UNIVERSITE CHEIKH ANTA DIOP DE DAKAR

REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE

FACULTE DES SCIENCES JURIDIQUES ET POLITIQUES

****

Département de droit privé

Carrières judiciaires

*****

MEMOIRE DE MASTER II RECHERCHE

SUJET : *La répression de la cybercriminalité au Sénégal*

Présenté et soutenu par :

Marthe Andrée Mélanie Badji

Sous la direction du professeur :

Sidy Nar Diagne, Docteur *des facultés de droit, Maitre de conférences à l'université cheikh Anta Diop de Dakar*

Année Universitaire : 2018-2019

UNIVERSITE CHEIKH ANTA DIOP DE DAKAR

REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE

FACULTE DES SCIENCES JURIDIQUES ET POLITIQUES

****

Département de droit privé

Carrières judiciaires

*****

MEMOIRE DE MASTER II RECHERCHE

SUJET : *La répression de la cybercriminalité au Sénégal*

Présenté et soutenu par :

Marthe Andrée Mélanie Badji

Sous la direction du professeur :

Sidy Nar Diagne, docteur *des facultés de droit, Maitre de conférences à l'université cheikh Anta Diop de Dakar*

Année Universitaire : 2018-2019

« L’université n’entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire ; ces opinions doivent être considérées comme propres à leur auteur »

Remerciements

Je tiens à remercier toutes les personnes qui m'ont aidé lors de la réalisation de ce mémoire.

Je voudrais remercier d'abord mon directeur de mémoire le professeur SIDY NAR DIAGNE, pour sa patience, sa disponibilité, et surtout ses conseils qui m'ont beaucoup orienté dans mes recherches.

Je remercie également à l'ensemble des professeurs qui ont participé à ma formation.

Je tiens à dire un grand merci à mes parents qui m'ont montré la voie de l'éducation, par leur aide financier, par leurs conseils inconditionnels, qui m'ont aidé à progresser dans mes études.

Je tiens aussi à remercier toutes les personnes qui m'ont aidé d'une manière ou d'une autre dans la réalisation de ce mémoire :

A mes frères et sœurs, pour leurs conseils, leurs encouragements, qui m'ont beaucoup aidé dans la réalisation de ce mémoire.

Mon époux pour m'avoir accompagné, encouragé, assisté lors de la réalisation de ce mémoire.

A les amis pour m'avoir également aidé à réaliser ce mémoire, car leur présence me donnait le courage de se battre pour aller de l'avant.

Je tiens aussi à remercier ALIOUNE BADARA DIAGNE, pour avoir relu son travail et à François DIOUF, pour m'avoir aidé dans la mise en forme de ce travail.

Dédicaces

A mon époux

A mon fils

A ma mère

A mon père

Liste de sigles et abréviations

AU : Union africaine

ART. : Article

BULL. : Bulletin

CASS. CRIM : Chambre criminelle de la Cour de Cassation

CE : Conseil d'Etas

CEDEAO : Communauté Economique des Etats de l'Afrique de l'Ouest

CGTN : Commission Générale de Terminologie et Néologie.

CHRON : Chronique

CITMC-4 : Conférence de l'union africaine des ministres en charge de la communication et des technologies de l'information.

CJCE : Cours de justice des communautés européennes.

CHRON. : Chronique.

CM : Conseil des Ministres

CP : Code pénal.

CPP : Code de procédure pénale.

CTO : Chief Technology Officer (Directeur de la technologie).

DECL. : Déclaration.

DIR. : Sous la direction.

ENVR. : Ecole à vacation régional

ISO : Organisation international des normalisations.

N.T.I.C : Nouvelles technologies de l'information et de communication.

OCLCTIC : Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

ONU: Organisation des Nations Unies

OQLE: Office québécois de la langue française

OTAN: Organisation du Traité de l'Atlantique Nord.

SEPA: Single Euro Payement Area (l'espace unique de paiement en euro).

