifs prudentiels).
- en droit pénal substantiel, l’effort de modernisation des instruments de répression de la cybercriminalité, en étudiant les expériences des Etats africains tendant à l’adoption d’incriminations nouvelles spécifiques aux TIC, l’adaptation de certaines incriminations, des sanctions et du régime de responsabilité pénale en vigueur dans les États africains à l’environnement numérique.
- en droit pénal procédural, l’effort d’adaptation de la procédure classique aux TIC et l’introduction de procédures spécifiques à la cybercriminalité.

Les études nationales réalisées sur l’Afrique du Sud, l’Egypte, le Cameroun, le Ghana, le Kenya, le Nigéria, le Maroc et le Sénégal ont permis de :

(1) Dresser un état des lieux de la cybercriminalité dans les différentes régions d’Afrique

- en faisant un inventaire des cas les plus répandus de cybercriminalité qui s'opèrent par la violation de normes techniques (atteintes aux réseaux, aux bases de données, aux ordinateurs etc.) ou de normes sociales (pédopornographie, blanchiment de capitaux etc.) ;
- en présentant les réponses de politique criminelle consacrées qu'elles soient étatiques (lois et institutions) ou sociétales (codes éthiques et de déontologie, chartes, autoprotection des usagers etc.)
- en identifiant les infractions nouvelles assorties de sanctions à intégrer dans les législations pénales
- en identifiant les adaptations à introduire dans le droit pénal et la procédure pénale
- en proposant des principes directeurs de politique criminelle pour un traitement harmonisé de la cybercriminalité en Afrique.
- en identifiant les adaptations à introduire dans le droit pénal et la procédure pénale
- en proposant des principes directeurs de politique criminelle pour un traitement harmonisé de la cybercriminalité en Afrique
- en procédant à une analyse stratégique des traites internationaux existants sur la cybercriminalité pour en mesurer le niveau pertinence et la capacité à répondre au phénomène en Afrique.

(2) Identifier et analyser, sur la base d'une grille d'analyse commune, les questions juridiques et réglementaires, les obstacles, les inefficacités et les lacunes qui compromettent l'existence, l'effectivité et l'efficacité du traitement de la cybercriminalité en Afrique, et élaborer des recommandations pour les surmonter.

(3) Identifier les voies de l'harmonisation et de la coopération policière et judiciaire en vue de l'efficacité du traitement de la cybercriminalité.

(4) Identifier les besoins et priorités en matière de recherches sur le continent et les institutions idoines pour entreprendre ces recherches.

La présente synthèse rend compte des traits saillants des études nationales sur les questions suivantes :

- La compréhension du phénomène cybercriminel et son ampleur dans le pays étudié
- L'identification des réponses à la cybercriminalité dans le pays considéré ;
- L'identification des priorités de recherches sur la cybercriminalité et la sécurité en Afrique.

III. Méthodologie

Les études nationales ont été réalisées sur la base d'un guide méthodologique commun (voir annexe) à tous les chercheurs et qui respecte les normes scientifiques de l'exploration et de la comparaison.

Pour avoir un aperçu le plus exhaustif du phénomène en Afrique, les études ont couvert un certain nombre de pays représentatifs à la fois de la diversité régionale africaine (Centre, Est, Nord, Ouest, Sud) et des situations nationales. Les pays suivants ont été ciblés :

- Centre : Cameroun

- Est : Kenya

- Nord : Égypte et Maroc

- Ouest : Sénégal et Nigéria

- Sud : Afrique du Sud

Pour faciliter l'analyse comparative entre les différents systèmes étudiés, une grille d'analyse commune a servi de feuille de route à l'équipe de recherche. Elle a permis sur la base de la méthodologie des sciences juridiques et sociales, de soulever des questions d'intérêt commun qui sont abordées dans le rapport. Elle a été élaborée et proposée par le Coordonateur aux membres de l'équipe avant le lancement de la recherche. La méthodologie était articulée autour du choix et de l'organisation des lectures, d'une grille de lecture et des entretiens exploratoires.

Pour les recommandations relatives aux pistes de recherche et à l'harmonisation, les chercheurs ont été invités à faire preuve de créativité et d'esprit d'innovation.

L'équipe a procédé à une revue documentaire et à une revue juridique.

- ☞ **Revue documentaire**
    - Revue de la littérature sur les cas de cybercriminalité les plus saillants dans sa zone d'étude ;
    - Revue de la littérature sur les différentes approches juridiques, réglementaires et institutionnelles ;
    - Revue de la littérature sur les normes internationales et régionales ;
    - Identification des meilleures pratiques à partager ;
    - Identification des lacunes du cadre juridique qui empêchent le traitement efficace de la cybercriminalité ;
    - Identification des structures de recherches et de formation (laboratoires, centres, réseaux etc.) qui travaillent ou ont vocation à travailler sur la cybercriminalité.
    - Revue de cas pratiques connus de cybercriminalité en Afrique.
- ☞ **Revue du cadre juridique, institutionnel et réglementaire**

L'équipe a procédé à l'analyse du cadre juridique, institutionnel et réglementaire en tenant compte des réponses sociétales développées dans chaque zone.

Il a accordé une importance notamment aux questions suivantes :

- Les infractions consacrées ou à consacrer dans le droit pénal : les délits informatiques, les infractions de droit commun commises par le biais de l'informatique et de l'internet.
- Les règles de procédure pénale : les règles en vigueur et le niveau d'adaptation ;
- L'implication de administrations (police, justice, pénitentiaire) dans le traitement de la cybercriminalité
- La disponibilité des moyens matériels et logistiques des autorités chargées de la prévention et de la répression de la cybercriminalité
- Le niveau de conscience des populations face à la cybercriminalité
- La formation des professionnels de la justice au traitement de la cybercriminalité.

- ☞ **Entretiens**

La revue documentaire et celle du cadre législatif, réglementaire et institutionnel ont été complétées par des entretiens avec :

- des acteurs nationaux ou régionaux impliqués dans le traitement de la cybercriminalité à différents niveaux politique, législatif, judiciaire et policier.
- des acteurs du secteur économique et financier impliqués dans la prévention ou susceptibles d'être victimes de la cybercriminalité : banques centrales, banques commerciales, entreprises de transfert d'argent, établissements de monnaie électronique.

IV. Équipe

L'équipe des chercheurs et experts a été coordonnée par le Professeur Abdoullah Cissé, juriste et légiste, expert en cyberdroit qui a à son actif :

- L'élaboration de la législation sénégalaise et de la CEDEAO sur la lutte contre la cybercriminalité;
- La création d'un master en droit africain du cyberespace en formation ouverte et à distance à l'Université Gaston Berger de Saint-Louis
- La coordination de l'étude en vue l'élaboration de la convention de l'Union africaine sur la la cybersécurité et les transaction numérique en Afrique.

Il a été assisté dans la tâche de coordination par Mme Roughiatou THIAM, juriste spécialisée en cyberdroit et propriété intellectuelle et M. Boubacar Diallo, docteur en droit, enseignant à l'Université de Saint-louis a participé à la réalisation de la note de synthèse.

Les études nationales ont été conduites par les experts suivants :

PAYS	CHERCHEURS
Afrique du Sud	Sven Abraham
Cameroun	Paul-Gérard POUGOUE, Agrégé des Facultés de Droit, Professeur Titulaire Vice-Recteur à l'Université de Yaoundé II et Pr Jean-Marie TCHAKOUA, professeur agrégé de droit
Égypte	Dr. Bassem AWAD Chief Judge, Egyptian Ministry of Justice Lecturer at the Egyptian Universities Ph.D. in Intellectual Property, University of Montpellier, France LL.M in International Business Law, University of Paris I (Panthéon-Sorbonne)
Ghana	Kwame GYAN
Kenya	Dr Ben Sihanya Governance Programme, Innovative Lawyering and Sihanya Mentoring

Maroc	ALI EL AZZOUZI | Expert Consultant Sécurité | PCI QSA - CISA - Lead Auditor ISO 27001 - ITIL Casablanca | Maroc
Nigéria	Basil Udotai, Esq., Managing Partner, Technology Advisors ICT LAWYERS & CONSULTANTS Abuja, NIGERIA
Sénégal	Pr Abdoullah CISSE, expert en cyberdroit, professeur aux universités de Saint-Louis et de Dakar (Sénégal)

V. Atelier de restitution

Au terme de l'étude et du dépôt de l'ensemble des rapports, un Atelier de restitution a été organisé à Dakar, les 29 et 30 novembre 2010. Il visait essentiellement à :

- examiner, amender et valider les différents documents qui ont été produits ;
- échanger et partager sur les résultats de l'étude exploratoire sur la cybercriminalité et la sécurité en Afrique ;
- définir les perspectives ouvertes par cette étude exploratoire en termes de recherches et d'actions autour des questions de la cybercriminalité et la sécurité en Afrique ;
- examiner l'opportunité de la mise en place d'un réseau africain sur le cybercriminalité.

L'atelier a réuni une cinquantaine de participants représentatifs de la plus grande diversité des acteurs impliqués sur la question de la cybercriminalité et la sécurité en Afrique. On a pu ainsi noter :

- une diversité géographique à travers les régions (Est, ouest, nord, sud et Centre) de l'Afrique représentées par les (nombre) nationalités réunies ;
- une diversité linguistique et de cultures juridiques à travers la présence de francophones comme d'anglophones, de juristes issus de pays de tradition civiliste comme de *common law* comme des juristes de tradition musulmane ;
- une diversité des profils et des compétences marquée par la présence d'experts dans les domaines juridiques et techniques liés à la cybercriminalité, mais également, de personnalités issues des secteurs de l'enseignement et de la recherche (universitaires et structures d'appui à la recherche, lycées) et de la justice (magistrats, avocats), des services de sécurité, des technologies, de la régulation du secteur des télécoms et des TIC, du secteur privé, des organisations régionales et continentales dans les domaines financiers et de lutte contre le blanchiment, des organisations de la société civile…

  En prélude au démarrage des travaux, le Coordonnateur de l'étude exploratoire a présenté un exposé sur « l'Afrique et les défis de la cybercriminalité et de la sécurité ».

Abordant d'abord les enjeux et défis, il a mis l'accent sur la progression du risque numérique et sur la cybercriminalité comme un phénomène lié à la civilisation numérique. Nos façons de vivre, nos modes de production et notre sécurité sont en effet de plus en plus dépendants des systèmes informatiques. A cela s'ajoute du fait du développement des réseaux sociaux, un décloisonnement des sphères privées et professionnelles. Toutefois l'insuffisance de l'encadrement de la cybercriminalité transforme l'Afrique en paradis cybercriminel où la facilité de réalisation des infractions donne une idée de l'importance des victimes des cybercriminels. L'impact négatif de la cybercriminalité est perceptible au plan juridique, financier et sur l'image des personnes et des organisations.

Ensuite, l'accent a été mis sur l'analyse du risque numérique dans ses multiples manifestations. Une typologie a été esquissée qui a permis de faire le départ entre les risques liés à la sécurité des systèmes d'information, les risques liés aux données et notamment aux services bancaires et financiers et les risques liés aux personnes notamment les salariés et les internautes.

Enfin, le processus d'harmonisation des cyberlégislations en cours sur le continent a été présenté. La démarche retenue est conforme aux préceptes de la légistique (science de la création normative), les principaux domaines couverts sont la cybercriminalité et cybersécurité, les transactions électroniques, la protection des données à caractère personnel. Si aujourd'hui certains Etats de sont dotés de cyberlégislations, l'harmonisation est encours dans les Communautés Economiques Régionales (CEDEAO, CEAC) et l'Union africaine s'est fixée 2012 comme échéance pour l'adoption de la Convention africaine sur la cybersécurité et les transactions numériques.

Les préconisations formulées lors de cette conférence inaugurale tournaient autour de deux axes majeurs : d'une part l'impératif de maitrise du risque numérique et d'autre part l'impératif de maitrise du cadre juridique et institutionnel.

A la suite de cet exposé inaugural, les études nationales ont été présentées et ont fait l'objet de discussions nourries entre les participants.

Les principaux résultats de l'Atelier ont été intégrés dans les conclusions et recommandations de la présente synthèse.

1. Introduction

La synthèse des travaux menés dans le cadre des différentes études nationales a permis de constater une très grande diversité dans les manifestations du phénomène cybercriminel auquel répondent des normes juridiques et non juridiques au triple niveau national, communautaire et international déjà en vigueur ou en projet. L'analyse du phénomène et des réponses a donné lieu à de riches conclusions et recommandations qui ont été reprises dans le présent rapport. Il a été rédigé suivant la méthodologie harmonisée retenue pour les études nationales à laquelle s'est greffée une dimension comparative nécessaire, s'agissant d'une synthèse d'études nationales dont les idées essentielles sont ici présentées.

1.1. Méthodologie de la synthèse

1.1.1. Structure du rapport

La synthèse des études nationales emprunte la structuration préconisée dans le guide méthodologique. La plupart des études nationales a été menée suivant les indications contenues dans le guide méthodologique. Toutefois, le travail a été rendu difficile par le fait que certaines études nationales n'ont pas respecté les contraintes méthodologiques. L'atelier de restitution peut fournir l'occasion de compléter certaines parties des études nationales et du rapport de synthèse.

1.1.2. Dimension comparative

S'agissant d'une synthèse d'études nationales, elle repose très largement sur une démarche comparative. Ainsi, sur chaque question étudiée, la synthèse met l'accent, d'une part, sur les convergences et d'autre part, le cas échéant, sur les particularités nationales. Ces particularités peuvent s'exprimer soit en termes de divergences de position, soit en termes de silence, c'est-à-dire, d'absence, volontaire ou non, de position nationale sur une question déterminée.

1.1.3. Tableau de synthèse

La synthèse fait l'objet d'une présentation dans un tableau reprenant les différentes questions abordées par les études nationales. La présentation est faite sur trois colonnes principales portant sur la question étudiée, les convergences relevées et les particularités nationales. Ces dernières font l'objet de trois colonnes représentant l'Etat concerné, les divergences notées ainsi que les silences observés.

1.2. Contexte

a. Convergences

Avec l'essor des technologies de l'information et de la communication (TIC), on assiste à l'avènement de nouvelles infractions qui se réalisent ou qui sont favorisées par les TIC ou bien qui prennent les TIC comme cibles. Ainsi, la cybercriminalité constitue un pendant du développement des TIC et de la généralisation de leur utilisation dans tous les secteurs de la vie économique, sociale, culturelle et politique des Etats. Qu'elle soit nommée criminalité informatique, cybercrime, délinquance informatique, criminalité des hautes technologies, la cybercriminalité a pour particularité d'introduire une certaine ubiquité dans la criminalité et menace tout à la fois les individus, les

entreprises et les États. Sa conception partagée l'associe à « *tout comportement interdit par la législation et/ou par la jurisprudence qui: a) est dirigé contre les technologies de calcul électronique et de communication elles-mêmes; b) fait intervenir l'utilisation de technologies numériques pour la commission de l'infraction; et c) suppose l'utilisation incidente d'ordinateurs pour la commission d'autres infractions* ».[1]

Ainsi conçue, la cybercriminalité emporte des conséquences socio-économiques incalculables, pouvant aller des mouvements sociaux à la perturbation du système financier international en passant par le blocage, le détournement ou la paralysie des systèmes d'information ou des réseaux informatiques des banques, des trésors, de services postaux ou des opérateurs de téléphonie sans compter les dommages causés aux personnes, notamment celles qui reçoivent quotidiennement des offres par courriel (spamming), un phénomène très répandu et qui continue de causer d'énormes pertes à ces personnes.

C'est ce qui explique l'intérêt, pour l'ensemble des Etats, à mettre en place un cadre adéquat de lutte contre les phénomènes cybercriminels.

b. Particularités nationales

- Divergences

Afrique du Sud : Le nombre d'usagers d'Internet en Afrique du Sud était de 4, 5 millions en 2008. Le taux de pénétration d'Internet y est de 15%, plaçant le pays au 110^{e} rang mondial. Avec le développement de la capacité de la bande passante, le nombre d'usagers peut passer à 6 millions en fin 2010.

Egypte : Le nombre d'usagers d'Internet est passé de 0,65 million en 2000 à 19, 7 millions en fin 2010. Le taux d'utilisation d'Internet est de 20% pour les ménages, 59,6%pour les entreprises et 35% pour les entités publiques.

Maroc : Le Marché de l'Internet a enregistré une forte évolution au cours de l'année 2009, avec une croissance du parc d'abonnés de 56,7% (1.186.923 abonnés à fin 2009, contre 757.453 à fin 2008), avec un taux de pénétration de 3,81% à fin 2009 (contre 2,46% une année auparavant). Par ailleurs, il est à noter que 53 % des entreprises publiques et 87 % des entreprises privées ont accès à l'Internet[2].

[1] Cette définition est donnée par le Onzième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants : Bangkok, 18-25 avril 2005.

[2] Sur la réglementation en vigueur au Maroc, il est à noter certains textes spécifiques aux TIC.

- Cybercriminalité : Loi n° 07-03 du 11 novembre 2003 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données. Les articles 607-3 à 607-11 ont été ajoutés au Code Pénal promulgué par le Dahir n° 1-59-413 du 26 novembre 1962 ;
- Cryptographie : Loi n° 53-05 du 30 novembre 2007 relative à l'échange électronique de données juridiques ;
- Données personnelles : Loi n° 09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Nigéria : Au Nigeria, l'émergence des phénomènes cybercriminels est située dans les années 90 avec l'introduction des services Internet dans les grandes villes nigérianes, particulièrement à Lagos. L'extension et la sophistication des phénomènes cybercriminels dans ce pays lui vaut d'occuper une troisième place peu enviable dans le classement 2007 de la cybercriminalité dans les Etats après le Royaume-Uni et les Etats-Unis[3].

L'on note, généralement, une certaine disparité entre l'ampleur que prend le phénomène et la faiblesse des réponses en termes de capacités juridiques et techniques d'appréhension, de prévention, de poursuite et de répression de la cybercriminalité. Toutefois, un écart particulièrement important est relevé dans certaines études nationales (Nigeria, Cameroun) en raison du niveau élevé de cybercriminalité.

- Silences

Il convient de signaler l'absence d'informations, dans les diverses études nationales (à l'exception du Nigeria), sur la période d'émergence de la cybercriminalité ou sur l'importance du phénomène.

1.3. Question de départ

a. Convergences

L'ensemble des études nationales (ayant mentionné une question de départ[4]) s'interrogent sur la capacité du cadre juridique actuel à répondre, de manière adéquate, au phénomène de la cybercriminalité. De manière implicite, cette question induit également une réflexion sur l'opportunité d'une amélioration du cadre existant ou de la mise en place d'un nouveau cadre de lutte contre la cybercriminalité.

b. Particularités nationales

Certaines particularités peuvent être relevées dans les différentes études nationales.

- Divergences

Certaines études nationales ont posé leur question de départ dans une formulation qui semble viser exclusivement le cadre juridique de lutte contre la cybercriminalité : Afrique du Sud[5], Nigéria[6], Maroc[7].

---

[3] http://allafrica.com/stories/200809060060.html

[4] Afrique du Sud, Cameroun, Egypte, Ghana, Nigéria.

[5] "Do we need a new framework of protection for cyber crime in South Africa or is this simply crime that already is codified in our jurisprudence?
Does the ECT act provide adequate protections for crime as it happens in cyberspace ?"

D'autres études ont formulé la question de manière assez large pour prendre en charge les dimensions juridique, institutionnel et technique de la lutte contre la cybercriminalité : Cameroun[8], Egypte[9], Ghana[10] et Sénégal[11].

2. Typologie des cas de cybercriminalité

La synthèse de la typologie des phénomènes cybercriminels a été réalisée suivant la grille méthodologique proposée, même si toutes les études nationales ne l'ont pas respectée. Ainsi, ont été successivement présentées les situations dans lesquelles les technologies sont objets, moyens et simples supports de phénomènes relevant de la cybercriminalité.

2.1. Les technologies, objets de la cybercriminalité

Dans le cadre des technologies, objets de la cybercriminalité, sont envisagées les situations dans lesquelles un phénomène cybercriminel vise les technologies de l'information et de la communication comme cible. Il peut s'agir d'atteintes aux systèmes informatiques, aux systèmes automatisés des données ou aux systèmes de cryptologie.

2.1.1. Les atteintes aux systèmes informatiques

a. Convergences

L'existence d'atteintes aux systèmes informatiques a été relevée dans l'ensemble des études nationales. Toutefois, toutes les études n'utilisent pas les mêmes termes pour distinguer entre les différentes atteintes aux systèmes. Trois grandes catégories d'atteintes aux systèmes informatiques peuvent malgré tout être distinguées : les atteintes à la confidentialité, les atteintes à l'intégrité et les atteintes à la disponibilité des systèmes informatiques.

La première catégorie ***d'atteintes à la confidentialité*** vise à la fois l'accès frauduleux[12] à un système informatique et le maintien frauduleux dans un système informatique. L'accès frauduleux[13] renvoie

---

[6] "to what extent has the Nigerian legal, political and social systems responded to the scourge of cybercrime that accompanied the large scale introduction of information and communications technology (ICT) in the country?"

[7] "La réglementation en vigueur vise uniquement le cadre juridique de lutte contre la cybercriminalité et n'intègre pas les dimensions institutionnelles et techniques".