TGI: Tribunal de grande instance

TR: Tribunal régional

TGHC: Tribunal régional hors classe

UEMOA : Union économique et monétaire ouest-africaine.

UNODC: Office des Nations Unies contre la Drogue et le Crime.

V: Voir

Sommaire

Introduction

Selon un auteur, « *La communication est au cœur de toute sociabilité* », autrement dit l'homme depuis son existence, cherche à exprimer ses sentiments, ses idées, ses émotions, tout au long de son histoire[1] à travers différentes façons. En effet, un des premiers moyens de communication en Afrique est le bruit. C'est l'exemple du tamtam, qui était pour la société Africaine un moyen de faire passer un message. L'Afrique était dominée par une transmission orale des messages. Puis, on assiste à une évolution des moyens de communication, allant de l'apparition de l'écriture, à la création de supports, l'enseigne, la peinture, l'imprimerie, la presse ; ensuite, viennent le téléphone, le cinéma, la radio, la télévision, etc. Aujourd'hui, les moyens de communication les plus utilisés sont les nouvelles technologies de l'information et de la communication.

« Le terme nouvelles technologies de l'information et de la communication (N.T.I.C) a souvent été utilisé dans la littérature francophone durant des années 1990 et au début des années 2000 pour caractériser certaines technologies dites « nouvelles »[2]. Elles constituent aujourd'hui un des moyens indispensables pour le développement d'un pays. Selon le Grand dictionnaire terminologique de l'Office Québécois de la Langue Française (l'O.Q.L.F), les technologies de l'information et de la communication(T.I.C) sont *« l'ensemble des technologies issues de la convergence de l'information et de la communication, qui ont permis l'émergence de moyens de télécommunication plus efficaces en améliorant le traitement, la mise en mémoire, la diffusion et l'échange de l'information* ». Parmi ces TIC, nous pouvons citer l'internet.

En effet, l'internet est « *une technologie de l'information et de communication qui a commencé à être utilisée dans les entreprises, les administrations et les ménages vers la fin du XX° siècle* »[3]. Il peut être définie comme un réseau de communication international qui

[1] JEAN-CLAUDE MOUSSOKI « Les moyens de communication traditionnels en zones rurale dans l'espace culturel Koogo : cas du département du Pool », Mémoire en vue l'obtention du Diplôme d'Etudes Approfondies (D.E.A), année 2003-2004, p.1. https://www.memoireonline.com. Consultée de 5/1O/2019à 10heures

[2] Technologies de l'information et de la communication, https://fr.m.wikipedia.org. Consultée le 5/10/2019 à 11h 30.

[3] L'Internet et la démocratie numérique- Cybercriminalité, ordre public économique et déstabilisation de l'Etat, https://books.penedition.org consulté le 06/08/2019 à 13h12

permettant aux particuliers et aux entreprises de s'échanger entre eux à d'aide d'un ensemble de réseau et d'ordinateurs[4].

Pourtant, ces innovations issues de l'apparition des TIC, ont favorisé l'existence de nouvelles formes de délinquances ou de criminalités commises à l'aide d'internet, qui peuvent porter atteintes aussi bien les personnes physiques que morales. Selon le doyen CARBONNIER « *l'évolution des mœurs et des techniques donne naissance à de nouvelles formes de délinquance* »[5].C'est également dans ce sens que Monsieur Abama Ouane affirme que « *les infrastructures et services du numérique ainsi que les caractéristiques d'Internet, favorisent l'expression de la criminalité et étendent les possibilités et les opportunités criminelles* »[6]. Le développement des NTIC a mené à l'apparition de nouveaux types de délinquance, souvent dénommées sous le nom de la cybercriminalité.

Vu qu'il s'agit d'une forme de délinquances dépendant des TIC, nous ne pouvons pas rester sans savoir que le Sénégal, fait partie des pays où les citoyens utilisent de plus en plus l'internet, pour s'informer ou dans le cadre de leurs activités professionnelles. Et par conséquence se voit victime de cette forme de délinquance qui se développe avec considération dans le pays. Les internautes sont dans une insécurité totale du fait qu'ils risquent d'être victime d'attaques portant atteintes à leurs biens, leur honneur ou à leur sécurité.

L'insécurité les citoyens due à l'apparition de la cybercriminalité a conduite aux autorités publiques à prendre des mesures visant à contrecarrer ces actes illicites. L'engagement pris par les autorités publiques dans le but de se protéger et de protéger ses citoyens contre la cybercriminalité, nécessite de s'interroger sur la répression de la cybercriminalité au Sénégal.

La répression s'analyse comme l'action de sanctionner, de prendre des mesures punitives contre ceux qui violent, autrement dit ne respectent pas, aux lois ou aux options d'un gouvernement, d'une société ou à la morale[7].

Quant à la cybercriminalité, « *ce terme a été inventé à la fin des années quatre-vingt-dix, lorsque l'Internet se répandait en Amérique du Nord* »[8]. Il n'existe pas une définition

[4] L'Internet ?Definition, Histoire et Application, https://wikimemoires.net. Consultée le 12/10/2019 à 10h20.
[5] JEAN CARBONNIER, « *Sociologie juridique* », Paris, Presses Universitaires de France, 1978, p.401.
[6] ADAMA OUANE « Guide pratique de la cybersécurité et de la cyberdefense, (Grand-Bassam, Cote d'Ivoire, 8-10 février 2016, p. 9. https://www.francophonie.org, consulté le 06/08/2019, à 15h07
[7] Définition de répression, https://www.cnrtl.fr. consulté le 28/10/2019 à 19h33.
[8] STEPHANIE PERRIN, Cybercriminalité, https : //vecam.org, consultée le 12/09/2019 à15h17.

universelle de la cybercriminalité. Par conséquence, on assiste à une multitude de définition de cette notion. Ainsi, selon M. Ali Azzouzi « *ce terme est généralement utilisé pour décrire l'activité criminelle dans laquelle le système ou le réseau informatique est une partie essentielle du crime, il est souvent employé pour désigner les activités criminelles traditionnelles dans lesquelles les ordinateurs ou les réseaux sont utilisés pour réaliser une activité illicite* « [9] Cette définition englobe aussi bien les infractions spécifiques aux TIC et les infractions traditionnelles commises par l'utilisation des TIC. De même Monsieur Mohamed Chawki définie la cybercriminalité comme étant *« une toute activité illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite* »[10]. Cette définition peut s'ajouter à celle du Ministre de l'Intérieur français et plus l'OCLCTIC, qui définit la cybercriminalité comme *« ensemble des infractions pénales susceptible de se commettre sur les réseaux de télécommunication en général et plus particulièrement sur les partageant le protocole TIC-IP, appelés communément l'Internet* »[11]. En sus, l'ONU, définit cette délinquance comme « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent* » et dans une acception plus large *« toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique ou contre un système ou un réseau informatique* »[12].

Le législateur Sénégalais n'est pas indifférent au souci de trouver une définition adéquate à cette activité illicite. Ainsi, la loi n°2008-11 portant sur la cybercriminalité dispose que « la criminalité informatique concerne toute infraction qui implique l'utilisation des technologies de l'information et de la communication. A cet égard, les notions de cybercriminalité, de criminalité informatique, de cybercriminelle, ou technologies etc. ont la même signification »[13]. Toutes ces définitions ci-dessus montrent qu'il n'existe pas de définition homogène de la cybercriminalité valable dans toutes les législations. Cette absence l'homogénéité dans la définition de la cybercriminalité ne fait pas pour autant obstacle à la