[8] Quelles sont les armes dont dispose le Cameroun face à la cybercriminalité ? Vers quelles pistes de recherche orienter les efforts de lutte contre le phénomène ?

[9] This study contributes to an understanding of the cybercrime environment in Egypt, particularly for how far the present legislation in Egypt deal with these new criminal offences, and in what way is the legal structure lagging to curb the crime. It is not an exhaustive legal analysis of the current legislation; it emphasizes and highlights also technological and organizational possible procedures to combat cybercrime.

[10] "Is the existing legal, regulatory and institutional framework in Ghana sufficiently robust for handling the phenomenon of cybercriminality in the country?"

[11] Quelles sont les réponses et strategies de lutte contre la cybercriminalité ?

[12] Au Sénégal, des exemples d'accès frauduleux ont été relevés et une jurisprudence a été citée. Tribunal Régional Hors Classe de Dakar, n° 4241/ 09 du 18 septembre 2009. Le juge des flagrants délits a considéré que constitue un accès frauduleux, au sens de l'article 431-8 du code pénal, le fait pour un collaborateur d'une société spécialisée dans la vente et la distribution de pneumatiques et de chambres à air d'accéder aux

aux cas de piratage informatique, intrusion (phénomène connu sous le nom de « hacking ») ou interception. Sont pris en compte, pour sa répréhension, non seulement tous actes visant à s'introduire ou permettre l'introduction sans droit ni titre, dans un système informatique donné, mais également, le fait, en le faisant, de se procurer quelque avantage ou de causer quelque dommage. Quant au maintien frauduleux dans un système informatique, il vise le fait de se maintenir ou tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique. Ainsi, lorsqu'un individu non habilité, ayant accédé par hasard ou par erreur à un système, ou bénéficiant d'une autorisation de connexion limitée dans le temps, reste dans le système au lieu d'interrompre la connexion, on considère qu'il y a maintien frauduleux dans un système informatique.

La deuxième catégorie, les ***atteintes à l'intégrité*** des systèmes informatiques, est aussi désignée comme une altération des systèmes. Elle consiste dans l'action ou la tentative soit de fausser le fonctionnement du système, soit d'en entraver le fonctionnement. C'est ce qui est visé à travers les phénomènes de perturbation ou d'interruption du fonctionnement d'un système ou d'un réseau. Fausser ou perturber le fonctionnement d'un système, c'est lui faire produire un résultat qui n'en était pas attendu. C'est en cela que cette atteinte se différencie de l'entrave au fonctionnement ou l'interruption du fonctionnement du système ayant pour résultat d'empêcher l'aboutissement du traitement informatique. Les virus et pourriels (« spam » en anglais) sont cités comme des atteintes à l'intégrité des systèmes.

La troisième catégorie, les ***atteintes à la disponibilité*** des systèmes informatiques se rapporte au fait d'introduire ou de tenter d'introduire des données dans un système informatique de manière frauduleuse, c'est-à-dire, lorsque des caractères magnétiques nouveaux sont incorporés dans un système, sans que l'on y soit autorisé. Ainsi, à la différence du simple cas d'accès frauduleux à un système informatique, il est noté une introduction ou une tentative d'introduction de données dans le système. Toutefois, la proximité avec le délit d'accès frauduleux est telle qu'un chevauchement est possible.

b. Particularités nationales

Afrique du Sud : La Section 86 (1 à 5) du ECT Act incrimine les atteintes aux systèmes d'information en qualifiant d'infraction l'accès non autorisé à un système, l'altération de données dans un système automatisé. La Section 2 de la Regulation of interception of communications and provision of communication – related information (RIPCI) act, act 70 of 2002, interdit l'interférence non autorisée avec des données.

---

données de l'ordinateur du directeur commercial de la dite société avant de se faire envoyer dans sa propre boîte électronique des informations commerciales concernant des contrats d'achat de pneus avec un partenaire étranger.

[13] Accès illégal suivant certaines études comme celle du Maroc.

Ghana : L'étude nationale ghanéenne ne retient pas cette classification et les infractions visées à travers les atteintes aux systèmes sont présentées de manière laconique comme des atteintes aux personnes ou aux organisations[14].

Maroc : Il est à noter l'incrimination spécifique de certains actes : accès illégal (Article 607-3 du Code Pénal) ; atteinte à l'intégrité des données (Article 607-4 du Code Pénal) ; sabotage informatique (Article 607-5 du Code Pénal).

Nigéria : L'étude nigériane rapporte un très grand nombre d'atteintes à la confidentialité ou à la disponibilité des systèmes du fait du hacking qui a même frappé des sites officiels gouvernementaux. Toutefois, en ce qui concerne ces derniers sites, les dommages sont limités du fait que les sites attaqués comportent très peu de contenus dynamiques présentant un intérêt pour des cybercriminels.

Egypte : Le rapport national égyptien ne consacre pas de titre aux atteintes aux systèmes informatiques. Ainsi, au titre des technologies, objet de la cybercriminalité, l'étude évoque exclusivement les atteintes aux systèmes de cryptologie. Toutefois, en traitant du Hacking, l'étude révèle que l'intrusion dans un système sans autorisation n'est pas considérée, en elle-même, comme une infraction. Pour être incriminée et sanctionnée, l'accès non autorisée doit être sous-tendue par l'intention ou le dessein de détériorer ou détruire (article 361 du Code pénal, v. Etude Egypte, p. 8).

2.1.2. Les atteintes aux systèmes automatisés des données

Est considérée comme une donnée informatisée « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique* ».

a. Convergences

Toutes atteintes aux données informatisées constituent des phénomènes cybercriminels, qu'elles consistent dans la destruction, l'endommagement, l'effacement, la détérioration, l'altération ou la modification frauduleuse. Différents phénomènes cybercriminels spécifiques sont retenus à ce titre, dans les différentes études, comme des atteintes aux systèmes automatisés des données :

- L'interception et la tentative d'interception frauduleuse par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique ;

- Le faux informatique entendu comme la production d'un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales ;

- L'usage de faux informatique qui consiste dans l'utilisation intentionnelle de données issues d'un faux informatique ;

[14] V. Etude Ghana : 3.1.1 et 3.1.3.

- La fraude informatique qui renvoie à l'obtention frauduleuse, pour soi-même ou pour autrui, d'un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique.

b. Particularités nationales

Dans l'ensemble des études nationales, de telles atteintes sont présentées comme des phénomènes cybercriminels, mais ne sont pas toujours analysées comme des atteintes aux systèmes automatisés des données.

2.1.3. Les atteintes au système de cryptologie

Convergences :
Dans les études nationales, sont considérées comme des atteintes au système de cryptologie toutes activités permettant d'accéder frauduleusement à tout ou partie d'un système informatique protégé. De telles activités:

- tendent à enfreindre l'organisation imposée aux fournisseurs de services de cryptologie
- peuvent prendre diverses formes, notamment, l'usage, la production, la vente, l'importation, la détention, la diffusion, l'offre, la cession ou la mise à disposition
    - soit des équipements, programme informatique, dispositif ou donnée conçus ou spécialement adaptés à cet effet,
    - soit des mot de passe, code d'accès ou données informatisées similaires obtenus frauduleusement ;
- visent à permettre l'accès non autorisé à un système informatique en divulguant indûment une convention de chiffrement ou à refuser de remettre aux autorités habilités ou de mettre en œuvre sur leur demande des conventions de chiffrement susceptible d'avoir été utilisées pour préparer, faciliter ou commettre une infraction.

Particularités nationales

Afrique du Sud : Les fournisseurs de services de cryptologie doivent être enregistrés et leur activité est encadrée de manière stricte par la section 29 du ECT Act 25 de 2002. La section 21 de la RICPCI, Act 70 of 2002, permet, sur la base d'une injonction, de contraindre les prestataires de services de cryptographie, à mettre à disposition une clé de décryptage d'une communication électronique.

Cameroun : L'étude nationale sur le Cameroun présente, au titre des atteintes au système de cryptologie, l'article 88 de la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité qui punit « celui qui, ayant connaissance de la convention sécrète de déchiffrement, d'un moyen de cryptographie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, refuse de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités ».

Egypte : Selon l'étude nationale sur l'Egypte, une loi n° 15/2004 a été consacrée à la signature électronique et sanctionne l'altération ou la falsification de signatures électroniques ou encore l'usage de signatures falsifiées ou altérées.

Maroc : La cryptologie fait l'objet de réglementation au Maroc à travers la Loi n° 53-05 du 30 novembre 2007 relative à l'échange électronique de données juridiques.

2.2. Les technologies, moyens de la cybercriminalité

Certains phénomènes sont qualifiés de cybercriminels parce qu'ils sont commis au moyen des technologies de l'information et de la communication. A ce titre, il est possible de distinguer, selon les intérêts atteints par ces phénomènes, entre les atteintes aux intérêts des Etats, les atteintes aux personnes, les atteintes aux biens et les atteintes à la propriété intellectuelle.

2.2.1. Le cyberterrorisme et les atteintes aux intérêts des Etats

a. Convergences

Les phénomènes cybercriminels commis au moyen des technologies donnent une portée nouvelle au terrorisme et, plus généralement aux différentes atteintes aux intérêts des Etats dont quelques rares expériences ont été relevées dans les études nationales et concernent toutes les régions de l'Afrique étudiées, mais à des degrés divers. En ce qui concerne le cyber terrorisme, il convient de remarquer que s'il n'est pas totalement inconnu dans les Etats étudiés, il ne vise pas ces Etats. C'est pourquoi il n'a pas été rapporté, dans les études, de cas de cyber terrorisme visant ces Etats.

Certaines explications ont été avancées, notamment la faible pénétration d'Internet (Ex : au Nigeria, 7, 4% de la population seulement serait connectée à Internet, soit 11 millions de personnes sur un total de 150 millions), l'introduction très lente des pratiques de e-gouvernance ou la nature des sites gouvernementaux qui sont davantage statiques et informationnels que dynamiques et transactionnels.

1) En tant que phénomène cybercriminel, le cyber terrorisme n'a pas été défini[15], mais certains cas qui peuvent s'y rapporter ont été recensés dans l'étude nationale marocaine. Ainsi, est signalée l'existence d'un groupe de jeunes pirates marocains dénommé « *Team Evil* » qui,

[15] Toutefois, des définitions ont été citées dans certaines études nationales (ex. Afrique du Sud), sans que cela n'induise l'existence du phénomène dans les Etats concernés. Ainsi, Denning D. ("Cyberterrorism. " Testimony before the special oversight panel of terrorism Committee on Armed service , US house of representatives, 23 May 2000 (http://www.cs.georgetown.edu/~denning/infosec/cyberteerroe.html, last accessed on 15 November 2009)), propose la definition suivante: "Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructure could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not". De meme, a été rappelée, dans l'étude sud africaine, la definition du FBI (FBI,2002, Code of Federal Regulations, 28CFR, Section 0.85 on Judicial administration, July 2001) selon laquelle le terrorisme serait : "the unlawful use of force or violence, committed against persons or property, to intimidate or coerce a government, the civilian population or any segment thereof, in furtherance of political or social objectives".

depuis 2004, attaque régulièrement des sites gouvernementaux et privés israéliens et américains en les revendiquant comme des actes de solidarité envers les palestiniens et en posant, comme condition d'arrêt de leurs activités, la cessation des attaques israéliennes contre la Palestine.

2) Les autres actes cybercriminels portant atteinte aux intérêts des Etats sont des phénomènes connus mais qui sont maintenant réalisés au moyen des TIC. Il en est ainsi de :

   i. La trahison pour livraison à une puissance étrangère ou à ses agents, sous quelque forme ou par quelque moyen que se soit, un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ;

   ii. Acte d'espionnage destiné à s'assurer, par quelque moyen que se soit, la possession d'un tel renseignement, objet, document, procédé, donnée informatisé ou fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;

   iii. La destruction, complicité de destruction de tel renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé en vue de favoriser une puissance étrangère.

3) Portent également atteinte aux intérêts des Etats d'autres formes de délinquance liée à l'information et la communication telles que :

   i. La participation illégale à la réunion de données qui désigne l'action de rassembler, dans l'intention de les livrer à tout pays ou tiers, des renseignements, objets, documents, procédés, données ou fichiers informatisés dont la réunion et l'exploitation sont de nature à nuire à la défense nationale

   ii. La détention en raison de sa fonction ou sa qualité d'un renseignement, d'objet, de document, de procédé, de donnée numérisée ou de fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ou dont la connaissance pourrait conduire à la découverte d'un secret de défense nationale. Il en est de même, sans intention de trahison ou d'espionnage, de leur destruction, soustraction, reproduction, ou divulgation à une personne non qualifiée ou au public.

b. Particularités nationales

   Divergences

Egypte : L'étude égyptienne révèle que le code pénal égyptien (article 86 a.) sanctionne les actes de terrorisme de la peine de mort ou des travaux forcés à perpétuité. Toutefois, il n'existe pas de dispositions particulièrement consacrées aux actes de cyber terrorisme, comme le fait, par exemple, de proposer des modes d'emploi pour la fabrication d'explosifs sur Internet. Aussi, pour traiter de ces questions, les juges tentent-ils d'étendre les dispositions existant.

Maroc : Le cyber terrorisme n'est pas spécifiquement couvert comme l'est le terrorisme de manière générale dans la loi n° 03-03 relative à la lutte contre le terrorisme du 28 mai 2003.

L'atteinte à un système de traitement automatisé de données supposé contenir des informations relatives à la sûreté intérieure ou extérieure de l'État ou des secrets concernant l'économie nationale (Article 607-4 du Code Pénal) est sanctionnée par des peines d'emprisonnement et des amendes.

Silences

Ghana : L'étude ghanéenne cite, sans autre précision, le cyber terrorisme au titre des atteintes à la société (« attack on society »).

Cameroun : Dans l'étude nationale camerounaise, le terrorisme et les atteintes aux intérêts de l'Etat ne sont pas abordés.

Maroc : L'espionnage, la trahison, la destruction de documents et de données ne sont pas traités en droit marocain.

2.2.2. Les atteintes aux personnes

2.2.2.1. Les atteintes aux libertés individuelles et à la vie privée

a. Convergences

L'Internet et, de manière plus générale, les TIC, ont multiplié les occasions d'atteintes à différentes libertés individuelles et d'intrusion dans la vie privée des personnes. Aussi, dans le cadre de la lutte contre la cybercriminalité, une attention soutenue est-elle accordée à la protection contre différentes sortes d'atteintes aux libertés et à la vie privée. Elles sont multiples et multiforme. Elles peuvent porter atteinte à l'identité de la personne (ex. usurpation d'identité), à son image, sa voix, au secret de sa correspondance… Ainsi, de nombreux cas de cybercriminalité basés sur le vol d'identité ou, plus généralement, de données d'identification personnelle ont été rapportés dans les diverses études nationales. Le développement des réseaux sociaux constitue un amplificateur de tels phénomènes.

b. Particularités nationales

Afrique du Sud : D'importants développements ont été consacrées à la protection de la vie privée et particulièrement, des informations et données personnelles en Afrique du Sud. Les sections 50 – 51 du ECT act, 25 of 2002, traite de la protection des informations personnelles obtenues par des moyens électroniques. Si une information personnelle est stockée dans une base de données considérée comme sensible, les sections 52 – 58 de l'ECT act accorde une protection plus importante aux individus.

Cameroun : L'article 300 du Code pénal réprime la violation de la correspondance, définie comme le fait, sans l'autorisation du destinataire, de supprimer ou ouvrir la correspondance d'autrui. S'attachant spécifiquement aux télécommunications, l'article 53 de la loi du 14 juillet 1998 régissant les télécommunications au Cameroun punit : « (1) Toute personne admise à participer à l'exécution d'un service de télécommunication qui viole le secret d'une correspondance, ou qui, sans l'autorisation de l'expéditeur ou du destinataire, divulgue, publie ou utilise le contenu de ladite correspondance (…)[16] ; (2) Toute personne qui, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement ou involontairement une communication privée et qui la divulgue (…)».

Nigéria : L'étude sur le Nigeria relève une recrudescence de la cyberdélinquance basée sur le vol d'identité, notamment par le biais de réseaux sociaux comme facebook, pour commettre toutes sortes de crimes. Elle rapporte également la duplication du numéro de téléphone d'un Gouverneur de l'un des Etats du Nigéria (Delta State) dont certains contacts ont été appelés pour demander le versement de sommes d'argent très importantes sur un compte déterminé.

Silences

Maroc : L'usurpation d'identité numérique n'est pas traitéé par la loi marocaine.

2.2.2.2. Les atteintes spécifiques aux droits de la personne au regard du traitement des données à caractère personnel.

Les TIC multiplient les occasions de porter atteinte aux personnes, notamment à l'occasion du traitement de données personnelles. De ce point de vue, la protection de telles données recèle nécessairement une dimension liée à la cybercriminalité. C'est pourquoi des infractions sont instituées en vue de protéger les personnes à l'occasion du traitement des données personnelles. C'est dans ce cadre que rentre la loi relative à la cybersécurité et à la cybercriminalité au Cameroun ou la loi sénégalaise sur la protection des données personnelles.
Il convient de noter qu'au regard du traitement des données à caractère personnelle, la loi sénégalaise de 2008 sur la protection des données personnelles semble être la plus exhaustive en ce qui concerne les infractions prévues.

i. La mise en œuvre des traitements de données à caractère personnel en violation des formalités légales préalables

Sont incriminé les faits, même de négligence, et de traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données à caractère personnel.

[16] Rapprocher de l'article 45 de la loi n°2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun qui punit « l'autorité de certification et/ou ses agents qui divulguent, incitent ou participent à la divulgation des informations qui leur sont confiées dans le cadre de l'exercice de leurs activités… ».

ii. Le non-respect de la mise en demeure de cesser le traitement de données à caractère personnel adressée par la Commission des Données Personnelles

Cette atteinte consiste à procéder, même de manière non intentionnelle à un traitement qui a fait l'objet de la mesure prévue au point 1 de l'article 30 de la loi sur les données à caractère personnel,

iii. La mise en œuvre des traitements de données à caractère personnel en violation des normes simplifiées ou d'exonération établies par la commission des Données personnels.

Cette action est constitutive d'un cas de cybercriminalité lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par l'article 19 de la loi sur les données à caractère personnel précitée, quiconque n'aura pas respecté, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la commission des données personnelles.

iv. La mise en œuvre des traitements de données à caractère personnel, hors des cas autorisés, incluant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques.

On parle de cybercriminalité, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi sur les données à caractère personnel précitée, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques.

v. La mise en œuvre des traitements de données à caractère personnel en violation de l'obligation de préserver la sécurité des données.

Elle consiste à traiter des données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 71 de la loi sur les données à caractère personnel précitées.

vi. La collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite[17]

vii. La mise en œuvre des traitements de données à caractère personnel en violation du droit d'opposition de la personne concernée

Est incriminé le fait de procéder ou de faire procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne conformément

[17] V. Ph. BELLOIR, Le délit de collecte déloyale de données à caractère personnel à l'épreuve d'Internet, RLDI, Juin 2006, n°17, p. 28 et s.

aux dispositions de l'article 68 de la loi sur les données à caractère personnel, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes

viii. La mise et la conservation sur support ou en mémoire informatique de données sensibles

Sera considéré comme cyberdélinquant, l'individu qui aura, hors les cas prévus par la loi, mis ou conservé sur support ou mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales, ou qui sont relatives à la santé ou à l'orientation sexuelle de celui-ci.
Les dispositions du premier point du présent article sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

ix. La mise et la conservation sur support ou en mémoire informatique de données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté

Les menaces qui pèsent sur la vie privée peuvent avoir pour origine, hors les cas prévus par la loi, la mise ou la conservation sur support ou mémoire informatique des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

x. La mise en œuvre des traitements illicites de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé.

La criminalité de haute technologie peut prendre la forme d'un traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé dans l'hypothèse où :

- sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ainsi que des dispositions prises pour leur traitement, leur conservation et leur protection ;

- malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

xi. La conservation des données à caractère personnel au-delà de la durée nécessaire à leur finalité

La criminalité liée à l'informatique peut se caractériser en cas de conservation des données à caractère personnel au-delà de la durée nécessaire prévue par l'article 35 de la loi sur les données à

caractère personnel, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

xii. Le traitement de données à caractère personnel à des fins autres qu'historiques, statistiques ou scientifiques au-delà de la durée nécessaire à leur finalité

Quiconque aura, hors les cas prévus par la loi, traité à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée nécessaire prévue par l'article 35 de la loi sur les données à caractère personnel.

xiii. Le détournement de finalité de données à caractère personnel

Quiconque, détenant des données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, aura détourné ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la commission des données personnelles autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement.

xiv. La divulgation illicite de données à caractère personnel

Cette atteinte, fait partie de la catégorie de cas de cybercriminalité qui consiste à recueillir, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, porté, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir.
L'imprudence et la négligence sont incriminées étant entendu que la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

xv. L'entrave à l'action de la Commission des Données Personnelles

Sont consacrées diverses infractions liées à cette entrave, à savoir :

- l'opposition à l'exercice des missions confiées à ses membres ou aux agents habilités en application de la loi sur les données à caractère personnel ;
- le refus de communiquer à ses membres ou aux agents habilités en application de la loi sur les données à caractère personnel, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
- la communication des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée où qui ne présentent pas ce contenu sous une forme directement accessible.