[9] ALI AZZOUZI, « La cybercriminalité au Maroc », Préface de MOUHAMED CHAWKI, 2010, p.17
[10] MOUHAMED CHAWKI, Essai sur la notion de cybercriminalité, IEHEI, juillet 2006, p.23.
[11] Le Ministre de L'Intérieur français. Disponible sur http://www.interieur.gouv.fr/, consultée le 12/09/2019 à 15h 16.
[12] Dixième Congrès des Nation Unies pour « La prévention du crime et le traitement des délinquants », Vienne, 10-17 avril 2000.p. 4.
[13] La loi n°2008-11 du 25 janvier 2008 portant sur la Cybercriminalité

répression des comportements jugés comme étant dangereux pour le bien-être des citoyens et la sécurité des Etats.

Par ailleurs, l'utilisation de l'Internet constitue un avantage considérable pour les entreprises, les sociétés et même les citoyens. Il joue un rôle majeur dans la compétitivité des entreprises et facilite également de nouvelles organisations et de nouvelles pratiques professionnelles dans la mesure où il permet le renforcement de la flexibilité, l'augmentation de la productivité, l'amélioration de la valeur produite, ou encore le développement de la capacité d'innovation, et dans l'efficacité des administrations et des services publics tels que, santé, éducation, sécurité. Elle constitue aussi un mode de sociabilité dans la mesure où elle aide les jeunes à sortir de l'isolation, à l'aide des forums ou des réseaux sociaux par la création de nouvelles relations avec des personnes représentant les même centre d'intérêt quel que soit leurs positions géographiques[14].

En effet, la grande majorité des citoyens des différentes pays utilisent l'internet pour accéder à l'information et cela rend plus efficace leurs conditions de travail. L'utilisation d'internet comme moyen de communiquer et de s'informer, de travailler, ou de s'épanouir s'accroit de plus en plus partout dans le monde avec l'avènement de la mondialisation et l'apparition de certaines applications comme Facebook, Twitter, Google, You Tube, Whatsapp etc. Beaucoup de personnes ont accès plus rapidement aux informations qui leurs permettent de savoir ce qui se passe dans plusieurs pays du monde.

De même, de nos jours, l'internet est devenu un moyen de faire le commerce. En effet, de nombreux commerçants l'utilisent pour faire la publicité de leurs produits voire même la vente sur internet. Toutefois, il est à noter que la présence de l'internet dans, les activités professionnelles et oisives a favorisé l'extension de la cybercriminalité, au point qu'il est nécessaire de prendre des mesures destinées à mettre fin à ce phénomène.

En effet, la protection les citoyens contre les actes cybercriminels est une obligation qui pesé sur les autorités publiques car « *les pouvoirs publics, avant l'apparition de l'Internet avaient le devoir de garantir la protection traditionnelle des droits et libertés fondamentaux, avec l'apparition de l'Internet, l'on observe une transposition des infractions classiques dans le monde numérique, et l'apparition de nouvelles formes d'infraction à travers l'utilisation de*

[14] LAURIANE MPOUKI « Avantages et inconvénient d'internet chez les jeune », bantuhub.com. 12/10/2019 à 10h54.

ces TIC. Les pouvoirs publics, dans ces conditions, ont toujours cet impérieux devoirs de protection des droits et libertés fondamentaux au risque de se voir paralyser »[15].