2.2.2.3. Association de malfaiteurs informatiques

Cette infraction se caractérise par la participation à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la loi sur la cybercriminalité.

Dans la perspective sud-africaine, la section 3 du ECT act, act 25 of 2002 consacre la théorie de l'équivalence fonctionnelle qui permet d'étendre l'application de la prévention du crime organise (act, act 121 of 1998) à tous les actes criminels commis dans le même but.

2.2.3. Les atteintes aux biens

2.2.3.1. Escroquerie sur les réseaux

a. Convergences

L'infraction d'escroquerie sur les réseaux est relevée dans la plupart des études nationales (Afrique du Sud, Cameroun, Egypte, Ghana, Nigéria, Sénégal, …). La forme la plus classique est celle qui utilise l'Internet, mais elle n'est pas exclusive. De plus en plus d'escrocs utilisent des réseaux de téléphonie (notamment le GSM). Le mode opératoire généralement utilisé est l'envoi massif d'e-mails ou de sms prometteurs de contrats d'affaires, de transferts d'importantes sommes d'argent issues d'un héritage, des gains substantiels à des loteries étrangères ou encore, à plus petite échelle, de promotion au travail, voire de mauvaises nouvelles concernant un proche. Il s'agit principalement pour les cyberdélinquants de demander une assistance pour transférer des fonds d'un pays à un autre moyennant une contrepartie financière[18] ou de solliciter un transfert de crédit téléphonique ou un simple appel vers un numéro de téléphone souvent surtaxé (V. Cameroun).

Cette infraction, dont les conséquences peuvent aller jusqu'à la commission d'homicides, est devenue une véritable industrie en Afrique et particulièrement au Nigeria, encore appelée « fraude 419 », selon la section 419 du Code pénal nigérian. La police sud-africaine, par exemple, mais aussi Scotland Yard, Interpol et les services secrets américains ont créé des départements spéciaux pour lutter contre ce type d'infractions. Sur Internet, il existe plusieurs associations chargées de répertorier les sites « suspects » ou lorsque les faits sont caractéristiques de l'escroquerie sur internet, ces associations peuvent demander aux hébergeurs de les clôturer.

Elle apparaît récurrente et il semble que les auteurs de ce type d'infractions ont souvent été arrêtés[19]. Par ailleurs, il existe certains pare-feux et systèmes anti-spam qui bloquent automatiquement les sites et e-mails répertoriés comme étant frauduleux.

b. Particularités nationales

Divergences

[18] E. A. CAPRIOLI, Escroquerie « à la nigériane » et sites électroniques de rencontres, Comm. com. électr., décembre 2007, note sous TGI la-Roche-sur-Yon, 24 septembre 2007, p. 46

[19] - Cybercriminalité : Nigeria, Sénégal, Côte d'Ivoire, Burkina, Ghana, Bénin, Togo « fichés » par les Indiens. Ouestaf News: par Amadou Makhtar FALL. mardi 22 juillet 2008 / Ouestaf News/http://start5g.ovh.net/~regultel/spip.php?article 635

- Cybercriminalité à Kédougou un émigré sénégalais vivant aux USA en fait… les frais. Sud quotidien, mardi 31 mars 2009: par Mamadou cheikh fall

http://www.xibar.net/CYBERCRIMINALITE-Un-emigre-senegalais-vivant-aux-Usa-en-fait-les-frais_a15638.html

South Africa: L'ECT act, act 25 of 2002, section 87 interdit l'extorsion, la fraude et la contrefaçon. La fraude peut également être sanctionnée sur la base du droit commun.

Cameroun : Au Cameroun, deux stratagèmes ont été plusieurs fois utilisés. Tout d'abord, il est arrivé que pratiquement au même moment, plusieurs abonnés à la téléphonie mobile reçoivent sur leur téléphone portable des messages leur annonçant explicitement ou leur faisant croire qu'ils avaient gagné tantôt de l'argent, tantôt un crédit de communication, tantôt un voyage en Europe avec leur famille, et les invitant, pour les formalités y afférentes, à appeler à un numéro de téléphone qui était clairement indiqué. A chaque fois, au bout du fil, le répondant confirmait le gain et entretenait de très longues conversations téléphoniques avec les victimes, qui devaient plus tard se rendre compte que l'annonce était mensongère. Ensuite, le second stratagème consiste à appeler un abonné très tard la nuit, pour lui annoncer qu'un des siens qu'on nomme très clairement est victime d'un accident de la circulation et se trouve aux services d'urgence (parfois qu'il en est mort) et de demander un transfert immédiat de crédit de communication pour permettre à l'informateur de donner plus de détails sur l'accident. Les fonctionnaires avides de nomination sont aussi assez régulièrement escroqués par des appelants qui leur signalent que leur dossier de nomination à tel poste est en bonne voie, mais qu'il faudrait fournir un pot-de-vin pour un heureux aboutissement.

Egypte : En Egypte, le système légal classe de tels actes comme des fraudes et escroqueries classiques. Les juridictions appliquent les dispositions pénales traditionnelles. Ces dispositions ne sont pas adaptées aux fraudes sur Internet dans la plupart des cas (Etude Egypte, p. 9).

Ghana : L'étude nationale ghanéenne fait état de l'existence d'une forme d'escroquerie appelée « gold scam » qui consiste dans le fait de créer une société aurifère réelle ou fictive et, sur cette base d'escroquer des clients étrangers en utilisant le moyen des TIC.

Sénégal : Les juridictions répressives sénégalaises du fond ont eu l'occasion de sanctionner à plusieurs reprises l'escroquerie en ligne sur le fondement du droit commun de l'escroquerie, puisque dans la plupart des cas les cyberescrocs obtiennent la remise de fonds à la suite de l'emploi de manœuvres frauduleuses (mensonge accompagné d'éléments extérieurs : mails, fichiers attachés, documents envoyés…)[20].

Silences
Maroc : L'escroquerie sur les réseaux n'est pas traitée par la loi marocaine.

[20] V. notamment, T.R.H.C.Dakar, 15 mai 2007 ; Sur un cas d'escroquerie en ligne au Sénégal, V. S. B. YAGUE, Un cas typique de cybercriminalité, in « Informatique et libertés, quel cadre juridique pour le Sénégal ? », Séminaire, Actes, Dakar, 29 et 30 août 2005, p. 143 et s.

2.2.3.2. Le spamming et le fishing[21]

Les atteintes à la propriété se commettent principalement par la voie de l'escroquerie de façon générale, mais de manière plus spécifique à travers les instruments de paiement électroniques.

L'exemple typique en Afrique de l'Ouest reste le « 419 scam » (fraude 419). Ce procédé consiste à envoyer à une victime potentielle un spam, mail non sollicité. Le contenu du spam sera alléchant et reproduira à peu près ceci: « *Je vous demande de l'aide pour sortir illégalement une très grosse somme d'argent du Nigeria. En échange, vous toucherez une commission sur cette somme. Il vous suffit de donner votre numéro de compte en banque afin que l'argent y soit versé*».

Afrique du Sud : L'ECT act, act 25 of 2002, section 86 (1) et Section 45 prohibe le spamming et les attaques visant à bloquer le service.

Maroc : Le phishing (hameçonnage) n'est pas traité par la loi marocaine.

2.2.3.3. Le vol

La soustraction frauduleuse d'information au préjudice d'autrui est assimilée au vol.
Au Sénégal, cet acte est incriminé semble-t-il, par une extension de la théorie du vol classique[22], étant entendu que la jurisprudence avait, déjà trois années avant l'adoption de la loi sur cybercriminalité, par une interprétation téléologique très courageuse (peut-être aussi contestable), admis la possibilité d'un vol de données informatiques : jugement n° 1981 du Tribunal Régional Hors Classe de Dakar du 6 mai 2006, affaire dite de la « *Clinique du Cap* », confirmée par l'arrêt n° 680 de la Cour d'Appel de Dakar du 16 avril 2007. Cet arrêt fait l'objet de pourvoi en cassation devant la Haute Juridiction qui malheureusement, a rendu un arrêt de cassation[23].
Au Maroc, le vol de données et l'espionnage informatique ne sont pas traités par la loi.

2.2.3.4. L'escroquerie portant sur une information

Cet acte est mis en œuvre à travers la réception d'informations personnelles, confidentielles ou encore protégées par le secret professionnel par l'usage de manœuvres frauduleuses quelconques ou en utilisant de faux noms ou de fausses qualités.

---

[21] Sur le fishing, V. B. AMAUDRIC du CHAFFAUT et Th. LIMOUZIN-LAMOTHE, Op. Cit., p. 142 et 143; N. MARTIN, Phishing : what's happening ? Quelles solutions juridiques pour lutter contre le phishing ? Legalis. Net 2007-I, p. 68 et s.

[22] J. PASSA, La propriété de l'information : un malentendu, Droit et Patrimoine, 2001, n°91 ; M.P LUCAS de LEYSSAC, Une information seule est-elle seule susceptible de vol ou d'une autre atteinte juridique aux biens, D. 1985.Chron. p. 48 ; P.CATALA, Ebauche d'une théorie juridique de l'informatique, D. 1984, Chron. p. 9 ; D. CIOLINO-BERG, Vol d'information sur Internet, Comm.- com. électr., nov. 2003.

[23] P. A. Touré, *La cyberstratégie de répression de la cybercriminalité au Sénégal : la présentation de la loi n° 2008- 11 du 25 janvier 2008 portant sur la cybercriminalité*, juillet 2008

2.2.3.5. Le recel d'information

Cette action est admise comme étant un cas de cybercriminalité dès lors qu'il s'agit d'informations enlevées, détenues ou obtenues à l'aide d'un crime ou d'un délit[24]. A ce niveau encore, la première Chambre correctionnelle du Tribunal Régional Hors Classe de Dakar après avoir écarté la thèse du recel portant sur une information dans l'affaire Madiambal DIAGNE ayant fait l'objet d'un jugement du 21 novembre 2006[25], l'a finalement retenue dans un autre jugement rendu le 1e avril 2008, dans une affaire de recel portant sur une information couverte par le délit d'initié ; cette espèce a été rendue bien avant l'entrée en vigueur de la loi sur la cybercriminalité ; ce qui renseigne sur l'importance de la politique criminelle judiciaire dans le traitement de la cybercriminalité.

2.2.3.6. L'abus de confiance

a. Convergences

L'abus de confiance n'a pas été retenu dans toutes les études nationales comme relevant de la cybercriminalité. Il consiste dans le fait de porter atteinte à la fortune d'autrui en détournant ou détruisant ou dissipant tout bien susceptible d'être soustrait et qu'on a reçu à charge de le conserver, de le rendre, de le représenter ou d'en faire un usage déterminé. Tout bien peut faire l'objet d'abus de confiance qu'il soit corporel, comme un ordinateur, ou incorporel, comme la connexion Internet. Si aucun cas de jurisprudence n'a été cité dans les pays étudiés, des décisions étrangères ont toutefois été rapportées, notamment, de la Chambre criminelle de la Cour de cassation française, sanctionnant le détournement par un salarié de l'ordinateur et de la connexion de l'usage pour lequel ils avaient été mis à sa disposition, et ce, afin de consulter et de stocker des images pornographiques, au titre d'un abus de confiance[26].

b. Particularités nationales

L'étude nationale sénégalaise ne fait pas état de l'abus de confiance parmi les atteintes aux biens commis au moyen des TIC.

2.2.3.7. Le blanchiment d'argent

Le blanchiment n'a pas fait l'objet de développements spécifiques dans la plupart des rapports nationaux. Il est cité dans les rapports Cameroun, Sénégal et Ghana, sans davantage de développements, comme phénomène cybercriminel. L'étude sur l'Egypte, dans laquelle il est traité au titre des atteintes à la propriété fait office d'exception notable.

---

[24] S. JACOPIN, Le début d'une évolution sur la nature de la chose susceptible d'appropriation frauduleuse, RDP, avril 2001, p. 4 ; D. CHEVROTIN, Bévue sur le caractère non « recelable » d'une information, Dr. Pén. mars 2001, p. 4 ;

[25] V.TRHC Dakar, n° 5310 du 21 novembre 2006, affaire Madiambal DIAGNE : « « (…) attendu que toutefois quelle que soit l'infraction d'origine, la chose recelée doit avoir une existence matérielle ; Qu'elle ne saurait dès lors porter sur une telle information mais seulement sur son support matériel ; Qu'au regard de ce principe, le recel ne peut être retenu en l'espèce, qu'en effet, il n'a pas été dit que le procès verbal support matériel des informations publiées a été dérobé ou subtilisé (…) »

[26] Crim. 19 mai 2004, n° 03-83.953. *D*. 2004, somm.2749, obs. Lamy.

Le blanchiment d'argent est spécifiquement prohibée par le "Financial intelligence centre ac, 2001 (Act 38 of 2001) et par le Prevention of organized crime act 1998 (act 121 of 1998). Le currencies and exchange act, act 9 of 1933) pourrait également servir de base légale à l'interdiction des crimes financiers dans l'environnement électronique.

2.2.4. Les atteintes à la propriété intellectuelle

a. Convergences

Les atteintes à la propriété intellectuelle qui sont favorisées par les technologies de l'information et de la communication sont les délits de contrefaçon. La contrefaçon est prévue en matière de brevet d'invention[27], de marque de produits ou de services[28], de modèle d'utilité[29] et de droit d'auteur[30]. Dans toutes ces matières, il s'agit d'atteinte au monopole d'exploitation conféré par le titre protégé. Cette atteinte se réalise très souvent par les moyens classiques de fabrication, de vente ou d'exposition de produits physiques. Mais elle peut également se réaliser par le moyen des technologies de l'information et de la communication. Dans la société de l'information, ces atteintes aux créations charriées par le cyberespace sont devenues une véritable préoccupation[31] pour les titulaires de droits de propriété intellectuelle. C'est le cas par exemple des logiciels. L'atteinte à la propriété intellectuelle peut également porter sur un nom de domaine qui bénéficie d'une protection.

---

[27] Accord de Bangui du 24 février 1999 modifiant celui du 02 mars 1977 instituant une organisation africaine de la propriété intellectuelle, annexe I, article 58 : Sous quelques réserves prévues par le texte, « toute atteinte portée aux droits du breveté, soit par l'emploi de moyens faisant l'objet de son brevet, soit par le recel, soit par la vente ou l'exposition en vente ou soit par l'introduction sur le territoire national de l'un des Etats membres d'un ou plusieurs objets, constitue le délit de contrefaçon ».

[28] Accord de Bangui du 24 février 1999 modifiant celui du 02 mars 1977 instituant une organisation africaine de la propriété intellectuelle, annexe III, article 37..Ce texte vise « a) Ceux qui, frauduleusement apposent sur leurs produits ou les objets de leur commerce, une marque appartenant à autrui ; b) ceux qui sciemment vendent ou mettent en vente un ou plusieurs produits revêtus d'une marque contrefaisante ou frauduleusement apposée ou ceux qui, sciemment, vendent, mettent en vente, fournissent ou offrent de fournir des produits ou des services sous une telle marque ; c) ceux qui font une imitation frauduleuse d'une marque de nature à tromper l'acheteur ou font l'usage d'une marque frauduleusement imitée ; d) ceux qui sciemment vendent ou mettent en vente un ou plusieurs produits revêtus d'une marque frauduleusement imitée ou portant des indications propres à tromper l'acheteur sur la nature du produit ou ceux qui fournissent ou offrent de fournir des produits ou des services sous une telle marque ». Le texte ajoute : a) Ceux qui sciemment livrent un produit ou fournissent un service autre que celui qui leur a été demandé sous une marque déposée ; b) ceux qui font usage d'une marque portant des indications propres à tromper l'acheteur sur la nature du produit ».

[29] Accord de Bangui du 24 février 1999 modifiant celui du 02 mars 1977 instituant une organisation africaine de la propriété intellectuelle, annexe II, article 41 : « Toute atteinte portée aux droits du titulaire du modèle d'utilité enregistré, soit par l'emploi de moyens faisant l'objet de son modèle d'utilité, soit par le recel, soit par la vente ou l'exposition en vente ou soit par l'introduction sur le territoire national de l'un des Etats membres d'un ou plusieurs objets, constitue le délit de contrefaçon »

[30] A cet égard, l'article 64 de l'annexe VII de l'Accord de Bangui renvoie à la législation nationale. L'article 80 de la loi n° 2000/11 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins du droit d'auteur définit la contrefaçon.

[31] Piratage de logiciels informatiques : Une moyenne de 82 % pour le Sénégal. jeudi 2 août 2007 http://www.osiris.sn/article2941.html

Une grande partie des logiciels propriétaires utilisés dans les micro-ordinateurs dans la plupart des pays en développement sont piratés. Le taux de piratage des logiciels installés dans les micro-ordinateurs a atteint un niveau inquiétant. Selon le responsable régional de la lutte anti-piratage de Microsoft Afrique de l'Ouest, Serge Ntamack, le taux s'élève à « 80 % dans l'Afrique Subsaharienne ». Ces chiffres ont été obtenus à l'issue d'une étude réalisée par un organisme indépendant qui fait des recherches à ce sujet et qui est la jonction entre les éditeurs de logiciels dont Oracle et Microsoft, investis dans la lutte contre le piratage[32].

b. Particularités nationales :

Afrique du sud : La section 27 du Copyright act, act 98 de 1978 interdit la copie illégale, la diffusion et la distribution de contenus protégés. Le Business Software alliance en Afrique du Sud indique un taux de piratage de logiciel qui s'élève à 35 %, ce qui représente un coût de 324 millions USD.[33].

Cameroun : Le Cameroun a adopté une législation interne à côté du texte de l'Organisation africaine de la propriété intellectuelle. En son article 80, la loi n° 2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins définit la contrefaçon comme :
« a) toute exploitation d'une œuvre littéraire ou artistique faite en violation de la présente loi, par représentation, transformation ou distribution par quelque moyen que ce soit ;
b) toute production, communication au public ou mise à la disposition du public par vente, échange, location d'une interprétation, d'un phonogramme, d'un vidéogramme, réalisées sans l'autorisation lorsqu'elle est exigée, de l'artiste interprète, du producteur de phonogramme ou de vidéogramme, ou de l'entreprise de communication audio-visuelle ;
c) toute atteinte au droit moral, par violation d'un droit de divulgation, du droit à la paternité ou du droit au respect d'une œuvre littéraire ou artistique ;
d) toute atteinte au droit à la paternité et au droit à l'intégrité de la prestation de l'artiste interprète ».

Egypte : En Egypte une loi, « Egyptian Intellectual Property Rights Act (EIPRA) 82/2002 », est consacrée à la propriété intellectuelle.

Maroc : La Loi n° 02-00 relative aux droits d'auteur et droits voisins du 15 février 2000 telle qu'amendée et complétée par la loi n° 34-05 du 14 février 2006 est applicable en cette matière au Maroc.

Sénégal : Le Sénégal totalise une moyenne de 82 % de logiciels piratés alors que la moyenne mondiale est de 35 %, soit un manque à gagner de 40 milliards de dollars Us (environ 19.190.000.000.000 F Cfa). Une loi n° 2008-09 du 25 janvier 2008, sur le droit d'auteur et les droits voisins a été adoptée au Sénégal, conformément à l'Accord portant révision de l'accord de Bangui du

[32] Revue de presse, Sud Quotidien, édition du 2 août 2007.
[33] http://www.bsa.org/country.aspx?sc_lang=en-za last accessed 15 December 2010

02 mars 1977[34]. Ces textes prévoient un impressionnant dispositif qui intègre désormais les logiciels et les bases de données dans l'énumération indicative des œuvres de l'esprit protégées au titre du droit d'auteur[35]. Cette énumération expresse présente un grand mérite, puisqu'elle autorise le Juge pénal à sanctionner les comportements constitutifs d'atteintes à ces créations numériques (copie servile de logiciels, reproduction de bases de données…) sur le fondement de l'infraction de contrefaçon, dont le champ a été sensiblement élargi, pour servir les intérêts de la répression. Par ailleurs, devant les fréquentes atteintes dont la propriété intellectuelle classique est l'objet dans le cyberespace, en raison notamment de la généralisation de la pratique du *peer to peer* et la facilité de la copie dans l'environnement électronique, le législateur sénégalais dans la loi du 25 janvier 2008 sur le droit d'auteur et les droits voisins, a envisagé de légaliser le recours aux mesures techniques de protection, qui sont dorénavant pénalement protégées par l'infraction de contrefaçon.

2.2.5. Les infractions relatives aux moyens de paiement électroniques

a. Convergences

Le développement des moyens de paiement électroniques a offert de nouveaux moyens d'atteintes aux biens des personnes. C'est pourquoi les infractions liées aux cartes ou virements électroniques, par exemple visent à protéger contre de telles atteintes.

Par ailleurs, sans doute certaines particularités des sociétés africaines constituent-elles également des facteurs de développement de fraudes aux cartes bancaires. Ainsi, de nombreux cas de remise de codes de cartes bancaires à des proches ont été relevés, singulièrement dans l'étude nigériane.

---

[34] L'accord de Bangui a institué l'organisation africaine de la propriété intellectuelle (OAPI) sur le droit d'auteur et toutes ses annexes. Cette protection s'applique aussi en vertu de l'engagement pris par le Sénégal et les autres membres de l'OAPI d'adhérer:

- à la Convention de Paris pour la protection de la propriété industrielle du 20 mars 1883, telle que révisée en dernier lieu à Stockholm, le 14 Juillet 1967 ;
- à la Convention de Berne pour la protection des s littéraires et artistiques, du 9 septembre 1886, telle que révisée en dernier lieu à Paris, le 24 juillet 1971, et/ou à la Convention universelle sur le droit d'auteur révisée à Paris le 24 juillet 1971 ;
- à l'Arrangement de la Haye concernant le dépôt international des dessins ou modèles industriels, du 6 novembre 1925, tel que révisé à la Haye le 28 novembre 1960 et à Stockholm, le 14 juillet 1967 ;
- à l'Arrangement de Lisbonne concernant la protection des appellations d'origine et leur enregistrement international, du 31 octobre 1958, tel que révisé à Stockholm, le 14 juillet 1967 ;
- à la Convention instituant l'Organisation Mondiale de la Propriété Intellectuelle, signée à Stockholm, le 14 juillet 1967 ;
- au Traité de coopération en matière de brevets, signé à Washington, le 19 juin 1970 ;
- au Traité de Nairobi concernant la protection du symbole olympique de 1981 ;
- au Traité de Budapest sur la reconnaissance internationale des dépôts des micro-organismes aux fins de la procédure en matière de brevets de l977,
- à la Convention Internationale pour la Protection des Obtentions Végétales du 02 décembre 1961, révisée à Genève le 10 novembre 1972, le 23 octobre 1978 et le 19 mars 1991 ; au Traité concernant l'enregistrement des marques fait à Vienne le 12 juin 1973 ; à la Convention de Rome sur la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion de 1961.

[35] V. art. 6 et 8 de la loi sénégalaise sur le droit d'auteur et les droits voisins

b. Particularités nationales

Divergences

Afrique du sud : Le rapport 2010 du South African Banking Risk Information Centre (SABRIC) indique une diminution de 32% des transactions sur cartes contrefaites pendant les trois dernières années représentant un montant de 20 millions USD et une diminution de 60 % de l'usage de cartes volés, ce qui représente un montant de 5 millions USD. Ces résultats ont été obtenus grâce à l'introduction massive de cartes à puce électronique durant la même période[37].

Cameroun et Sénégal :

Des dispositions régionales existent aussi bien en Afrique centrale qu'en Afrique occidentale pour lutter contre la cybercriminalité liée aux moyens de paiement électroniques. A ce titre, on peut citer le Règlement n° 15/2002/CM/UEMOA relatif aux systèmes de paiement dans les Etats membres de l'UEMOA (Afrique occidentale, y compris Sénégal) et le Règlement n° 02/03-CEMAC-UMAC-CM relatif aux systèmes, moyens et incidents de paiement (Afrique Centrale, y compris Cameroun). Les dispositions pénales de ces Règlements contiennent plusieurs infractions, dont la contrefaçon ou la falsification de carte, l'usage d'une carte contrefaite ou falsifiée, l'acceptation d'une telle carte, la fabrication, la détention, la cession d'équipements de contrefaçon ou de falsification de moyens de paiement…

Egypte : En Egypte, il n'existe pas de dispositions consacrées spécifiquement aux infractions sur les cartes bancaires considérées légalement comme des fraudes classiques. Ainsi, les juridictions appliquent les dispositions pénales traditionnelles. Ces dispositions ne sont pas adaptées à ce type de fraudes dans la plupart des cas (Etude Egypte, p. 9).

Ghana : Les fraudes aux cartes bancaires sont très fréquentes au Ghana. En 2008, le pays était classé au 7e rang mondial du point de vue de l'importance des fraudes sur Internet, ce qui lui vaut de figurer sur une liste noire, rendant impossible l'utilisation de carte bancaire sur Internet au Ghana.

Nigéria : Il est relevé l'importance des « ATM fraud » (fraudes aux cartes bancaires), dans l'étude sur le Nigéria, du fait d'une politique consistant à encourager le recours aux opérations sur carte bancaire et à décourager les opérations aux guichets dans les agences bancaires en les surtaxant. Ainsi, les 30 millions de détenteurs de cartes bancaires ont réalisé plus de 100 millions de transactions ATM chaque mois. Certaines statistiques de la presse écrite font état de deux victimes sur cinq détenteurs de cartes bancaires au Nigéria[38].

Silences

Maroc : En droit marocain, il n'a pas été relevé d'infractions spécifiques aux cartes bancaires.

[37] www.sabric.co.za/media last accessed 15 December 2010.

[38] Odidison Omankhanlen, 'ATM Fraud rises: Nigerians groan', http://ndn.nigeriadailynews.com/templates/?a=18250

2.3. Les technologies, supports de la cybercriminalité

2.3.1. Les atteintes sexuelles aux mineurs

a. Convergences

Différentes atteintes sexuelles aux mineures sont incriminées comme des phénomènes cybercriminels. Il s'agit de la pornographie infantile ou à caractère pédophile, ou encore de l'outrage à la pudeur sur mineur. Ces atteintes sexuelles sont généralement comprises de manière large. Ainsi, par exemple, est considérée comme pornographie infantile « *toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite*[40]». Ces atteintes sont classées en cinq catégories à savoir :

- la production, l'enregistrement, l'offre, la mise à disposition, la diffusion, la transmission d'une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique ;

- la mise à disposition, l'importation ou l'exportation d'une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique ;

- la possession d'une image ou d'une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées ;

- la facilitation de l'accès à des images, documents ou représentation présentant un caractère de pornographie infantile à un mineur ;

- les atteintes sexuelles en bande organisée : les atteintes sexuelles aux mineurs font l'objet d'une attention particulière lorsqu'elles ont été commises en bande organisée.

Lorsque de tels actes mettent en scène la pédophilie, ils sont également incriminés, même si aucune définition de la pédophilie n'a été donnée (Sénégal et Cameroun).

b. Particularités nationales

Divergences

Afrique du Sud : La section 28 de la Constitution sud-africaine, act 108 of 1996, interdit la dégradation de la personne. La section 27 du Film and publications act interdit la pornographie infantile.

[40] Loi sénégalaise sur la Cybercriminalité, 2008

Cameroun : La pornographie infantile est prévue par les articles 76, 80 et 81 et de la loi relative à la cybersécurité et à la cybercriminalité. La pédophilie est expressément visée par l'article 80 de la même loi.

Egypte : En juin 2008, l'Egypte a modifié sa loi n°12/1996 sur les enfants pour inclure la criminalisation de la pornographie infantile conformément à l'article 9 de la Convention sur la cybercriminalité.

Nigéria : De nombreux cas d'atteintes sexuelles aux mineurs sont rapportés dans le rapport nigérian, mais selon les auteurs, il s'agit de trafic d'enfants vers l'Europe sans que l'impact des TIC sur ce trafic n'ait été déterminé.

Sénégal : La pornographie infantile est prévue et réprimée par la Loi sénégalaise sur la Cybercriminalité de 2008.

Silences

Maroc : La pornographie enfantine n'est pas traitée par la loi marocaine.

2.3.2. Les infractions de presse

a. Convergences

Au titre des infractions de presse, sont visées une très grande variété de situations qui mettent en cause, de manière générale, les bonnes mœurs, l'honneur, la respectabilité ou la tranquillité des personnes. De telles atteintes sont considérées comme cybercriminelles lorsqu'elles sont commises par tous moyens de diffusion publique, notamment : la radiodiffusion, la télévision, le cinéma, la presse, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures, les discours, chants, cris ou menaces proférés dans les lieux ou réunions publics, tout procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique.

Ainsi sont considérés comme des actes de cybercriminalité :

- la fabrication, la détention en vue d'en faire commerce, distribution, location, affichage ou exposition ;
- l'importation, l'exportation, le transport aux mêmes fins ;
- l'affichage, l'exposition ou projection aux regards du public ;
- la vente, la location, la mis en vente ou en location, même non publiquement ;
- l'offre, même à titre gratuit, même non publiquement sous quelque forme que ce soit, directement ou par moyen détourné ;
- la distribution ou la remise en vue de leur distribution par un moyen quelconque de tous imprimés, tous écrits, dessins, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images contraires aux bonnes mœurs.

b. Particularités nationales

Cameroun : Au titre des infractions de presse, mais sans que cette qualification soit expressément retenue dans l'étude nationale (qui évoque des infractions protégeant la moralité, les bonnes mœurs, ou la tranquillité des personnes), le Code pénal camerounais incrimine l'outrage aux mœurs (art. 264 b.), la publication équivoque (art. 266) ou encore la menace (art. 301 et 302) ou le chantage (art. 303). De manière plus spécifique, la loi n° 2006/018 du 2 décembre 2006 régissant la publicité au Cameroun prévoit plusieurs infractions qui sont susceptibles d'être considérées comme des phénomènes cybercriminels lorsqu'ils utilisent les voies de communication électroniques. Certaines sont destinées à protéger la moralité et d'autres ont des finalités économiques, par exemple de protection des consommateurs ou de la concurrence, comme dans le cadre de la prohibition de la publicité mensongère ou du dénigrement.

Par ailleurs, la loi relative à la cybersécurité et à la cybercriminalité reprend certaines de ces infractions lorsque celles-ci ont été commises au moyen des communications électroniques (articles 77 et suivants).

Egypte : La diffamation commise sur Internet est sanctionnée au même titre que celle qui serait commise sur un autre support. Il peut donc s'agir d'un cybercrime, de même que les injures… Des cas de diffamation utilisant le mail ont été relatés.

Les infractions de presse ne sont pas spécifiquement traités comme de la cybercriminalité, mais relèvent du droit commun (Etude Egypte, p. 15).

Nigéria : Selon l'étude nigériane, les infractions de presse ne sont pas répandues dans ce pays. Le seul cas rapporté est celui de la fermeture d'une chaîne de télévision populaire qui aurait diffusé des nouvelles selon lesquelles le Président aurait été en incapacité pour cause de maladie, citant comme source l'Agence de presse nigériane. Après investigations, un e-mail prétendument émanant de l'Agence de presse nigériane avait été envoyé à une organisation de presse française depuis un ordinateur en Côte d'Ivoire.

Sénégal : Au Sénégal, de tels actes sont incriminés, de manière spécifique par la loi de 2008 sur la cybercriminalité. Ainsi, par cette intégration expresse des moyens de communication numérique par voie électronique dans les actes de publication, les rédacteurs de la loi de 2008, ont entendu dissiper toute ambigüité sur l'assimilation des infractions (diffamation, injures publique, diffusion de fausses nouvelles…) commises via Internet à des infractions de presse. Ces infractions en rapport avec le droit à l'honneur sont essentiellement commises par voie de presse, mais entendue plus largement et englobant les actes commis par les bloggeurs, les membres d'un forum de discussion. Au Sénégal, il est devenu fréquent de constater dans les forums de discussion organisés par les sites d'information (seneweb.com ou rewmi.com par exemple), que des personnes en profitent pour diffuser des propos attentatoires à l'honneur ou à la considération d'autres citoyens. Avant l'adoption de cette Loi sur la cybercriminalité qui réprime les infractions de presse, le juge sénégalais

avait eu à connaitre, d'un cas de commission de cette infraction dans l'affaire « Robert Sagna ».[41] Il avait assimilé, en s'appuyant sur l'ancien article 248 du Code pénal, le réseau Internet à un « procédé technique destiné à atteindre le public » et donc de moyen de diffusion publique.

2.3.3. La xénophobie et le racisme en ligne

a. Convergences

La xénophobie et le racisme en ligne sont considérés comme des cas de cybercriminalité. Selon les Etats, ils sont définis de manière plus ou moins large. Généralement, ils couvrent : « *tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure ou cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes*. ».

A ce titre, est constitutif de xénophobie et de racisme en ligne tout acte de:

a) création, de téléchargement, de diffusion ou de mise à disposition d'écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique ;

b) insulte commise par le biais d'un système informatique ou menace de commettre une infraction pénale, envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques ;

c) la négation, l'approbation ou justification d'actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique. En effet, quiconque aura intentionnellement nié, approuvé ou justifié des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique, sera passible de sanction pénale en vertu de la loi sur la cybercriminalité.

b. Particularités nationales

Divergences

Cameroun : Au Cameroun, les actes de xénophobie ou de racisme sont prévus par l'article 241 du Code pénal qui considère comme une circonstance aggravante le fait que ces délits soient commis

[41] Tribunal Régional de Ziguinchor, Affaire Robert Sagna/ Site sénégalaisement.com, jugement n° 02, 6 janvier 2004. Il était reproché au site senegalaisement.com d'avoir diffusé des informations inexactes et qui se serait livré à une concurrence déloyale dans l'irrespect des casamançais.

par voie de presse. La loi relative à la cybersécurité et à la cybercriminalité incrimine de tels actes lorsqu'ils sont commis par la voie de communication électronique ou d'un système d'information (article 77).

Maroc : Il n'est pas relevé d'infraction spécifique à la xénophobie et au racisme en ligne mais l'article 39 bis du Dahir n° 1-58-378 (3 joumada I 1378) formant Code de la presse au Maroc incrimine le racisme[42].

Nigéria : Selon l'étude nigériane, ces atteintes sont très peu répandues dans ce pays.

Sénégal : La Loi sénégalaise sur la Cybercriminalité de 2008 incrimine la xénophobie et le racisme en ligne.

Silences :

Afrique du Sud : Même si la xénophobie est très importante en Afrique du Sud, elle n'a pas vraiment lieu sur Internet. Seule la couverture médiatique rend visible le racisme et la xénophobie en ligne sans que la technologie n'en soit le support. C'est sans doute pour cette raison qu'aucune règle n'y est consacrée au racisme et à la xénophobie en ligne tandis que des mesures sont prises pour lutter contre la xénophobie qui a fait d'importantes victimes en Afrique du Sud.

Egypte : La loi égyptienne ne consacre pas d'incrimination du racisme ou de la xénophobie en ligne. Ainsi, pour traiter de telles questions, il est fait recours à la notion d'atteinte à l'ordre public (Etude Egypte, p. 15).

2.3.4. Les dérives sectaires

a. Convergences

Il semble qu'aucun des rapports n'ait fait état de l'existence de situations pouvant être qualifiées de dérives sectaires ou de phénomènes criminels relevant d'une telle qualification.

b. Particularités nationales

Nigéria : Au Nigéria, il semble que les dérives sectaires ne soient pas répandues.

Egypte : La loi égyptienne ne consacre pas d'incrimination des dérives sectaires. Ainsi, pour traiter de telles questions, il est fait recours à la notion d'atteinte à l'ordre public (Etude Egypte, p. 15).

[42] Article 39 bis : (ajouté , article 3 de la Loi n° 77-00 promulguée par le Dahir n° 1-02-207 du 3 octobre 2002-25 rejeb 1423 ,(B.O du 6 février 2003)) : Quiconque aura, par l' un des moyens énoncés à l' article 38, incité à la discrimination raciale, à la haine ou à la violence contre une ou plusieurs personnes en raison de leur race, leur origine, leur couleur ou leur appartenance ethnique ou religieuse, ou soutenu les crimes de guerre et les crimes contre l' humanité sera puni d' un emprisonnement d' un mois à un an et d' une amende de 3.000 à 30.000 dirhams ou de l' une de ces deux peines seulement.

2.3.5. Les autres infractions

Certaines études nationales relèvent des infractions particulières.

2.3.5.1. L'homosexualité

Parmi les incriminations particulières qui sont relevées, certaines se prêtent à de réelles critiques au regard de la protection de liberté et de la dignité humaines. Il en est ainsi, par exemple de l'homosexualité qui est incriminée dans certains Etats, parfois expressément.

Ainsi, au Cameroun, l'homosexualité, conçue comme le fait d'entretenir des rapports sexuels avec une personne de son sexe, est incriminée par l'article 347 bis du Code pénal. Allant plus loin, la loi relative à la cybersécurité et à la cybercriminalité réprime non seulement les rapports sexuels eux-mêmes, mais aussi la proposition de réaliser ces rapports (article 83).

2.3.5.2. Le harcèlement

L'étude sur le Ghana révèle l'existence du phénomène du harcèlement qui prend de nouvelles proportions avec l'e-mail et les moyens de communication électroniques. Il se rapproche parfois de la diffamation en ligne lorsque des informations malveillantes sont envoyées par des médias électroniques.

3. Typologie des réponses à la cybercriminalité

Les réponses à la cybercriminalité laissent la place à de très grandes particularités nationales, la matière pénale constituant un domaine de souveraineté des Etats fortement marqué par le caractère strictement national des réponses étatiques de politique criminelle, singulièrement, celles qui relèvent du réseau pénal.

3.1. Les réponses étatiques

3.1.1. Les sanctions prévues

Au regard des études nationales, il est possible de relever deux tendances, d'une part à la sévérité dans la répression et d'autre part, à la diversité des peines retenues à titre principal, accessoire ou de sûreté. La sévérité des peines prévues semble dénoter du fait que l'ensemble des Etats étudiés est sensibilisé à la gravité du phénomène de la cybercriminalité et de l'importance des menaces que ce phénomène fait peser sur les Etats, les économies, les sociétés et les personnes. La diversité des peines révèle, quant à elle, le souci de prendre en compte la complexité du phénomène cybercriminel pour y apporter des réponses adaptées.

Toutefois, il existe un risque réel d'incohérences tant au sein des Etats qu'entre les Etats. Au sein des Etats, les risques d'incohérences proviennent, d'une part, du possible concours entre les sanctions aux infractions dites « classiques » contenues dans les Codes pénaux et les sanctions nouvelles issues des textes destinés à répondre spécifiquement aux phénomènes cybercriminels et d'autre part, de la multiplication des interventions des législateurs face à la diversité des phénomènes cybercriminels. Et entre Etats, les risques d'incohérence et surtout d'inefficacité viendraient de l'absence

d'harmonisation des réponses nationales aux niveaux communautaire et international face à un phénomène qui ignore les frontières.

3.1.1.1. Les sanctions pénales

a. Convergences

Il existe une très grande diversité dans les sanctions prévues face aux phénomènes cybercriminels. Une telle diversité est aisément compréhensible au regard de deux facteurs essentiels : d'une part, la variété des sanctions constitue le pendant de l'hétérogénéité des phénomènes relevant de la cybercriminalité et d'autre part, les sanctions sont propres à chaque Etat et, dans de rares cas, à chaque région (Exemple de l'Afrique centrale ou occidentale en ce qui concerne certaines infractions liées aux systèmes et moyens de paiement électroniques) ou Organisation régionale (Exemple de l'OAPI en ce qui concerne les infractions en matière de propriété intellectuelle dans les Etats membres).

Peines principales :

Il est possible de relever certaines tendances qui semblent se dégager des diverses études nationales. Ainsi, aux peines privatives de liberté s'ajoutent souvent des peines pécuniaires comme peines principales.

Peines privatives de liberté

Des peines d'emprisonnement demeurent présentes, dans tous les pays, comme peine principale pour les infractions retenues. Elles peuvent être cumulatives ou alternatives avec des peines pécuniaires, notamment. Mais il semble que la prison demeure encore un principe important de réponse pénale à la cybercriminalité dans les divers Etats étudiés.

Peines pécuniaires (amendes)

Il convient de noter que les peines privatives de liberté s'accompagnent, ou peuvent être remplacées, dans certains cas, de manière quasi systématique, d'amendes retenues en tant que peines principales. Ainsi, il semble que les infractions relevant de la cybercriminalité mettent souvent en cause des intérêts économiques, même si certaines portent atteinte à d'autres valeurs ou principes comme la sûreté de l'Etat ou la dignité des personnes. Dès lors, les Etats africains ont saisi l'importance de la mise en place de sanctions pénales adaptées qui tiennent compte de cette forte dimension économique des phénomènes cybercriminels. Aussi, les cybercriminels sont-ils souvent frappés « dans leurs portefeuilles » par des amendes dont les montants sont considérables. Ces amendes sont, par ailleurs, adaptées aux personnes morales délinquantes.

On note ainsi, dans l'étude sur le Cameroun, que « dans la rubrique des infractions utilisant les techniques de la communication comme supports et celle des infractions utilisant ces techniques comme cibles, le législateur semble vouloir frapper les cyber-délinquants beaucoup plus dans leur portefeuille. Outre le fait que les minima et les maxima des amendes sont souvent très élevés, il

faudrait souligner le recours très récurrent à la faculté donnée au juge de prononcer l'emprisonnement et l'amende alternativement ou cumulativement. Dans la pratique, et s'agissant d'infractions économiques, les juges prononcent souvent la seule peine d'amende, ne recourant à l'emprisonnement que de façon exceptionnelle. Au demeurant, c'est par cette sanction pécuniaire qu'on peut atteindre les personnes morales ».