La cybercriminalité peut revêtir plusieurs formes. Il s'agit entre autre : du phreaking. C'est « *le piratage de système de téléphone filaire ou sans fils* »[16]. Il consiste le plus souvent à « *mettre en place des moyens pour contourner la facturation des usages téléphoniques ou à établir les communications anonymes ou encore à écouter des conversations téléphonique*s »[17]. Le phreaking peut être analysé comme « *un maintien dans un système automatisé de données* »[18] ou à une interception de données informatiques. Il y a aussi le hacking, qui regroupe un ensemble de techniques exploitant des failles et vulnérabilités d'un élément ou d'un groupe d'éléments d'un système d'information. Il peut avoir pour conséquence, « *le maintien frauduleux dans tout ou partie d'un système de traitement automatisé, entraver ou fausser le fonctionnement d'un système de traitement automatisé* »[19]. Il y a également le cas du spamming, qui consiste en un *«envoi d'un même message électronique non sollicité à un très grand nombre de destinataire au risque de les importuner* »[20]. Il consiste à saturer un serveur de mail par le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données[21]. Le spamming peut être réalisé par courriel[22], par SMS[23], ou par vocal[24]. Par ailleurs, il y a ce que l'on appelle le phishing ou hameçonnage, « *c'est une technique de fraude visant à obtenir des informations confidentielles, telles que des mots de passe ou des numéros de cartes de crédit, au moyen de message ou de sites usurpant l'identité d'institutions financières ou d'entreprises*

[15] L'Internet et la démocratie numérique-Cybercriminalité, ordre public économique et déstabilisation de l'Etat, *op. cit.*

[16] EMMANUELLE MATINGON, « La cybercriminalité : un focus dans le monde des télécoms, mémoire en vue de l'obtention du Diplôme d'Etude Approfondies, 2011-2012, p24.

[17] Par exemple de fait de se brancher sur la ligne téléphonique d'un tiers afin de passer, au moyen de sa ligne téléphonique, des communications à l'insu de celui-ci et lui faire supporter le cout de ces communications. Exemple cité par EMMANUELLE MATIGNON, ibidem.

[18] *Ibidem.*

[19] *Ibid* .p. 25.

[20] Commission Générale de Terminologie et de Néologie (CGTN) : JO 12 septembre 2000.

[21] EMMANUELLE MATIGNON, op. cit. p. 27.

[22] C'est l'envoie en masse des e-mails publicitaires non sollicités cité par MADAME EMMANUELLE MATIGNON, *Ibidem.*

[23] L'envoie d'un SMS non-sollicité qui invite à appeler un numéro surtaxe ou à renvoyer un SMS surtaxé. *Ibidem*.

[24] *Ibidem*.

commerciales[25] *connues et réputées* »[26]. Sur ce type d'infraction nous pouvons citer l'exemple de la fraude à la carte bancaire

La cybercriminalité ne se limite pas uniquement aux préjudices causés à un système informatique ou à système automatisé de données, elle peut aussi être un moyen facilitant la commission d'infractions traditionnels telles que le vol, d'escroquerie, le terrorisme, etc. En somme, nous pouvons noter que la cybercriminalité englobe les infractions telles que : les atteintes aux systèmes informatiques, les atteintes aux traitements automatisé de données, les violations de données personnelles, les atteintes liées à la diffusion de contenus illicites, la contrefaçon de marques d'œuvres et de logiciels aussi que les infractions de droit commun commises via l'utilisation des TIC.

En sus de cela, les cybercriminels peuvent avoir plusieurs motivations telles que : la curiosité intellectuelles *« la soif de la connaissance et le désir d'explorer de nouvelles compétences sont à l'origine de l'apparition du phénomène de hacking* »[27], l'ego, l'idéologie et d'argent. Aujourd'hui la cybercriminalité est beaucoup plus orientée vers la recherche de d'argent que d'une simple curiosité, d'ego ou d'idéologie. C'est dans cette ordre d'idée que Monsieur ALI AZZOUZI affirme que « *la cybercriminalité est devenue au fil des temps une activité extrêmement profitable. Des sommes importantes ont été détournées avec succès* »[28].