Peines complémentaires

Les peines complémentaires peuvent être obligatoires (la publication de la décision judiciaire sur un support de communication numérique) ou facultatives. Les juges ont ainsi une large palette de peines complémentaires facultatives qui peuvent consister dans :

- la coupure de l'accès au site ayant servi à commettre l'infraction ;
- l'interdiction d'émettre des messages de communication numérique ;
- l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction ;
- la l'interdiction de l'hébergement du site ayant servi à commettre l'infraction ;
- la fermeture de sites ou d'établissement.

b. Particularités nationales

Egypte : Il apparait que le système légal égyptien ne dispose pas encore de dispositions spécifiquement destinées à combattre le cybercrime. La lutte contre la cybercriminalité dépend donc encore largement des dispositions pénales classiques. Toutefois, des efforts significatifs sont en train d'être engagés pour doter le pays de textes adaptés. Ainsi, en 2007, un projet de loi sur la protection des informations et données personnelles et la lutte contre les infractions liées à l'information a été initié. Il a été ralenti en 2009, la priorité étant accordée à d'autres textes.

Malgré les efforts intenses du Gouvernement dans le secteur des TIC, les lois actuelles destinées à lutter contre la cybercriminalité sont insatisfaisantes et devraient être revues et unifiées pour stimuler davantage le développement de ce secteur. Certaines lois ont été récemment modifiées pour faire face les nouveaux phénomènes de cybercriminalité. Il en est ainsi de la « Child law 12/1996 » modifiée en 2008, de la « E-signature law 15/2004 » et de la « Intellectual property Act 82/2002 ».

3.1.1.2. Les autres types de sanctions prévues

a. Les sanctions administratives

Les sanctions administratives ne sont prévues que dans les pays ayant consacré des dispositions spécifiques. Elles peuvent être diverses et consistent, par exemple, dans des interdictions temporaires, des retraits d'autorisation, voire des amendes.

b. Les sanctions civiles

Les sanctions civiles existent dans tous les Etats. Elles consistent, notamment, dans la réparation des dommages qui sont causés à la victime du cybercrime.

3.1.2. Les règles applicables à la procédure pénale

Elles consacrent un aménagement des mécanismes procéduraux classiques de traitement des infractions et un renforcement de ce dispositif par l'adoption de nouvelles procédures (la conservation rapide des données informatisées archivées, l'interception de données informatisées…**).** La consécration des formes de cybercriminalité introduites dans les codes pénaux nécessite une modification à la procédure pénale de manière à apporter le maximum possible d'efficacité aux moyens juridiques mis en œuvre pour prévenir et réprimer les infractions commises. C'est le cas, notamment, en Afrique du Sud, au Cameroun, au Sénégal, au Ghana ou en Egypte où d'importantes modifications ont été apportées aux règles procédurales en matière pénale afin de poursuivre et sanctionner les cybercriminels. Ainsi, certaines règles, notamment, en matière de prescription, de preuve ou d'établissement de procès verbal ont été adaptées au numérique en consacrant, au titre de la prescription, la conservation rapide de données informatisées archivées, la perquisition et la saisie informatique ou l'interception des données informatiques ; au titre de la preuve, l'admission des procédés électroniques en matière pénale ; ou encore, en aménageant, la possibilité d'établissement de procès verbaux électroniques.

Certains rapports n'ont toutefois consacré aucun développement aux règles applicables à la procédure, à l'image du Nigéria.

3.1.3. Le traitement judiciaire

Lorsqu'une cyberinfraction est commise, les enquêtes et la constatation sont de la compétence des officiers de police judiciaire à compétence générale, fonctionnaires de police ou gendarmes. Toutefois, la technicité ou la spécialité de certaines matières rendent nécessaire une intervention d'agents relevant d'autres administrations qui reçoivent une habilitation à cet effet. Les administrations sont ainsi souvent impliquées dans tous les processus de traitement des phénomènes de cybercriminalité, des enquêtes à l'exécution de la peine, en passant par les poursuites, l'instruction et le jugement. Elles interviennent dans la mise en place de « filets », dans l'arrestation des auteurs présumés de délits, leur mise à disposition pour comparution devant le procureur et la juridiction de jugement. Ainsi :

- des experts en TIC peuvent être désignés par les juges en vue de les appuyer dans la détermination ou la mise en œuvre de mesures conservatoires des preuves ;
- lorsque le traitement d'un phénomène cybercriminel requiert une investigation interviennent des acteurs tels le juge d'instruction, l'officier de police judiciaire, les membres et agents de commissions spécialisées comme les Commissions nationales chargées des données personnelles, par exemple, pour constater l'effacement de données ;
- en cas de poursuite et d'information judiciaire, en dehors du ministère public, certains agents relevant de divisions spécialisées de police ou de gendarmerie peuvent intervenir lorsqu'elles existent dans les Etats.

3.1.3.1. La coopération internationale

La cybercriminalité présente la particularité d'ignorer les frontières étatiques. Elle est transfrontalière car non seulement les auteurs, complices et victimes des infractions peuvent se trouver dans des pays ou des continents différents, mais aussi l'élément matériel de certaines infractions peut être localisé sur des territoires différents. Or elle menace, au-delà des individus, les Etats eux-mêmes qui se trouvent ainsi soumis à des atteintes à leur sûreté et, particulièrement au risque de terrorisme. Face à un tel phénomène, il est évident qu'une réponse strictement nationale serait inefficace. Les Etats consentent ainsi plus aisément à coopérer dans le domaine de la lutte contre la cybercriminalité.

Dans cette optique, l'étude nationale camerounaise fait remarquer que la loi relative à la cybersécurité et à la cybercriminalité fait de la coopération internationale et de l'entraide policière et judiciaire une priorité. Il en est de même de la loi sénégalaise sur la cybercriminalité.

De même, la loi sud africaine, section 90 de act 25 of 2002, prend en compte la nature internationale de la cybercriminalité en prévoyant la compétence des autorités juridictionnelles dès lors qu'un lien existe avec l'Afrique du sud. L'Afrique du sud est également member de SADC et, à ce titre, est signataire de l'accord d'assistance mutuelle et du Réseau des chefs de police d'Afrique de l'Est.

3.2. Les réponses sociétales

En dehors du rapport sur le Cameroun, tous les autres ont consacré de nombreux développements aux différentes réponses sociétales aux phénomènes cybercriminels. Les réponses envisagées peuvent impliquer des sphères strictement nationales. Dans cette optique, on peut citer et noter, dans le cadre du rapport national nigérian, l'action d'organisations comme The Global Network for cybersolutions, Youth against cybercrime and fraud in Nigeria, Paradigm Initiative Nigeria ou encore, Nigerian Computer Society. Ont été notées également, dans le rapport national sur le Ghana des réactions sociétales contre la cybercriminalité de la part de personnalités religieuses ou du milieu de l'éducation. Dans le rapport sur l'Egypte, ont été soulignées d'importantes expériences sur le partenariat public-privé en vue d'accroitre la vigilance et la réaction de la société face au cybercrime dont les plus saillantes sont le « Cyber Peace Initiative » et le « Family e-safety initiative ». Dans le rapport sur le Maroc, il est noté que la stratégie Maroc Numeric 2013 constitue une véritable feuille de route en matière d'instauration de confiance numérique. Plusieurs réponses sociétales sont ainsi prévues dans ce cadre au titre desquels on peut citer principalement l'instauration d'une culture de sécurité à travers des actions d'éducation, de formation et de sensibilisation par rapport aux différents enjeux liés à la cybercriminalité.
Mais les réponses sociétales s'inscrivent surtout dans des dynamiques internationales. Ainsi, diverses orientations sont souvent contenues dans des documents stratégiques et manuels que les acteurs de la société de l'information peuvent valoriser et utiliser. Il s'agit, généralement, des meilleures pratiques à partager résultant du cadre international, relevées dans le rapport national sénégalais et formalisées dans :

- le manuel pour la prévention et la répression de la criminalité informatique[43] : il s'agit d'une publication des Nations Unies qui cible les différents Etats membres de la communauté internationale en vue de la mise en place de législations adaptées, et harmonisées en matière de lutte contre la cybercriminalité. A cet effet, en plus de bénéficier de référentiel dans le domaine procédural, ils disposent de cadre conceptuel et des repères pour saisir les phénomènes criminels dans lesquelles l'informatique est l'objet du délit et des infractions dans lesquelles l'informatique est le moyen du délit.

- le Guide des Bonnes Pratiques en matière de Sécurité Economique[44], illustré d'exemples concrets, a été conçu pour servir de boussole et poser les jalons d'un renforcement de la sécurité économique en entreprise. Dans la mesure où l'efficacité de stratégie promue est fonction de l'interaction des différents acteurs, le guide prévoit un réel partenariat privé-public pour l'évaluation constante et la détection des risques auxquels sont exposées les entreprises et à les protéger contre ceux-ci. Il faut noter que le présent Guide est issu d'une collaboration entre la Brigade de Surveillance du territoire de Strasbourg, la Direction Régionale des Renseignements Généraux d'Alsace, la DRIRE Alsace, le détachement de la Direction de Protection et de la Sécurité de la Défense de Strasbourg, la Trésorerie Générale, la Gendarmerie Nationale et la Région Alsace.

- le Guide des Bonnes Pratiques en matière d'Intelligence économique qui est la résultante de l'instruction adressée aux différents les préfets[45] de région d'élaborer un plan triennal cohérent d'intelligence économique offensif à l'attention des manageurs et chefs d'entreprise. Ce guide intègre l'ensemble des enjeux et exigences de l'intelligence économique devant certaines pratiques, parfois déloyales, utilisées par la concurrence pour s'approprier ses innovations, son savoir-faire, ou pour la déstabiliser et l'affaiblir. Il mettra l'accent à cet effet, sur la création d'un noyau dur d'informations stratégiques, et la valorisation des moyens de protection disponibles afin de pouvoir mettre en œuvre ceux qui apparaissent les plus appropriés dans le cadre de l'utilisation des TIC.

- le guide pratique du chef d'entreprise face au risque numérique : risques identifiés et solutions proposées en 10 études de cas[46]. Ce guide met en relief le fait que « les entreprises sont au cœur de la lutte contre l'insécurité numérique ». En marge des ambitions affichées dans le Forum, l'idée clé qui transparait dans ce Guide est que les entreprises doivent en devenir un acteur à part entière. De sorte que, la sensibilisation et la formation des cadres,

---

[43] Revue internationale de politique pénale, No. 43 et 44. Nation Unies .1994. (Publication des Nations Unies, numéro de vente: F.94.IV.5).

[44] http://www.e-alsace.net/documents/fck/file/documents_pdf/Guide_IE12-09-2007[1].pdf) www.e-alsace.net/index.php/headnews/get

[45]Préfecture de la région franche –comté préfecture du Doubs/France www.veille.ma/+Dossier-special-Veille-Magazine+.htm; intel.ecobesancon@interieur.gouv.fr) (http://www.veille.ma/IMG/pdf/guide-des-bonnes-pratiques-en-matiere-intelligence-economique.pdf

[46]Le Forum International sur la Cybercriminalité .3e version du 24 mars 2009. http://www.veille.ma/IMG/pdf/risque-numerique-guide-pratique-chef-entreprise.pdf

des managers, des chefs d'entreprise aux risques numériques sont considérées comme des moteurs de la prise de conscience individuelle et collective. En informant les acteurs économiques de la réalité du risque et des réponses apportées par les pouvoirs publics, ce guide illustre concrètement la coopération entre l'Etat et les entreprises françaises. En effet, issu d'un partenariat public-privé (institutions, universitaires, profession du Droit, les Forces de sécurité françaises et étrangères et entreprises), ce Guide est principalement destiné aux PME-PMI. Il met entre autre l'accent sur les axes de travail qu'il appartient aux autorités désignées de définir pour mener au mieux la protection des personnes et des biens dans le cyberespace et permettre ainsi le développement de l'économie numérique ;

- le Guide de la cybersécurité pour les Pays en développement, Union Internationale des Télécommunications, 2007. Ce guide a été élaboré en vue de « fournir aux pays en développement un outil pour leur permettre de mieux comprendre certains enjeux liés à la sécurité des technologies de l'information, ainsi que des exemples de solutions mises en place par d'autres pays pour faire face à ces problèmes. Il cite également d'autres publications permettant d'obtenir de plus amples renseignements sur la cybersécurité. Ce guide ne constitue pas un document ou un rapport exhaustif sur la question, mais vise à récapituler les principaux problèmes que rencontrent actuellement les pays qui veulent tirer parti des avantages offerts par la société de l'information[47] » ;

- le Guide de la cybersécurité pour les Pays en Voie de Développement. Union Internationale des Télécommunications, 2006. Ce manuel s'intéresse principalement aux besoins et éléments de solution de la cybersécurité qui est ici analysée selon ses dimensions managériales, politique, économique, sociale juridique et technologique. Les réponses qui y sont proposées, dans leur dimension globale, se veulent aussi différenciées pour permettre un élargissement des perspectives de lutte tout en tenant compte des infrastructures de communication. (www.itu.int/ITU-D/cyb);

- le Guide à destination des fournisseurs d'accès à internet. Il a été produit par le[48]Centre de Recherches Informatique et Droit. (CRID, FUNDP – Namur) dans le cadre d'un contrat de recherches financé par le Ministère des Affaires économiques, 2002. Il est exposé dans l'avant propos de ce Guide que dans « ce document est axé sur des recommandations destinées aux fournisseurs d'accès à Internet en vu de leur faciliter le respect de leurs obligations juridiques relatives à à la vie privée, aux pratiques commerciales et à leur responsabilité. Ces recommandations générales sont destinées à expliciter certaines lois applicables aux fournisseurs d'accès Internet.

[47] www.itu.int/ITU-D/cyb

[48] Guide en Version en françaishttp://mineco.fgov.be/information_society/enterprises/providers_internetguide/home_fr.html

3.3. Les réponses techniques

3.3.1. Les réponses consacrées

a. Convergences

Les réponses techniques sont orientées vers la sécurisation des systèmes et réseaux informatiques. Ces réponses s'appuient dans une large mesure sur la cryptologie, composée de la cryptographie et de la cryptanalyse. Elles sont destinées à assurer la protection et la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises.

La cryptologie est à l'heure actuelle la solution technique incontournable pour protéger les échanges et les systèmes d'information sur les nouvelles technologies contre d'éventuelles violations de leur intégrité. A cet effet, elle vise à garantir la confidentialité des systèmes, des données stockées, échangées ou circulant sur l'Internet, sur l'Intranet voire sur un simple réseau privé.

Le recours à certaines technologies comme les puces électroniques, par exemple sur les cartes bancaires concourent à la sécurisation des transactions.

Il convient de noter que toutes les études nationales relèvent l'importance que revêtent les réponses techniques et l'insuffisance des seules réponses juridiques à prendre en charge de manière satisfaisante la lutte contre la cybercriminalité. Toutefois, un certain retard et quelques insuffisances sont souvent déplorés du fait, principalement des la faiblesse des moyens à disposition pour mettre en place des réponses techniques adéquates aux phénomènes cybercriminels.

b. Particularités nationales

Afrique du sud : La cryptologie est largement utilisée. L'ECT act, act 25 of 2002, section 80 autorise la mise en disposition d'inspecteurs destinés à intégrer des équipes de police disposant d'équipements de haute technologie. Le RICPCI act, section 16 of act 70 of 2002, permet également aux représentants de la loi d'avoir accès à des informations cryptées par le biais d'injonctions de décryptage. La section 32 of act 70 of 2002 permet aussi la mise en place de centres d'interception qui seront utilisés pour surveiller les communications.

Cameroun : Dans l'ensemble, on trouve au Cameroun très peu de réponses techniques au phénomène de la cybercriminalité. En l'état actuel, l'étude sur le Cameroun n'a relevé que le Règlement COBAC relatif à la lutte contre le blanchiment des capitaux et le financement du terrorisme prescrit une vigilance particulière en ce qui concerne tous les transferts de fonds, « quel que soit le support de réception ou d'exécution de l'ordre ou le procédé technique utilisé »[49]. Toutefois, après avoir déploré la grande faiblesse des moyens techniques dont dispose

[49] Article 24 du Règlement CABOC R-2005/01 du 1er avril 2005 relatif aux diligences des établissements assujettis en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme en Afrique centrale. Ce texte est pris à la suite du Règlement CEMAC n° 01/03/CEMAC-UMAC portant prévention et répression du blanchiment des capitaux dans les Etats membres de la CEMAC.

l'Administration, certaines réponses techniques en cours de réalisation ont été présentées : l'installation d'un serveur de surveillance des domaines de la zone « .cm » à l'Agence nationale des TIC et l'identification des abonnés au téléphone et des terminaux. Par ailleurs, la loi relative à la cybersécurité et à la cybercriminalité prévoit certaines dispositions techniques. Ainsi, ce texte institue un organe devant assurer, pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques ainsi qu'une redevance à laquelle sont assujettis les autorités de certification accréditées, les auditeurs de sécurité, les éditeurs de logiciels de sécurité et les autres prestataires de sécurité agréés. Cette redevance est destinée à la constitution d'un fonds dénommé « Fonds spécial des activités de sécurité électronique » et devant permettre le financement de la recherche, du développement, de la formation et des études en matière de cybersécurité (article 9). Il s'y ajoute certaines obligations spécifiques :

- aux opérateurs de réseaux et aux fournisseurs de services de communications électroniques, fournisseurs d'accès, de services et des contenus d'installer des mécanismes de surveillance de trafic des donnés de leur réseau et de conserver les données de connexion de trafic pendant une période de dix (10) ans ;

- aux fournisseurs de contenus des réseaux de communication électroniques et systèmes d'information de mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs ;

- aux réseaux de communications électroniques et systèmes d'information de se soumettre de manière obligatoire et périodique à un audit de leurs systèmes de sécurité par l'organe de régulation ;
- Enfin, aux opérateurs du secteur de la communication de fournir aux utilisateurs un certain nombre d'informations relatives à la sécurité

Maroc : La stratégie Maroc Numeric 2013 constitue une véritable feuille de route en matière d'instauration de confiance numérique. Plusieurs réponses techniques sont prévues. Il s'agit principalement de :

- la mise en place de Ma-CERT (traitement des incidents de sécurité)
- la mise en place du portail national de sécurité des SI
- la mise en place des datacenters bunkerisés

Nigéria : L'étude sur le Nigéria relève certaines réponses techniques qui sont, parfois partagées avec d'autres Etats, notamment, le recours aux puces électroniques sur les cartes bancaires ou la régulation des domaines « .ng » par la Nigerian Internet Registration Association (NIRA) instituée en 2005. D'autres réponses techniques peuvent retenir l'attention de façon plus particulière. Ainsi la « Economic and Financial Crimes Commission » est en train de mettre au point un système de contrôle des e-mails sortant du Nigéria. Une fois opérationnel, il devrait permettre d'isoler et détruire les e-mails frauduleux et avertir les destinataires.

Sénégal : Au Sénégal, la cryptologie est utilisée dans plusieurs secteurs notamment l'administration, les télécommunications et l'informatique, plus précisément au niveau des centres d'appels, des sociétés de transfert d'argent, ainsi que pour les paiements électroniques.

Les dispositifs de lutte contre la cybercriminalité mis en place rendent difficile la commission de certaines infractions. En effet, les cyberdélinquants devront avoir recours à des technologies avancées, et d'un niveau supérieur pour pouvoir contourner les dispositifs de protection. C'est dans cette logique les établissements de monnaie électronique ont par exemple utilisé les plateformes monétiques basées sur les normes EMV (Europay MasterCARD Visa).
Le Sénégal a également opté pour les cartes d'identité numériques et les passeports biométriques pour mieux lutter contre les fraudes identitaires.

3.3.2. Articulation entre les réponses étatiques, sociétales et techniques

Les différentes approches juridiques, techniques et sociétales ne sont pas concurrentes, mais complémentaires. Toutefois, les mécanismes opérationnels ne sont pas encore mis sur place, au regard des contraintes liées à la disponibilité des moyens matériels et logistiques des autorités chargées de la prévention et de la répression de la cybercriminalité, même s'il est vrai que l'apport de la recherche ne doit pas être négligée.
Aujourd'hui, les difficultés de mobilisation des ressources matérielles, financières et humaines demeurent un défi à relever, cela d'autant plus que la lutte contre la cybercriminalité demeure une priorité nationale et régionale dans toutes les parties de l'Afrique. Il est vrai que des efforts sont entrain d'être fait, par les autorités étatiques.
Par contre, les moyens logistiques sont quasi inexistants pour assurer la surveillance des réseaux informatiques, ce qui explique que les autorités ne soient pas complètement opérationnelles.

4. Conclusions et recommandations

4.1. Conclusions et recommandations générales

L'étude exploratoire sur la cybercriminalité et la sécurité en Afrique intervient dans un contexte de faible connaissance du phénomène à l'échelle du continentale. Les rapports nationaux présentés ont permis à partir d'une grille méthodologique harmonisée de cerner le phénomène dans ses diverses expressions dans les cinq régions d'Afrique avec des études de cas illustratifs à l'appui. Les conclusions sont très enrichissantes en ce qu'elles ouvrent de façon claire des pistes de recherches sur les questions cruciales à approfondir à travers la formulation précise de problématiques.