Cette nouvelle forme de délinquance est caractérisée par sa dangerosité considérables au point que, M. Romain Boss déclare que *« la cybercriminalité est l'une des formes de criminalité ou de délinquance les plus dangereuses et les plus fréquentes qui se réalisent par l'utilisation de l'internet* ». En effet, « *Elle constitue une les formes de délinquance qui connait actuellement la croissance la plus forte. Et de plus en plus de malfaiteurs exploitent la rapidité, fonctionnalité des technologies modernes, ainsi que l'anonymat qu'elles permettent, pour commettre des infractions sur le réseau Internet* »[29]. C'est une nouvelle forme des criminalités ou de délinquance sur les réseaux Internet, dont les conséquences se révèlent particulièrement graves pour la sécurité humaine. La dangerosité de ce phénomène est due à son caractère mondial d'une part et d'autre part à d'utilisation des moyens techniques spécifique par les cyber- délinquants, dans la réalisation des infractions, rendant

[25] Définition de la Commission Générale de Terminologie et de Néologie(CGTN) JO 12 février 2006.
[26] EMMUNUELLES MATIGNON, *op.cit*. p. 27.
[27] ALI EL AZZOUZI, *op. cit.* , p.91.
[28] *ibid*. P. 18.
[29]ROMAIN BOSS « La lutte contre la cybercriminalité au regard de l'action des Etats », thèse, Université de Lorraine, 2016, p.44.

leur identification plus complexe. Dans le même contexte, Colin Rose estime que *« la cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques et nucléaires »*[30]. Cette phrase illustre le degré de dangerosité que représente la cybercriminalité.

En effet, « *les intrusions dans des systèmes informatiques, les atteintes à la confidentialité, à l'intégrité ou à la disponibilité des systèmes, le vol de données, la prise de contrôle à distance ou le sabotage engendrent des pertes directes ou indirectes pour les entités qui en sont victimes et qui portent atteinte à leur pérennité et compétitivité* »[31]. Et par conséquent, les entreprises ainsi que les personnes physiques méritent une protection de leurs personnes et de leurs biens par les autorités publiques. Conscient du danger que constitue la cybercriminalité, le législateur Sénégalais s'est lancé dans une lutte sans cesse contre ce phénomène.

Ainsi se pose la question de savoir : Quelle est la portée de la répression de la cybercriminalité au Sénégal ?

L'étude de ce sujet s'articulera entour de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité du Sénégal. Il s'agit ici particulièrement d'étudier les dispositions substantielles et procédurales prise par le législateur Sénégalais pour lutter contre la cybercriminalité.

En sus, ce sujet nous permet, d'illustrer l'importance des différentes dispositions prise par les autorités publiques Sénégalais, pour combattre la cybercriminalité dans sa globalité ainsi que les difficultés qui peuvent survenir dans la mise en œuvre de ces derniers. Par ailleurs il faut noter que la fréquence des activités cybercriminelles emport la nécessité de procéder à une sensibilisation des internautes dont certains ignorent encore l'existence ou la dangerosité de cette forme de délinquance et d'aider les victimes de cyber délits d'obtenir, non seulement la réparation de leurs préjudices, mais aussi et surtout la condamnation des auteurs, grâce à la connaissance des différentes sanctions que ces derniers peuvent encourir. L'étude de ce sujet permettra, en outre, de combler ce besoin de sensibilisation dans la mesure où le dispositif de la répression de la cybercriminalité joue un rôle de dissuasion sur toute personne ayant la volonté de se livrer à ces types de délinquance. En effet, les dispositions de lutte contre la cybercriminalité doivent avoir un caractère dissuasif et un caractère préventif. Car à travers ces dispositifs, toute personne serait en mesure de savoir à

[30] COLIN ROSE, cité par MOHAMED CHAWKI dans « Essai sur la notion de cybercriminalité », *op. cit*., p. 2.
[31] ADAMA OUANE, *op. cit*., P.11.

l'avance, les comportements prohibés, par les Autorité publiques et quelles seraient les conséquences en cas de violations de ces interdictions. Cette peur d'être sanctionnées que peuvent ressentir les délinquants, les pousseront à abandonner leurs idées criminelles. En définitive, l'importance de l'étude de ce sujet réside dans le caractère protecteur du dispositif de la répression de la cybercriminalité du Sénégal. Ce qui à pousser au Pr Abdoullah Cissé à affirmer que « *Le traitement de la cybercriminalité participe à la sécurisation du cyberespace par la protection qu'il assure aux ordinateurs, aux systèmes d'informations, aux enfants, aux transactions commerciales et financières numériques sans compter la protection des données à caractère personnel* »[32].

Il est question dans ce sujet de mettre l'accent sur les dispositions prises par le législateur Sénégalais pour lutter contre la cybercriminalité, ainsi que les insuffisances que présentent ces dispositions afin de tentons d'apporter les solutions dans le but de renforcer des dispositions déjà mises en place.

Ainsi, pour mieux appréhender ce sujet nous allons dans un premier temps montrer que la répression de la cybercriminalité au Sénégal se manifeste par une mise en place d' un dispositif de répression de la cybercriminalité (chapitre1) et dans un second temps montrer l'insuffisance du dispositif de la répression de la cybercriminalité ainsi que les solutions à prendre pour plus d'efficacité dans la lutte contre la cybercriminalité. (chapitre2).

[32] ABDOULLAH CISSE « Exploration sur la cybercriminalité et la sécurité en Afrique : Etat des lieux et priorité de recherche » Synthèse des rapports nationaux, 2011, p. 5. https://idl-idrc.dspacedirec.org, consultée le 3/ 9/ 2019 à 10h 08.

Chapitre I : La mise en place d'un dispositif de répression de la cybercriminalité au Sénégal.

Vue le caractère immatériel de la cybercriminalité, le législateur Sénégalais se lance dans une voie d'adaptation du droit substantiel (Section I) et du droit procédural (section II) aux délits cybercriminels.

Section I : L'adaptation du droit substantiel aux cyber- délinquances.

L'adaptation du droit substantiel se manifeste par l'édiction des incriminations et sanctions liées à la cybercriminalité (Paragraphe I) et par la mise en place de la responsabilité des personnes morales en matière de cybercriminalité (Paragraphe II).

Paragraphe I : Les incriminations et sanctions liées à la cybercriminalité.

La cybercriminalité est une nouvelle forme de criminalité qui peut toucher aussi bien les individus, les entreprises que l'Etat. Le législateur Sénégalais à procéder à d'édiction de certain incriminations et sanctions propres aux TIC(A) et à l'adaptation des infractions traditionnelles aux cyberdelinquances (B).

A. *Les infractions propres aux Technologies de l'Information et de la Communication.*

L'avènement de la cybercriminalité ne reste pas sans conséquences majeures au sein de la société dans la mesure où il fait ressortir certains comportements qui portent atteintes aux intérêts des citoyens et de l'Etat. Face à ces comportements jugés inappropriés, le législateur Sénégalais a vu la nécessité d'édicter des incriminations ainsi que des sanctions spécifiques pour répondre à ces atteintes. L'incrimination peut être définie comme « *une description, par une norme juridique, d'un comportement dont la réalisation fait encourir une peine principale* »[33].

Les infractions spécifiques à la cybercriminalité sont relatives aux atteintes à la confidentialité, à l'intégrité du système informatique, aux données informatisées, aux contenus et, enfin, les infractions liées aux activités des prestataires techniques de services de communication au public par voie électronique.

[33] JACQUES-HENRI ROBERT, *Droit pénal général*, Presses Universitaires de France, 1ere édition, 1988, p. 99.

Les atteintes à la confidentialité : La confidentialité est définie par l'Organisation Internationale de Normalisation (ISO) comme étant « *le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé* »[34]. Ce besoin de protection de l'information peut être atteint à tout moment.

Les atteintes à la confidentialité se manifestent soit par un accès ou par une tentative d'accéder frauduleusement à un système informatique, soit par introduction dans ce système. L'introduction peut être faite dans le but de se procurer personnellement ou pour un tiers un avantage quelconque.