En termes d'impact, au moins trois perspectives méritent d'être signalées :

- La Commission Economique des Nations Unies pour l'Afrique (CEA) a décidé de mettre en place une chaire sur le cyberdroit à partir de 2010-11. La chaire pourra s'appuyer sur les résultats de la recherche et le réseau des chercheurs ayant travaillé sur le thème. Le CRDI pourra être un partenaire de choix de cette chaire ;

- L'Union africaine a placé le prochain sommet (janvier 2010) sous le thème des technologies de l'information et de la communication. Les documents préparatoires mentionnent dans les

recommandations l'élaboration d'une convention africaine sur la cybersécurité et la cybercriminalité devant être adoptée avant 2012. Deux des chercheurs du réseau CRDI (Basil, Abdoullah) ont travaillé sur les projets de textes de l'UA ;

- La conférence organisée conjointement par le MAECI et le CRDI (février 2010) sur « La prochaine frontière mondiale : l'innovation et la technologie dans la nouvelle Afrique» met l'accent sur la place de l'Afrique dans le monde numérique et s'interrogera sur comment l'accès à Internet et aux technologies numériques façonne-t-il la société et les entreprises africaines? Une étude sur la cybercriminalité et la sécurité en Afrique sera déterminante quant à l'éclairage qu'elle apportera sur l'examen de cette problématique.

Par ailleurs, il est apparu, au sortir de cette étude et de l'Atelier de restitution de Dakar, l'utilité, l'opportunité et la nécessité de poursuivre, au-delà de l'étude exploratoire, les efforts entamés en vue d'une meilleure compréhension de la cybercriminalité en Afrique qui, seule, permettra d'apporter les réponses adéquates, plurielles, différentielles et inclusives à un phénomène complexe et multidimensionnel. Un **Réseau africain sur la cybercriminalité** et la sécurité en Afrique a été identifié comme le cadre idéal en vue de mener de telles réflexions et actions. Et la décision a été prise, lors de l'Atelier de restitution, à l'unanimité des participants, de mettre en place ce réseau.

Les éléments clés du réseau ont été déclinés : l'orientation stratégique, les membres, les objectifs, le cadre juridique, les moyens et les grandes lignes d'un plan d'action.

1. L'orientation stratégique

Il a été précisé l'orientation principalement juridique du réseau. Toutefois, il doit être ouvert à toutes autres sensibilités et disciplines pouvant permettre de percevoir et cerner l'ensemble des facettes du phénomène de la cybercriminalité en Afrique en vue d'éclairer, d'accompagner et de compléter les réponses juridiques à consacrer.

2. Les membres

Les participants sont les membres fondateurs du réseau qui reste ouvert à l'adhésion ou la cooptation de toutes les compétences utiles.

3. Les objectifs

Le réseau aura pour objectif, dans le domaine de la cybercriminalité et la sécurité, de mener des réflexions et actions de :

- formation ;
- recherche ;
- information et communication ;
- plaidoyer ;
- expertise légistique ;

- coopération.

4. Le cadre juridique

Les grandes orientations du cadre juridique du réseau ont été identifiées. Le réseau devra ainsi :

a. se doter, d'une part, d'une charte qui devra préciser les principes de responsabilité et d'action et d'autre part, élaborer un cahier des charges ;

b. reposer sur une organisation souple et opérationnelle, structurée autour

- d'une coordination exécutive (coordinateurs général, régionaux et sous-régionaux) ;
- d'une coordination de projets (nationaux et thématiques) ;
- de cellules opérationnelles (cyberlégislations ; veille, information et communication ; formation ; développement et renforcement des capacités ; coopération) ;

c. déterminer le cadre de ses relations avec l'observatoire des cyberlégislations africaines créée sous l'égide la Commission Economique des Nations unies pour l'Afrique.

5. Plan d'action

Les grandes lignes d'un plan d'action basé sur les objectifs définis ont été déclinées.

a. Formation :

- Elaboration d'un module sur la cybercriminalité en Afrique en formation ouverte et à distance ;
- Organisation de formations présentielles par pays ciblant certains groupes (décideurs, parlementaires, banques, services de sécurité).

b. Recherche :

- Lancement des recherches sur les priorités de niveau 1 ;
- Rédaction d'un ouvrage sur une thématique prioritaire courant 2011 ;
- Rédaction de guides d'informations et de bonnes pratiques à destination de groupes cibles ;
- Rédaction d'un modèle de charte de conduite dans le cyberespace à destination des écoles et lycées ;
- Organisation d'un atelier sur la cybercriminalité et la sécurité en marge du Comité pour le Développement de l'information scientifique et technologique (CODIST II, avril 2011).

c. Information et sensibilisation :

- Mettre en place un dispositif de veille juridique et technologique sur le thème dont les résultats seront diffusés sur le site web du forum en rapport avec l'observatoire des cyberlégislations africaines de la CEA. Le site web permettra en outre d'enregistrer les contestations et plaintes des victimes ;

- Créer une base de données sur la cybercriminalité en Afrique ;

- Publier les informations sur un site dédié ;

- Animer un stand au CODIST ;

- Informer le public par la publication des guides sur la sécurité sur Internet à l'usage des groupes cibles.

d. Plaidoyer :

- Actions en faveur de l'élaboration, de l'adoption et de l'application d'une convention africaine sur la cybercriminalité et la sécurité ;

- Promouvoir le dialogue interinstitutionnel mais aussi le dialogue entre acteurs, experts et politiques.

e. Expertise en légistique : appui aux gouvernements dans l'élaboration des cyberlégislations et mise en place d'une base de données des experts africains en matière de cybercriminalité.

f. Promouvoir la coopération aux niveaux de la collecte de l'information, entre les institutions, entre les polices et les administrations judiciaires.

6. Les moyens

Pour la mise en œuvre de ses activités, le réseau compte d'abord sur les offres spontanées de services de ses membres. Les offres déjà enregistrées lors de l'atelier couvrent : la mise en place du site web et son hébergement, la veille juridique et la veille technologique, le plaidoyer, l'élaboration des outils méthodologiques, le plaidoyer et le fonctionnement du Réseau.

Celui-ci pourra également solliciter l'appui de partenaires tels que le GIM UEMOA, les Communautés économiques régionales (CER), les instituts universitaires de technologies (IUT), la Commission économique des Nations unies pour l'Afrique (CEA), le Centre de recherches pour le développement international (CRDI), les réseaux universitaires, les agences de régulation au niveau national et toute structure intéressée par les activités du Réseau.

L'adoption de ce plan d'action a permis la clôture de cet atelier de restitution sur une note très positive. L'occasion a alors été saisie pour magnifier :

- l'organisation très satisfaisante de cet atelier par toute l'équipe du CRDI ;

- la riche participation de l'ensemble des experts présents et représentés ainsi que de toutes les délégations nationales et des invités ;

- l'engagement et le soutien effectifs de la CEA et de tous les autres partenaires ;

- l'esprit constructif et l'atmosphère conviviale qui ont prévalu lors des discussions dans la salle de séminaire et en dehors ;

- la très remarquable coordination des travaux qui a déteint sur la qualité des échanges et des résultats de cet atelier.

4.2. Recommandations sur les problématiques à approfondir

Les priorités de recherches définies dans les divers rapports et au cours de l'atelier de restitution de Dakar ont été déclinées à trois niveaux dont le premier correspond à celles qui sont cruciales, le deuxième, à celle qui sont nécessaires et la troisième à celles qui sont utiles pour la cohérence avec l'environnement.

Les priorités de niveau 1 ont été classées en trois catégories distinctes selon qu'elles ont trait à la méthodologie, aux thématiques de recherche globale et aux thématiques spécifiques.

1. Problématiques d'ordre méthodologique

La complexité du phénomène de la cybercriminalité et les menaces qu'elle fait penser sur la sécurité des organisations étatiques, privées et sociétales semblent aller de pair avec l'absence d'une méthodologie adéquate pour cerner les contours du phénomène. Aussi, concernant la méthodologie, trois priorités ont été dégagées :

- la réalisation d'un guide méthodologique sous la forme d'un questionnaire d'audit de la cybercriminalité afin de mieux comprendre le phénomène. Le guide méthodologique qui a servi de base à la recherche pourra servir de point de départ.

- l'élaboration d'une typologie opératoire des phénomènes cybercriminels ;

- la mise en place d'instruments de mesure de l'ampleur de la cybercriminalité.

2. Problématiques d'ordre substantiel

En plus de la question méthodologique, certaines problématiques fondamentales ont été identifiées comme prioritaires. Il est possible de distinguer, parmi elles, entre les thématiques de recherche globale et les thématiques spécifiques.

a. Thématiques de recherche globale sur la cybercriminalité

Au titre de la recherche globale, trois thématiques ont été retenues :

- les perceptions de la cybercriminalité dans les contextes africains ;

- l'identité numérique et la cybercriminalité (avec une réflexion sur l'Afrique et l'évolution des réponses techniques à la cybercriminalité) ;

- la coopération (législative, judiciaire, policière, technologique) contre la cybercriminalité.

b. Thématiques spécifiques de recherche sur la cybercriminalité

Pour ce qui est des thématiques spécifiques, quatre ont été identifiées :

- démocratie, droits humains et cybercriminalité ;
- commerce électronique, finance et cybercriminalité ;
- les réponses africaines à la cybercriminalité (projet de convention africaine de lutte contre la cybercriminalité et pour la sécurité).
- cybercriminalité et groupes cibles (jeunes, femmes, familles, entreprises, juges, police, environnement…).

5. Tableau de synthèse

Question/Problème	Convergences	Particularités nationales		
		Etats	Divergences	Silences
1.1. Introduction/ Contexte	- Développement et généralisation de l'usage des TIC dans les pays étudiés ; - Développement corrélatif de la cybercriminalité ; - Importance et gravité des conséquences des phénomènes cybercriminels ; - Intérêt pour l'ensemble des Etats de la mise en place d'un cadre adéquat de lutte contre la cybercriminalité ; - Ecart entre ampleur de la cybercriminalité et faiblesse des réponses en termes de capacités juridiques et techniques d'appréhension, de prévention, de poursuite et de répression de la cybercriminalité.	Afrique du Sud	- 4, 5 millions d'usagers d'Internet en 2008 ; - 15% de taux de pénétration d'Internet (110^{e} rang mondial).	
		Cameroun		
		Egypte	- 12, 57 millions d'usagers d'Internet en fin 2008 ; - taux d'utilisation d'Internet de 15% pour les ménages, 59,6%pour les entreprises et 34% pour les entités publiques.	
		Ghana	- 7ème rang mondial en 2008 en matière de cybercriminalité dans les Etats.	
		Maroc	- Le Marché de l'Internet a enregistré une forte évolution au cours de l'année 2009, avec une croissance du parc d'abonnés de 56,7% (1.186.923 abonnés à fin 2009, contre 757.453 à fin 2008), avec un taux de pénétration de 3,81% à fin 2009 (contre 2,46% une année auparavant) ; - 53 % des entreprises publiques ont accès à l'Internet ; - 87 % des entreprises privées ont accès à l'internet.	
		Nigéria	- 3ème rang mondial en 2007 en matière de cybercriminalité après le Royaume-Uni et les Etats-Unis.	
		Sénégal		
1.2. Introduction/ Question de départ	- capacité du cadre juridique actuel à répondre, de manière adéquate, au phénomène de la cybercriminalité ; - incidemment, opportunité d'une	Afrique du Sud	- question visant uniquement le cadre juridique de lutte contre la cybercriminalité.	
		Cameroun	- question large intégrant les dimensions juridique, institutionnel et technique de la lutte contre la cybercriminalité.	

	amélioration du cadre existant ou de la mise en place d'un nouveau cadre de lutte contre la cybercriminalité.	Egypte	- question large intégrant les dimensions juridique, institutionnel et technique de la lutte contre la cybercriminalité.	
		Ghana	- question large intégrant les dimensions juridique, institutionnel et technique de la lutte contre la cybercriminalité.	
		Maroc	- la question vise uniquement le cadre juridique de lutte contre la cybercriminalité et n'intègre pas les dimensions institutionnelles et techniques.	
		Nigéria	- question visant uniquement le cadre juridique de lutte contre la cybercriminalité.	
2.1. Technologies, objets de la cybercriminalité				
2.1.1. Atteintes aux systèmes informatiques	Ont été notées trois catégories d'atteintes aux systèmes informatiques qui affectent la confidentialité (accès, intrusion ou maintien frauduleux dans un système), l'intégrité (perturbation ou interruption d'un système ou réseau) ou la disponibilité des systèmes (introduction ou tentative d'introduction de données dans le système sans autorisation).	Afrique du Sud	La Section 86 (1 à 5) du ECT Act incrimine l'accès non autorisé à un système et l'altération de données dans un système automatisé.	
		Cameroun	Phénomène incriminé par la loi relative à la cybersécurité et à la cybercriminalité.	
		Egypte	Pour être incriminée et sanctionnée, l'accès non autorisée doit être sous-tendue par l'intention ou le dessein de détériorer ou détruire (article 361 du Code pénal, v. Etude Egypte, p. 8).	
		Ghana	Cette classification n'est pas retenue.	
		Maroc	Accès illégal (Article 607-3 du Code Pénal) ; Atteinte à l'intégrité des données (Article 607-4 du Code Pénal) ; Sabotage informatique (Article 607-5 du Code Pénal).	
		Nigéria	Importance des atteintes à la disponibilité des systèmes du fait du hacking.	
		Sénégal	Toutes ces atteintes sont incriminées par la loi sur la cybercriminalité de 2008.	
2.1.2. Atteintes aux systèmes automatisés des	Diverses atteintes aux données informatisées consistant dans la destruction, l'endommagement,	Afrique du Sud		
		Cameroun	Phénomène incriminé par la loi relative à la cybersécurité et à la cybercriminalité.	

données	l'effacement, la détérioration, l'altération ou la modification frauduleuse… constituent des phénomènes cybercriminels. Entrent dans ce cadre, l'interception et la tentative d'interception frauduleuse, le faux informatique, l'usage de faux informatique ou encore la fraude informatique. Dans l'ensemble des études nationales, de telles atteintes sont présentées comme des phénomènes cybercriminels, mais ne sont pas toujours analysées comme des atteintes aux systèmes automatisés des données.	Egypte		
		Maroc	Falsification informatique (Article 607-7 du Code Pénal) ; Fraude informatique (Article 607-7 du Code Pénal).	
		Nigéria		
		Sénégal	Il s'agit d'atteintes aux systèmes automatisés des données prévues par la loi de 2008 sur le cybercriminalité.	
2.1.3. Atteintes au système de cryptologie	Sont considérées comme des atteintes au système de cryptologie les activités permettant d'accéder frauduleusement à tout ou partie d'un système informatique protégé.	Afrique du Sud	Les fournisseurs de services de cryptologie doivent être enregistrés et leur activité est encadrée de manière stricte par la section 29 du ECT Act 25 de 2002.	
		Cameroun	La loi relative à la cybersécurité et à la cybercriminalité incrimine le refus de coopération avec les autorités habilités par communication ou mise en œuvre d'une convention secrète ou d'un moyen de cryptologie.	
		Egypte		
		Ghana		
		Maroc	Accès illégal (Article 607-3 du Code Pénal) ; Atteinte à l'intégrité des données (Article 607-4 du Code Pénal) ; Utilisation d'un moyen de cryptographie pour préparer ou commettre un crime ou un délit ou pour en faciliter la préparation ou la commission (Article 33 de la loi n° 53-05).	
		Nigéria		
		Sénégal		
2.2. Technologies, moyens de la cybercriminalité				
2.2.1. Cyberterrorisme et atteintes aux	Le cyberterrorisme n'a pas de définition unique dans les rapports. Le phénomène ne semble pas important dans les Etats	Afrique du Sud		
		Cameroun	Terrorisme et atteintes aux intérêts de l'Etat ne sont pas abordés.	

intérêts des Etats	étudiés. D'autres atteintes aux intérêts des Etats ont parfois été relevés, notamment l'espionnage, la trahison, la destruction de documents, données…	Egypte		Pas de dispositions particulièrement consacrées aux actes de cyberterrorisme.
		Ghana	Le cyberterrorisme est cité, sans autre précision, au titre des atteintes à la société (« attack on society »).	Autres atteintes non abordées.
		Maroc	Le cyberterrorisme n'est pas spécifiquement couvert comme l'est le terrorisme de manière générale dans la loi n° 03-03 relative à la lutte contre le terrorisme du 28 mai 2003 ; Est couverte l'atteinte à un système de traitement automatisé de données supposé contenir des informations relatives à la sûreté intérieure ou extérieure de l'État ou des secrets concernant l'économie nationale (Article 607-4 du Code Pénal) est sanctionnée par des peines d'emprisonnement et des amendes.	L'espionnage, la trahison, la destruction de documents et de données ne sont pas traités en droit marocain ;
		Nigéria		
		Sénégal		
2.2.2. Atteintes aux personnes	Avec le développement des TIC, multiplication des cas d'atteinte à l'identité de la personne (ex. usurpation d'identité), à son image, sa voix, au secret de sa correspondance… D'autres atteintes spécifiques aux droits de la personne au regard du traitement des données à caractère personnel ont été présentées.	Afrique du Sud	D'importants développements ont été consacrées à la protection de la vie privée et particulièrement, des informations et données personnelles.	
		Cameroun	Développements consacrés à la protection du secret de la correspondance dans le Code pénal et la loi du 14 juillet 1998 régissant les télécommunications.	
		Egypte		
		Ghana		
		Maroc	Secret des correspondances (Article 11 de la Constitution du Royaume du Maroc) ; Protection des personnes physiques à l'égard du traitement des données à caractère personnel (Loi n° 09-08).	Ne sont pas traités par la loi marocaine : Usurpation d'identité numérique ; Pornographie enfantine ; Actes de nature raciste et xénophobe.
		Nigéria	Recrudescence de la cyberdélinquance basée sur le vol	

			d'identité, notamment par le biais de réseaux sociaux.	
		Sénégal		
2.2.3. Atteintes aux biens	Diverses atteintes aux biens ont été envisagées, notamment l'escroquerie sur les réseaux, le scamming et le fishing, le vol, l'escroquerie portant sur une information, le recel d'information, l'abus de confiance, le blanchiment d'argent.	Afrique du Sud		
		Cameroun		
		Egypte		
		Ghana		
		Maroc	Sabotage informatique (Article 607-5 du Code Pénal) ; Spamming (Article 10 de la loi n° 09-08) ; Blanchiment d'argent (Loi n° 43-05 du 17 avril 2007 relative à la lutte contre le blanchiment de capitaux).	Ne sont pas traités par la loi marocaine : Escroquerie sur les réseaux ; Interception illégale de données ; Espionnage informatique et vol de données ; Usurpation d'identité dans le cadre des communications électroniques ; Phishing (hameçonnage).
		Nigéria		
		Sénégal		
2.2.4. Atteintes à la propriété intellectuelle	L'ensemble des Etats a prévu et sanctionné les atteintes à la propriété intellectuelle, notamment le piratage qui prend une ampleur considérable en Afrique, avec un taux de 80 % de logiciels piratés en Afrique subsaharienne selon le représentant de Microsoft.	Afrique du Sud		
		Cameroun	Dispositions de l'OAPI applicables, en plus de dispositions nationales.	
		Egypte		
		Ghana		
		Maroc	Loi n° 02-00 relative aux droits d'auteur et droits voisins du 15 février 2000 telle qu'amendée et complétée par la loi n° 34-05 du 14 février 2006.	
		Nigéria		
		Sénégal	Dispositions de l'OAPI applicables, en plus de dispositions nationales.	
2.2.5. Infractions	Avec le développement des moyens de	Afrique du Sud		

relatives aux moyens de paiement électroniques	paiement électronique, il est noté la multiplication de fraudes les concernant. Elles atteignent des proportions inquiétantes dans certains pays.	Cameroun	Existence de dispositions communautaires luttant contre les fraudes aux cartes bancaires et moyens de paiement électroniques, notamment, le Règlement n° 02/03-CEMAC-UMAC-CM relatif aux systèmes, moyens et incidents de paiement.	
		Egypte		
		Ghana		
		Maroc		Pas d'infractions spécifiques en droit marocain
		Nigéria		
		Sénégal	Existence de dispositions communautaires luttant contre les fraudes aux cartes bancaires et moyens de paiement électroniques, notamment, le Règlement n° 15/2002/CM/UEMOA relatif aux systèmes de paiement dans les Etats membres de l'UEMOA.	
2.3. Technologies, supports de la cybercriminalité				
2.3.1. Atteintes sexuelles aux mineurs	Différentes atteintes sexuelles aux mineures sont incriminées comme des phénomènes cybercriminels. Il s'agit de la pornographie infantile ou à caractère pédophile, ou encore de l'outrage à la pudeur sur mineur.	Afrique du Sud	La section 28 du ECT Act prévoit l'incrimination de la pornographie infantile.	
		Cameroun	La pornographie infantile est prévue par la loi relative à la cybersécurité et à la cybercriminalité. La pédophilie est aussi expressément visée par ladite loi.	
		Egypte	En juin 2008, l'Egypte a modifié sa loi n°12/1996 sur les enfants pour inclure la criminalisation de la pornographie infantile conformément à l'article 9 de la Convention sur la cybercriminalité.	
		Ghana		
		Maroc	L'attentat à la pudeur consommé ou tenté sans violence, sur la personne d'un mineur de moins de dix-huit ans est sanctionné par des peines d'emprisonnement par l'article 484 du Code Pénal.	Pas d'infractions spécifiques à la pornographie infantile ni à des atteintes sexuelles

				aux mineurs par voie électronique.
		Nigéria	Il n'y aurait qu'un impact minime des TIC selon l'étude consacrée à ce pays.	
		Sénégal		
2.3.2. Infractions de presse	Au titre des infractions de presse, sont visées une très grande variété de situations qui mettent en cause, de manière générale, les bonnes mœurs, l'honneur, la respectabilité ou la tranquillité des personnes. De telles atteintes sont considérées comme cybercriminelles lorsqu'elles sont commises par tous moyens de diffusion publique, notamment : la radiodiffusion, la télévision, le cinéma, la presse, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures, les discours, chants, cris ou menaces proférés dans les lieux ou réunions publics, tout procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique. Ces phénomènes ne sont pas incriminés de la même manière dans tous les pays.	Afrique du Sud		
		Cameroun	Les infractions de presse sont prévues par le Code pénal, la loi relative à la publicité et la loi relative à la cybersécurité et à la cybercriminalité.	
		Egypte	Les infractions de presse ne sont pas spécifiquement traités comme de la cybercriminalité, mais relèvent du droit commun (Etude Egypte, p. 15).	
		Ghana		
		Maroc	Les infractions de presse ne sont pas spécifiquement traitées comme de la cybercriminalité, mais relèvent du droit commun : Dahir n° 1-58-378 (3 joumada I 1378) formant Code de la presse au Maroc qui incrimine les atteintes aux bonnes mœurs, à l'honneur et à la respectabilité.	
		Nigéria	Selon l'étude nigériane, les infractions de presse ne sont pas répandues dans ce pays.	
		Sénégal	Incrimination spécifique de tels actes par la loi de 2008 sur la cybercriminalité.	
2.3.3. Xénophobie et racisme en ligne	La xénophobie et le racisme en ligne, considérés comme des cas de cybercriminalité couvrent : « *tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans*	Afrique du Sud		La xénophobie est très importante en Afrique du Sud mais n'a pas vraiment lieu sur Internet. Aucune règle n'y est consacrée spécifiquement au racisme et à la xénophobie en ligne.

	la mesure ou cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes. »	Cameroun	Existence d'une incrimination commune de la xénophobie ou du racisme, la commission par voie de presse étant une circonstance aggravante. Une incrimination spécifique de la xénophobie ou du racisme en ligne est prévue dans la loi relative à la cybersécurité et à la cybercriminalité.	
		Egypte		La loi égyptienne ne consacre pas d'incrimination du racisme ou de la xénophobie en ligne.
		Ghana		
		Maroc	Pas d'infraction spécifique à la xénophobie et au racisme en ligne mais Article 39bis du Dahir n° 1-58-378 (3 joumada I 1378) formant Code de la presse au Maroc incrimine le racisme : Article 39 bis : (ajouté , article 3 de la Loi n° 77-00 promulguée par le Dahir n° 1-02-207 du 3 octobre 2002-25 rejeb 1423 ,(B.O du 6 février 2003)) : Quiconque aura, par l' un des moyens énoncés à l' article 38, incité à la discrimination raciale, à la haine ou à la violence contre une ou plusieurs personnes en raison de leur race, leur origine, leur couleur ou leur appartenance ethnique ou religieuse, ou soutenu les crimes de guerre et les crimes contre l' humanité sera puni d' un emprisonnement d' un mois à un an et d' une amende de 3.000 à 30.000 dirhams ou de l' une de ces deux peines seulement.	
		Nigéria	Atteintes très peu répandues dans ce pays.	
		Sénégal	Incrimination spécifique par la loi sur la Cybercriminalité de 2008.	
2.3.4. Dérives sectaires	Aucun des rapports n'a fait état de l'existence de situations pouvant être qualifiées de dérives sectaires ou de phénomènes criminels relevant d'une telle	Afrique du Sud		
		Cameroun		
		Egypte		
		Ghana		

	qualification.	Maroc		
		Nigéria		
		Sénégal		
2.3.1. Autres infractions prévues	Certains pays adoptent certaines incriminations spécifiques.	Afrique du Sud		
		Cameroun	L'homosexualité, conçue comme le fait d'entretenir des rapports sexuels avec une personne de son sexe, est incriminée. La loi relative à la cybersécurité et à la cybercriminalité prévoit de réprimer les rapports sexuels eux-mêmes, mais aussi la proposition de réaliser ces rapports.	
		Egypte		
		Ghana	Evocation du harcèlement qui prend de nouvelles proportions avec l'e-mail et les moyens de communication électroniques.	
		Maroc		
		Nigéria		
		Sénégal		
3.1. Réponses étatiques à la cybercriminalité				
3.1.1. Sanctions prévues	Des sanctions pénales et extrapénales sont prévues. On note une tendance à la sévérité des sanctions pénales et un recours important aux peines pécuniaire à côté des peines privatives de liberté. Ont été notés des risques d'incohérences, tant au niveau interne à chaque état qu'entre les Etats.	Afrique du Sud		
		Cameroun		
		Egypte		
		Ghana		
		Maroc		
		Nigéria		
		Sénégal		
3.1.1. Règles applicables à la procédure pénale	Il est noté une certaine inadaptation de la procédure pénale pour la poursuite et la répression de la cybercriminalité.	Afrique du Sud		
		Cameroun		
		Egypte		
		Ghana		
		Maroc		
		Nigéria		
		Sénégal		

3.1.1. Traitement judiciaire	En plus de la nécessité d'une formation des juges, il a été relevé l'importance du recours à l'expertise pour traiter de la cybercriminalité, ainsi que l'importance particulière d'une coopération internationale du fait que la cybercriminalité ignore les frontières étatiques.	Afrique du Sud		
		Cameroun		
		Egypte		
		Ghana		
		Maroc		
		Nigéria		
		Sénégal		
3.2. Réponses sociétales à la cybercriminalité				
3.2. Réponses prévues	Il existe une certaine disparité entre les Etats, en ce qui concerne la prise en charge sociétale de la cybercriminalité.	Afrique du Sud		
		Cameroun		
		Egypte		
		Ghana		
		Maroc		
		Nigéria		
		Sénégal		
3.3. Réponses techniques à la cybercriminalité				
3.3. Réponses consacrées	La même disparité entre les Etats, en ce qui concerne la prise en charge sociétale de la cybercriminalité est notée à propos des réponses techniques. Par contre, il existe une importante convergence dans le constat de l'insuffisance des moyens techniques de lutte contre la cybercriminalité dans les pays concernés, malgré les efforts que consentent les gouvernements.	Afrique du Sud		
		Cameroun		
		Egypte		
		Ghana		
		Maroc	La stratégie Maroc Numeric 2013 constitue une véritable feuille de route en matière d'instauration de confiance numérique. Plusieurs réponses techniques prévues sont prévues. Il s'agit principalement de : La mise en place de Ma-cert (traitement des incidents de sécurité) La mise en place du portail national de sécurité des SI La mise en place des datacenters bunkerisés.	
		Nigéria		
		Sénégal		

4.2. Recommandations sur les problématiques à approfondir	Voir la liste des thématiques retenues.	Afrique du Sud		
		Cameroun		
		Egypte		
		Ghana		
		Maroc		
		Nigéria		
		Sénégal		

6. Bibliographie

6.1. Textes constitutionnels et législatifs et instruments réglementaires

Afrique du Sud

- Telecommunications Act, No. 103 of 1996
- Electronic Communications Act, No. 36 of 2005
- Electronic Communications and Transaction Act, No. 25 of 2002
- South African Constitution Act, No.108 of 1996
- Electronic Communications and Transaction Act, No. 25 of 2002 – No. R.504 Accreditation Regulations
- Electronic Communications and Transaction Act, No. 25 of 2002 – No. R. 1166 Alternative Dispute Resolution Regulations
- Electronic Communications and Transaction Act, No. 25 of 2002 – No. R. 216 Cryptography Regulations

Cameroun

Textes en vigueur

- Code pénal ;
- loi n°2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun ;
- loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun ;
- loi n° 2006/018 du 29 décembre 2006 régissant la publicité au Cameroun ;
- loi n°2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins,
- loi n° 98/014 du 14 juillet 1998 régissant les télécommunications au Cameroun ;
- Arrêté n° 000006/MINPOSTEL du 27 mai 2009 fixant les modalités d'identification des abonnés et des terminaux des réseaux de téléphonie ouverts au public.

Avant-projet de loi

- Avant-projet de loi régissant les communications électroniques au Cameroun.

Egypte

- Penal Code, Law n°58 of 1937.
- Procedural Law n°150 of 1950.
- Law No. 80 of 2002 for combating money laundering
- Egyptian Intellectual Property Rights Act (EIPRA) 82/2002
- Communications Law 10/2003
- E-signature Law no°15/2004
- Child Law n°12/1996 as modified in June 2008.

Ghana

- Constitution of the Republic of Ghana, 1992
- Criminal Offences Act, 1960 (Act 29)
- Criminal and Other Offences (Procedure) Act, 1960 (Act 30)
- Evidence Act, 1975 (N.R.C.D. 323)
- Courts Act, 1993, (Act 459)
- Anti-Terrorism Act, 2008 (Act 762)
- National Communications Authority Act, 2008 (Act 769)
- National Information Technology Act, 2008 (Act 771)
- Electronic Transactions Act, 2008 (Act 772)
- Electronic Communications Act, 2008 (Act 775)

Sénégal

L'ensemble des dispositifs ci-dessous peut être retrouvé dans le site de l'OSIRIS (http://www.osiris.sn/plan.html).

Textes constitutionnels et législatifs

- Constitution du Sénégal du 22 janvier 2001
- Loi 2001-15 du 27/12/2001 portant Code des Télécommunications,
- Loi n° 2006-02 du 4 janvier 2006 modifiant la loi n° 2001-15 du 27 décembre 2001 portant code des télécommunications
- Loi n° 2008-10 du 25 janvier 2008 portant loi d'orientation sur la société de l'information
- Loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.
- Loi n° 2008-11 du 25 janvier 2008 sur la cybercriminalité
- Loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel
- Loi du 25 janvier 2008 sur le droit d'auteur et les droits voisins.
- Loi n° 2008-41 du 20 août 2008 sur la cryptologie au Sénégal.

Les instruments réglementaires

- Décret relatif à la certification électronique pris pour l'application de la Loi n°2008 08 du 25 janvier 2008 sur les transactions électroniques.
- Décret relatif aux communications électroniques pris pour l'application de la Loi n°2008 08 du 25 janvier 2008 sur les transactions électroniques.
- Décret portant application de la loi n°2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel.
- Décret n° 2008-718 du 30 juin 2008 relatif au commerce électronique pris pour l'application de la loi n° 2008 -08 du 25 janvier 2008 sur les transactions électroniques
- Décision n° 2006- 001 ART/DG/DRJ/DT/D.Rég relative à l'obligation d'identification des abonnés au service de téléphonie mobile.

Nigeria

- Constitution of the Federal Republic of Nigeria 1999

- The Advance Fee Fraud and Other Related Offences Act, 2006
- The copyright Act, Cap C28, Laws of the federation of Nigeria 2004
- Child Rights Act, 2003
- Nigerian Communications Act, 2003
- WIPO Internet Treaties
- Electronic Banking Guidelines, Central Bank of Nigeria.
- E-Transactions Bill, NITDA 2008
- Cybersecurity and Information Protection Agency (Establishment, etc) Bill

6.2. Les textes internationaux

- UN Convention on the Right of the Child, A/RES/44/25 Available online at : www.hrweb.org/legal/child.html
- Les principes directeurs de l'ONU (1990) pour la réglementation des fichiers informatisés contenant des données à caractère personnel.
- La Convention de Budapest du 21 novembre 2001 sur la cybercriminalité, adoptée le 8 novembre à Strasbourg lors de la 109ème session du Comité des ministres des affaires étrangères.< http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm>;
- Le protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, ouvert à la signature en janvier 2003. Ce texte représente un instrument pour la lutte à l'échelon international. Il a été ratifié par la France, par une loi promulguée le 19 mai 2005; http://www.admi.net/jo/20060525/MAEJ0630048D.html
- Cartographie des normes internationales traitant de la cybercriminalité

6.3. Les textes régionaux

Afrique

- Accord de Bangui du 24 février 1999 modifiant celui du 02 mars 1977 instituant une organisation africaine de la propriété intellectuelle ;
- La position Africaine commune[50] _11ème congrès des Nations Unies sur la prévention du crime et la justice pénale tenu à Bangkok (du 28 au 25 avril 2005).

Afrique centrale

- Règlement n°21/08-UEAC-133-CM-18 du 19 décembre 2008 relatif à l'harmonisation des réglementations et des politiques de régulation des communications électroniques au sein des Etats membres de la CAMAC ;
- Règlement n° 02/03-CEMAC-CM relatif aux systèmes, moyens et incidents de paiement ;

- Règlement n° 01/03/CEMA-UMAC portant prévention et répression du blanchiment des capitaux dans les Etats membres de la CEMAC ;
- Règlement COBAC R-2005/01 du 1er avril 2005 relatif aux diligences des établissements assujettis en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme en Afrique centrale ;
- Directive n°06/08-UEAC-133-CM-18 du 19 décembre 2008 fixant le régime du service universel dans le secteur des télécommunications au sein des Etats membres de la CEMAC ;
- Directive n°07/08-UEAC-133-CM-18 du 19 décembre 2008 fixant le cadre juridique de la protection des droits des utilisateurs de réseaux et des services de communications électroniques au sein de la CEMAC ;
- Directive n°08/08-UEAC-133-CM-18 du 19 décembre 2008 relative à l'interconnexion et à l'accès des réseaux et des services de communications électroniques dans les pays membres de la CEMAC ;
- Directive n°09/08-UEAC-133-CM-18 du 19 décembre 2008 harmonisant les régimes juridiques des activités de communications électroniques dans les Etats membres de la CEMAC ;
- Directive n°10/08-UEAC-133-CM-18 du 19 décembre 2008 harmonisant les modalités d'établissement et de contrôle des tarifs de services de communications électroniques au sein de la CEMAC ;
- Décision n°45/08-UEAC-133-CM-18 du 19 décembre 2008 portant création du Comité technique de régulation des communications électroniques dans les Etats membres de la CEMAC.

Afrique du Nord

Afrique occidentale

- Directive N° 07/2002/CM/UEMOA relative a la lutte contre le blanchiment de capitaux dans les États membres de l'union Économique et Monétaire Ouest Africaine (UEMOA)
- Instruction n° 01/2006/SP du 31 juillet 2006 relative à l'émission de monnaie électronique et aux établissements de monnaie électronique
-

Europe

- La Recommandation n° R (95) 13 du Conseil de l'Europe < http://www.coe.int/t/f/droits_de%27homme/media/4_ressources_documentaire/CM/Rec(1995)013_fr.asp > ;
- La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981
- La Décision-cadre2 2005/222/JAI du Conseil, du 24 février 2005, relative aux attaques visant les systèmes d'information; http://www.europa.eu/scadplus/le/fr/lvb/l33193.htm

- La Directive européenne sur la rétention des données de connexion, du 21 février 2005;http://europa.eu.int/eurlex/lex/LexUriServ/site/fr/com/2005/com2005_0438fr01.pdf
- Directive européenne du 12 juillet 2002 relative à la protection des données personnelles dans le secteur des communications électroniques » disponible sur www.europa.eu.int
- Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité, adoptées sous la forme d'une Recommandation du Conseil de l'OCDE lors de sa 1037e session, le 25 juillet 2002.
- La Convention relative à *l*'Organisation de Coopération et de Développement Economiques, en date du 14 décembre 1960, et notamment ses articles 1 b), 1 c), 3 a) et 5 b);
- La Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, en date du 23 septembre 1980 [C(80)58(Final)];
- La Déclaration *s*ur les flux transfrontières de données adoptée par les gouvernements des pays Membres de l'OCDE du 11 avril 1985 [C(85)139, Annexe] ;
- La Recommandation du Conseil relative *a*ux Lignes directrices régissant la politique de cryptographie*,* en date du 27 mars 1997 [C(97)62/FINAL] ;
- La Déclaration ministérielle relative à la protection de la vie privée sur les réseaux mondiaux, en date des 7-9 décembre 1998 [C(98)177/FINAL, Annexe]
- La Déclaration ministérielle sur l'authentification pour le commerce électronique, en date des 7-9 décembre 1998 [C(98)177/FINAL, Annexe];
- Council Framework Decision on Combating the Sexual Exploitation of Children and Children Pornography (2004)
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CET No: 201
- Council of Europe Convention on Cybercrime No: 69: www.conventions.coe.int

6.4. Les rapports, actes de séminaires, de conférences, de colloques

- Actes du Séminaire ADIE-Coopération française «Informatique et libertés, quel cadre juridique pour le Sénégal ? », disponible sur http/www.adie.sn
- AGHATISE E. J. (2006): Level of Awareness of Internet Intermediaries Liability. (HND Project work) Unpublished. Auchi Polytechnic, Auchi, Edo State, Nigeria.
- A glance on the internet in Egypt, in the internet the growing world, Report prepared by the National Telecom Regulatory Authority, available on the website of the Egyptian Ministry of Communications and Information Technology www.mcit.gov.eg [accessed on 30 August 2009].
- Butler, Graham (2008): ITU Global Strategic Report 1.7.8 p. 48
- CISSE Abdoullah (2007): Harmonisation of the Legal Framework Governing ICTs in West African States (UEMOA-ECOWAS)
- Cybercriminalité au Sénégal : www.adie.sn/.../contribution Cybercriminalité_ issakha.doc Monsieur ISSAKHA GUEYE Magistrat de formation Ancien Président de la Chambre Pénale de la Cour de Cassation au Sénégal

- Cybersecurity guide for developing countries, International Telecommunication Union (ITU), Edition 2007, available at: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc---f.pdf
- Gerike, Marco, ITU Global Strategic Report 1.6.2.1 p.34. www.cybercrime.de
- Goodman, Mark (2008): ITU Global Strategic Report 1.8 p. 51
- Hacking Offences, Australian Institute of Criminology and Australian high tech crime centre, 2005, available at: http://www.aic.gov.au/publications/htcb/htcb005.pdf.
- Internet Filtering in Sub-Saharan Africa, OpenNet Initiative
- Internet World Statistics "Kenya Internet Usage and Telecommunications Reports" available at < http://www.internetworldstats.com/af/ke.htm> accessed December 21, 2010.
- ITU Cybersecurity Work Programme to Assist Developing Countries 2007 – 2009, December 2007
- Models for cyber legislations in ESCWA member countries, United Nations Economic and Social Commission for Western Asia, New York, 2007, available at: www.escwa.un.org/information/publications/edit/.../ictd-07-8-e.pdf.
- Ombudsman for Banking Services "An Account of Activities for the period 1 January – 31 December 2008" http://www.obssa.co.za/documents/2008_obs_annual_report.pdf last accessed 30 October 2009
- Séminaire "Informatique et libertés, quel cadre juridique pour le Sénégal ?" (29 et 30 août 2005 Hôtel Méridien Dakar) Contribution de Maitre Lionel KALINA : Lutte contre la cybercriminalité : vers la construction d'un modèle juridique normalisé, actes du Séminaire ADIE-Coopération française «Informatique et libertés, quel cadre juridique pour le Sénégal ? », page 11, disponible sur http/www.adie.sn
- Papa Assane TOURE: audit des normes applicables à la cybercriminalité, actes du Séminaire ADIE-Coopération française «Informatique et libertés, quel cadre juridique pour le Sénégal ? », page 11, disponible sur http/www.adie.sn._juillet 2008
- Understanding cybercrime: a guide for developing countries, International Telecommunication Union (ITU), April 2009, available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html [Accessed 25 August 2009].
- Union Internationale des Télécommunications : 27- 29 Novembre 2007- Praia, Cap-Vert. - Atelier de l'Afrique de l'Ouest sur les Cadres Politiques et Réglementaires pour la Cybersécurité et la Protection de l'Infrastructure de l'Information Critique : http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/praia-cybersecurity-workshop-report-dec-07-f.pdf
- Rapport du Sénat français sur le Loi pour la confiance dans l'économie numérique ;
- Rapport explicatif de la convention sur la cybercriminalité, disponible sur www.coe.int

6.5. Les ouvrages spéciaux, cours et monographies

- AL-ERYAN, Mohamed, Cybercrimes, Dar Al-Gamaa Al-Gadida, Alexandria, 2004.
- AL-SAGHIR, Gamil, Internet and penal law, Dar Al-Nahda, Cairo, 2000.
- AL-SAGHIR, Gamil, Procedural aspects of Internet crimes, Dar Al-Nahda, Cairo, 2000.
- BAINBRIDGE, D.I, (2008) Introduction to Information Technology Law, Edinburgh, Pearson Education Limited, 6th edition
- CONTE (P) et LARGUIER (J), Droit pénal des affaires, Paris, Armand Colin, 2004 ;
- CORNWELL, H., (1987) Data Theft, Heinemann Professional Publishing Ltd,1st edition
- DAVID R. &. BRIERLEY J. E. C., Major Legal Systems in the World Today, 1978.
- HUSSEIN, Mohamed, Legal responsibilities in Internet networks, Cairo, 2002.

- KALINA MENGA (L), Cours de Droit pénal et TIC, Université Gaston Berger, UFR Sciences juridique et politique, Master Droit du cyberespace, année 2006/2007 ;
- KATSH E., (1995) *Law in a Digital World* Oxford University Press, New York.
- KOMMERS Donald P, The Constitutional Jurisprudence of the Federal republic of Germany, Second Edition, 1997.
- KYEI, Kwaku : Understanding Cyber Crime [ISBN 978-9988-1-1885-3] (undated and publisher unknown)
- LLOYD, I.J (2008). Information Technology Law. Oxford. Oxford University Press, 5th edition ;
- LONGE, O.B. (2004): Proprietary Software Protection and Copyright issues in contemporary Information Technology. (M.Sc. Thesis) Unpublished. Federal University of Technology, Akure, Nigeria.
- MAMDOUH, Khaled, Cybercrimes, Dar Al-Fekr Al-Gameay, Alexandria, 2009.
- MC QUOID-Mason. The law of privacy in SA 1978.
- NEETLING, POTGIETER and VISSER, Law of Delict, 5th Ed, 2007.
- RAMADAN, Medhat, Legal protection of e-commerce, Dar Al-Nahda, Cairo, 2001.
- RAMADAN, Medhat, Attacks on individuals and Internet, Dar Al-Nahda, Cairo, 2004.
- STEIN, Schjorberg (2009): A Global Protocol on Cybersecurity and Cybercrime, 4th Edition. Available online at: stein.schjolberg@cybercrimelaw.net
- WERY E., Sexe en ligne : aspects juridiques et protection des mineurs, Paris, LGDJ, Coll. Droit des technologies, 2004

6.6. Les notes, articles scientifiques et de presse

- AHWANY, H., Protection of intellectual property rights on the Internet (in Arabic), available at the following address: www.arablawinfo.com [Accessed 24 August 2009].
- AVGOULEA M, Bouras C et al., Policies for content filtering in educational networks: the case in Greece. Telematics and Informatics 20 (2003) 71 -95
- AYOADE J.O., Kosuge T., Breakthrough in privacy concerns and lawful access conflicts. Telematics and informatics 19(2002) 273 - 289
- (article anonyme) « Des jeunes exposés à la cybercriminalité » *in* htt://www.cameroon-online.com/actualite, actu-10198.html (consulté le 31 août 2009)
- BOURGEOIS, note sous Paris, 30 octobre 2002, LPA n° 104, 26 mai 2003, p. 12 ;
- BRENNER, S. 'Cybercrime Investigation And Prosecution : The Role Of Penal And Procedural Law', Murdoch University Electronic Journal Of Law (2001), http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82_text.html
- CAPITAL R. (2008) "Kenya Airways website hacked," available at < http://ribacapital.com/2008/01/24/kenya-airways-website-hacked/> accessed December 22, 2010.
- CARON, note sous Trib. Correctionnel de Vannes, 29 avril 2004, CEE 2004, comm ;
- CHOVES LOH : « Cybercrime :Police Boss to fight it out », in Cameroon-Tribune n° 9437/5638 du 18 septembre 2009, p. 14
- CHOPIN F., Cybercriminalité, Rep. pénal Dalloz ;
- CHIK, Warren B. "The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on the Internet : A Comparative Case Study of

Hong Kong and Singapore - Two Differing Asian Approaches" 2006; (14) International Journal of Law and Information Technology 47-100.

- CISSE A., « Quel cadre juridique pour le Sénégal ? Éléments de synthèse », Séminaire sur *le cadre juridique des technologies de l'information et de la communication au Sénégal*, DAKAR 29-30 août 2005. In http://www.adie.sn/docs/ADIE.pdf
- « Les déterminants juridiques à la promotion des technologies de l'information et de la communication (TIC) au Sénégal : enjeux, perspectives et méthodologie », *Revue trim. d'inf. sur les télécom., la régulation et la recherche de l'ARTP*, Oct.-déc. 2006, p.17 et suivants.
- Cybercriminalité : l'Etat prévoit une batterie de mesures : http://www.mediaf.org /fr/thèmes/fiche.php?itm=3300&md=&thm=5
- Cybercriminalité : Nigeria, Sénégal, Côte d'Ivoire, Burkina, Ghana, Bénin, Togo « fichés » par les Indiens: http://start5g.ovh.net/~regultel/spip.php?article635
- DIOUF Ndiaw, « Infractions en relation avec les nouvelles technologies de l'information et procédure pénale: l'inadaptation des réponses nationales face à un phénomène de dimension internationale », in http://www.afrilex.u-bordeaux4.fr/pdf/04doc12diouf.pdf ou Ohadata D-05-15, www.ohada.com.. voir également *Revue de l'Association sénégalaise de droit pénal*, 1997-1998 n° 5-6-7-8.
- DIOUF Ndèye Fatou, « Afrique de l'Ouest : Les pays de la CEDEAO s'engagent à lutter contre la cybercriminalité », samedi 18 octobre 2008 http://start5g.ovh.net/~regultel/spip.php?article867 (le site est devenu, depuis le juin 2009 http://www.itmag.sn/).
- ELALFY, M., Types of cybercrime (in Arabic), available at the following address: http://www.eastlaws.com [Acceded 5 September 2009].
- ELSONBATY, E., Cybercrime; insights from the Egyptian law, June 2007, available at *http://*www.coe.int/.../cybercrime/.../567%20if%20pres%20ehab%20egypt.pdf [Accessed 24 August 2009].
- Legal foundations to combat cybercrime, ITU Regional cyber security forum for Eastern and Southern Africa, August 2008, Lusaka, Zambia, available at www.itu.int/.../**elsonbaty**-legislation-enforcement-lusaka-aug-08.pdf *[*Accessed 29 August 2009*]*.
- FILLION, Droit pénal et innovations technologiques, RSC 1990, 270
- GHAFRY, H., The role of Internet in software piracy (in Arabic), available at the following address: http://www.eastlaws.com [Acceded 5 September 2009].
- E-commerce crimes (in Arabic), available at the following address: http://www.eastlaws.com [Acceded 5 September 2009].
- HEGAZY, M., Intellectual property in digital environment, available at the website of the Egyptian Centre for Intellectual Property and Information Technology (ECIPIT) at the following address: www.ecipit.org.eg/Arabic/pdf/Research_2.pdf [Acceded 25 August 2009].
- JEANDIDIER, Fraude et cartes magnétiques , JCP 1986, I, 3229 ;

- KALINA L., « Lutte contre la cybercriminalité : vers la construction d'un modèle juridique normalisé », actes du Séminaire ADIE-Coopération française *Informatique et libertés, quel cadre juridique pour le Sénégal ?*, page 11, disponible sur http/www.adie.sn
- KATYAL Neal Kumar " Criminal Law in Cyberspace" Working Paper No. 249030 Georgetown University Law Center, 2000 Working paper series in Business, Economics and Regulatory Policies and Public Law and Legal Theory
- LAMY, Observations sous crim. 19 mai 2004, D. 2004, somm. 2749 ;
- LEGROS B., note sous Trib. Correctionnel de Pantoise, 2 février 2005, D. 2005, 1435 ;
- Le Sénégal sécurisé l'activité électronique par | SUD QUOTIDIEN , vendredi 16 mai 2008 | 1360 Lectures
- Le Sénégal en lutte contre la cybercriminalité : http://www.afrik.com /article8361.html
- LIEVENS E., Protecting children in the new media environment: Rising to the regulatory challenge? Telematics and Informatics 24 (2007) 315 – 330
- LONGE, O.B 'Cyber Crime And Criminality In NIGERIA – What Roles Are Internet Access Points Playing ?' European Journal Of Social Sciences – Volume 6, Number 4 (2008)
- MAKOKHA K., (2010) "The Dynamics and Politics of Media in Kenya: The Role and Impact of Mainstream Media in the 2007 General Elections" in Dr Karuti Kanyinga and Duncan Okello (eds) *Tensions and Reversals in Democratic Transitions: The Kenya 2007 General Elections,* Institute of Development Studies (IDS), University of Nairobi, and the Society for International Development (SID) Eastern & Central Africa, Nairobi (launched 26.7.2010).
- MARAQA, Z., The conflicts between trademark and domain names in Arab countries, The electronic transactions conference, Dubai, 2009, available at the following address:http//:www.slconf.uaeu.ac.ae/papers/PDF%201%20English/e10.pdf [Accessed 24 August 2009].
- MATIA (J.R). « Cameroun : Internet-le nouvel filon des criminels », in AllAfrica.com (consulté le 31 août 2009) ;
- MBAYE A., « Informatique et libertés : vers la fin du non droit » (Source : Le Journal de l'économie, N° 479-480, 21 septembre 2005), www.osiris .sn, édité le dimanche 25 septembre 2005.
- MOHI, A., Cybercrimes in Egypt, Study prepared by the cybercrime combat department at the general administration of information and documentation, Egyptian Ministry of Interior, available at http://www.ituarabic.org/coe/2006/E-Crime/.../Doc9-Egy.PPT [Acceded 25 August 2009].
- NGOMBULU Ya SANGUI Ya MINA Bantu Lascony : « Cameroun : l'amour ou la mort : rendez-vous au cyber-café » in Cameroun Tic et Developpement.net, Vendredi 28 août 2009
- NYABIAGE J. (2010) "Kenya: Internet Hackers Attack Treasury" *Daily Nation*, November 8, 2010.
- OLOWUN, D., 'Cybercrimes and the boundaries of domestic legal responses: case for an inclusionary framework for Africa', 2009(1) Journal of Information, Law & Technology (JILT), available at http://go.warwick.ac.uk/jilt/2009_1/olowu [Acceded 10 September 2009].
- PADOVA Y., Un aperçu de la lutte contre la cybercriminalité en France, RSC 2002, 765 s.

- REITZ John, How to Do Comparative Law, (1998) 46 (4).The American Journal of Comparative Law 617.
- SIHANYA B. (1995) "Regulating and Transferring Telecommunications Technology in Kenya: Corporate Responses to Development Challenges".
- SIHANYA B. with OTIENO-ODEK J., "Regulating and Mainstreaming ICT in Kenya for socio-economic and cultural development," in Dr George Outa, Eric Aligula, Florence Etta (eds) *Mainstreaming ICT in Kenya: Research Perspectives from Kenya,* IDRC and Mvule Africa (peer reviewed).
- SIMPSON J., The Impact of the Internet in Banking: observations and evidence from developed and emerging markets. Telematics and Informatics 19(2002) 315 -330
- SMITH, R. G., Holmes, M. N. & Kaufmann, P. (1999): Nigerian Advance Fee Fraud., Trends and Issues in Crime and Criminal Justice, No. 121, Australian Institute of Criminology, Canberra (republished in The Reformer February 2000, pp. 17-19).
- SYLVESTER, Linn (2001): The Importance of Victimology in Criminal Profiling. Available online at: http://isuisse.ifrance.com/emmaf/base/impvic.html
- THIOBANE M., « Le paradis pénal du cyberspace » (mercredi 2 novembre 2005) http://www.osiris.sn/article2085.html
- THOMAS G. (2010) "WikiLeaks Disclosure Highlights Problems of Sharing Secret Information Within US Government" *Voice of America* November 30, 2010
- WALL, D.S., " Policing Cybercrimes: Situation the Public Police in Networks of Security within Cyberspace", Police Practice and Research, 8:2, 183- 205
- " The internet as a Conduit for Criminals," pp77-98 in Pattavina A.(ed) Information Technology and the Criminal Justice System, Thousand Oaks, Sage

6.7. Thèses, Mémoires de 3ème cycle universitaires

- MALONGA YOUNAS J-P, La répression des agissements liés aux nouvelles technologies de l'information : l'exemple du Congo, Thèse, Dakar 2003
- REVERDY P. M., La matière pénale à L'épreuve des nouvelles technologies, Thèse, Toulouse I, 2005.
- EL CHAER N., La criminalité Informatique devant la justice pénale, Thèse, Poitiers, 2003.
- CASILE F., Le code pénal à l'épreuve de la délinquance Informatique, Thèse, Aix-Marseille, 2002.
- KABORE Anatole, La problématique des perquisitions et saisies en ligne en Afrique de l'Ouest : état des lieux et perspectives: Cas du Burkina Faso, du Mali, du Sénégal et du Togo, mémoire de Diplôme d'Etudes Supérieures Spécialisées en «D*roit du Cyberespace Africain*», *Université Gaston Berger de Saint-Louis (Sénégal), UFR de Sciences Juridique et Politique*, *Année Académique 2006- 2007.*
- LEBEYA, Seswantsho Godfrey, "Organised crime in the South African Development Community With Specific reference to Motor Vehicle Theft" LLM Thesis University of South Africa, November 2007
- MAAT. Sandra Mariana. "Cyber Crime A comparative Law Analysis". LLM Thesis University of South Africa, November 2004

- SEUNA Chr., *L'informatique et la nouvelle loi camerounaise sur le droit d'auteur et les droits voisins*, Thèse de doctorat, Université de Yaoundé II, 2005 ;
- TOURE Pape Assane, Le traitement de la cybercriminalité devant le juge sénégalais, mémoire de D.E.A. Droit économique et des affaires 2004, université Gaston Berger de Saint-Louis.
- YAMEN TCHENDJO, *La régulation des télécommunications à l'ère de la convergence*, Mémoire de Master en Droit du cyberespace africain, Université Gaston Berger, 2006-2007.

6.8. Manuels et documents stratégiques

- Manuel pour la prévention et la répression de la criminalité informatique.
- Revue internationale de politique pénale, No. 43 et 44. Nation Unies .1994. (Publication des Nations Unies, numéro de vente: F.94.IV.5).
- Guide des Bonnes Pratiques en matière de Sécurité Economique publication.2007
- http://www.e-alsace.net/documents/fck/file/documents_pdf/Guide_IE12-09-2007[1].pdf) www.e-alsace.net/index.php/headnews/get
- Guide des Bonnes Pratiques en matière d'Intelligence Economique novembre 2008/ Préfecture de la région franche –comté préfecture du Doubs/France
- (www.veille.ma/+Dossier-special-Veille-Magazine+.htm; intel.ecobesancon@interieur.gouv.fr) (http://www.veille.ma/IMG/pdf/guide-des-bonnes-pratiques-en-matiere-intelligence-economique.pdf)

6.9. Les références électroniques

- l'Afrique de l'Ouest se mobilise contre la cybercriminalité, Radio France Internationale: article publié le 18/11/2008 sur http://www.rfi.fr/actufr/articles /107/article 75002.asp
- La cybercriminalité influe négativement sur l'économie de l'Afrique de l'Ouest : http://www.afriqueavenir.org/2009/06/08/la-cybercriminalite-influe-negativement-sur-leconomie-de-lafrique-de-louest-selon-un-officiel-beninois/
- Conférence régionale africaine sur la cybercriminalité :http://www.afcybersec.org/ rapports/afcybersec_08_yakro_ci_1227176170.pdf
- Cybercriminalité : quels outils pour l'Afrique ? : http://www.blogg.org/blog-35519-billet-cybercriminalite___quels_outils_pour_l_afrique__-277980.html
- Cybercriminalité : vers la mise en place d'une stratégie commune de... http://blesshnet.com/heberg/laraignee/lesw2/modules.php?name=News&file=article&sid=3331
- Les cybercriminels désormais sous le coup de la loi: / http://www.marches-tropicaux.com/Article.asp?art_id=8616
- Les enjeux éthiques de la mondialisation de la communication: l'exemple de l'Afrique de l'Ouest: http://www.er.uqam.ca/nobel/gricis/actes/bogues/Brunet.pdf
- Atelier de l'Afrique de l'Ouest sur les Cadres Politiques et Réglementaires pour la Cybersécurité et la Protection de l'Infrastructure de l'Information Critique: http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/gueye-senegal-perspective-praia-nov-07.pdf

- National Cybersecurirty strategies: case study -Nigeria: www.afcybersec.org/.../ afcybersec_08_yakro_ci_1227101590.pdf
- La cybersécurité: les moyens juridiques de protection :http://www.afcybersec.org/ rapports/afcybersec_08_yakro_ci_1227109593.pdf
- Site de la BCEAO. www.bceao.int sur le blanchiment de capitaux (Instruction n° 01/2006/SP du 31 juillet 2006, Directive N° 07/2002/CM/UEMOA)

6.10. Les sites internet

- http://www.osiris.sn/article2599.html
- Ouestaf News/http://start5g.ovh.net/~regultel/spip.php?article 635
- http://www.xibar.net/CYBERCRIMINALITE-Un-emigre-senegalais-vivant-aux-Usa-en-fait-les-frais_a15638.html.
- http://www.interpol.int/ Public/News/2008 /DAKARsenegalFR.asp7 août 2008
- http://www.osiris.sn/article4699.html
- http://www.echosdunet.net/recommande/breve_4434_premiere+plainte+pour+telechargement+illegal+senegal.html
- http://www.osiris.sn/article2924.html
- http://www.big-presse.com/big-article-Afrique-10493.php (Publié le 16/7/2009)
- http://www.osiris.sn/article556.html
- http://www.osiris.sn/ article4257.html
- http://www.osiris.sn/article2941.html
- http://www.afcybersec.org/rapports/ afcybersec08_yakro_ci_1227172073.pdf
- http://www.lesafriques.com/ medias-reflexion/la-cybercriminalite-en-pleine-expansion-en-afrique-4.html?Itemid= 308?articleid=5067
- http://ccurdc.societeg.com/rapportfinalcybercrimeafrica06.pdf
- http://www.afrik.com/ article15706.html
- http://www.afcybersec.org/ rapports/afcybersec_08_yakro_ci_1227103294.pdf
- http:// www.cipaco.org/spip.php?article1755&lang=en
- http://www.big-presse.com/big-article-Afrique-10493.php (Publié le 16/7/2009)
- http://www.rfi.fr/actufr/ articles/107/article_75002.asp
- www.osiris .sn, édité le dimanche 25 septembre 2005
- http://www.osiris.sn/article2085.html
- http://start5g.ovh.net/~regultel/spip.php?article867 (le site est devenu, depuis le juin 2009 http://www.itmag.sn/).
- http://www.afriklive.com/ L-Afrique-de-l-Ouest-se-mobilise-contre-la-cybercriminalite_a3923.html
- http://www.mali-ntic.com/article.php3?id_article=356

Sur les différentes approches de traitement du phénomène de cybercriminalité

- Site Web: www.itu.int/ITU-D/cyb
- Site : www.coe.int

- Site web: www.itu.int/itudoc/itu-t/86435.html: Security in telecommunications and information technology: an overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunication. ITUT; October 2004.
- Site www.forumInternet.org/: Espace d'information et de débat sur le droit de et sur l'Internet et des réseaux
- Site de la Commission nationale de l'informatique et des libertés (France): www.cnil.fr

- Site de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (France): www.interieur.gouv.fr/rubriques /c/c3_police_nationale/c3312_oclctic
- Observatoire de la sécurité des systèmes d'information et des réseaux: www.ossir.org
- Site du Clusif: www.clusif.asso.fr. Panorama de la cybercriminalité : www.clusif.asso.fr/fr/production/ouvrages/
- Site du National Institute of Standards and Technology (NIST) aux Etats- Unis: www.nist.gov
- Site de la National Security Agency aux Etats-UnisNSA: www.nsa.gov;
- Site du BSI: www.bsi.bund.de. Le BSI est l'Office Fédéral de la Sécurité de l'Information en Allemagne. Ce site est en anglais et allemand
- Site du DSD: www.dsd.gov.au; site du Defence Signals Directorate présente en Australie et Nouvelle Zélande. Ce site est dédié à la veille numérique et la sécurité de l'information.
- Le guide pratique du chef d'entreprise face au risque numérique : risques identifiés et solutions proposées en 10 études de cas / Le Forum International sur la Cybercriminalité .3e version du 24 mars 2009.
- . (http://www.veille.ma/IMG/pdf/risque-numerique-guide-pratique-chef-entreprise.pdf)
- Guide de la Cybersécurité pour les Pays en développement, Union Internationale des Télécommunications. Edition 2007.168 pages
- (www.itu.int/ITU-D/cyb)
- Guide de la Cybersécurité pour les Pays en Voie de Développement. Union Internationale des Télécommunications. 2006. 156 pages (www.itu.int/ITU-D/cyb) http://www.interpol.int/public/icpo/default.asp

6.11. Jurisprudence

Afrique du Sud

- Bernstein and others v Bester and others NNO 1996 (2) SA 751 (CC).
- Charlton v Parliament of the Republic of South Africa (C367/06) [2007] ZALC 47 (11 June 2007).
- City of Cape Town v Ad Outpost (Pty) Ltd and Others 2000 (2) SA 733 (C).
- Cronje v CCMA and Others 2002 9 BLLR 855 LC.
- Dauth v Brown and Weir Cash and Carry 2002 8 BALR 837 CCMA.
- Delonga v Costa 1989 (2) SA 857(A).

- Financial Mail (Pty) Ltd and another v Sage Holdings Ltd and Another 1993 (2) SA 451 (A).
- Government of the Republic of South Africa v Ngubane 1971 (4) SA 367 (T).
- S v Kidson 1999 1 SACR 338 (W).
- S v Makwanyane and Another 1995(3) SA 391 (CC).