De même constitue une atteinte à la confidentialité, le maintien frauduleux ou la tentative de se maintenir dans un système informatique. Ces délits cités ci-dessus, sont punis d'une peine l'emprisonnement de six mois à 3ans et d'une amende de 1.000.000 à 10.000.0000 de francs.

Concernant les atteintes à l'intégrité des systèmes informatiques, le comportement sanctionné consiste dans le fait d'entraver ou de fausser le fonctionnement du système informatique. Dans cette hypothèse aussi la tentative est prise en compte. La peine prévue est d'un an à 5ans d'emprisonnement et une amende de 5000000 à10.000.000francs.

Pour ce qui est des atteintes à la disponibilité des informations, tout comme les atteintes à la confidentialité, consiste dans l'accès ou la tentative d'accéder frauduleusement ou dans l'introduction ou la tentative d'introduire frauduleusement des données dans un système informatique. Ces atteintes sont punies d'une peine d'emprisonnement d'un an à 5ans et d'une amende de 5.000.000 à 10.000.000. Francs.

A côté de ces atteintes citées ci-dessus, nous pouvons noter les atteintes aux données informatisées

Ces atteintes concernent à la fois les attentes générale aux données informatisées et les atteinte spécifiques aux droits de la personne au regard du traitement des données à caractère personnel.

Les premières catégories notent des comportements tels que, l'interception ; l'endommagement, la modification, l'altération, la détérioration ou l'effacement des données informatisées.

[34] Définition de confidentialité, htrps://fr.m.wikipedia.org. Consultée le 2/07/2019 à 11h27.

En effet, les données informatisées peuvent être atteinte par une interception ou une tentative d'intercepter frauduleusement occasionné par l'utilisation des moyens techniques, des données informatisées lors de leurs transmission non public à destination, en provenance ou à l'intérieur d'un système informatique[35]. Il en est ainsi, de l'endommagement ou la tentative d'endommager, l'effacement ou la tentative d'effacer, l'altération ou la tentative d'altère, la modification ou la tentative de modifier, frauduleusement des données informatiques[36]. De même, la production ou la fabrication de données informatisées, par une introduction, l'effacement ou la suppression de données informatisées stockées, dans l'objectif de les utiliser à des fins légales comme si elles sont originales[37], constitue une atteinte aux données informatisées. Il s'agit-là de sanctionner le comportement de contrefaçon de documents informatisées. Saura également sanctionnée la personne qui, en connaissance de cause, use ou tente d'user ces documents contrefaits[38]. En fin sera puni, toute personne qui par introduction, altération, l'effacement ou suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique, aura obtenu frauduleusement pour soi-même ou pour autrui, un avantage quelconque[39]. Les atteintes générales aux données informatisées sont punies d'une peine d'emprisonnement de 1ans à 5ans et d'une amende de 5.000.000 à 10.000.000 francs.

La seconde catégorie d'atteintes concerne les comportements tels que, le non-respect, même par négligence, des formalités préalables[40] prévues par les lois sur des données à caractère personnel, lors d'un traitement de ces dernières. De même, si la Commission des Données Personnel prononce une sanction envers une personne conformément au point 1 de l'article 30 de la loi sur les données à caractère personnes[41], et si cette personne malgré cette sanction traite ou fait traiter des données à caractère personnel, elle porte atteinte aux données personnelles traitées et par la suite sera sanctionnée. La sanction dont il s'agit ici est souvent

[35] ARTICLE 431-12de la loi sur la cybercriminalité, *op. cit.*
[36] ART. 431-13.
[37] ART. 431-14.
[38] ART. 431-15.
[39] ART. 431-16.
[40] Formalités préalables voir les arts. 18, 19 ,20 et 21 de la loi n°2008-12 du 25juillet 2008, sur la protection des données à caractère personnel.
[41] ART.30, ibid., « Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, la Commission des Données Personnelles peut prononcer à son encontre de, après procédure contradictoire, les sanctions suivante :

1) Un retrait provisoire de l'autorisation accordée pour une durée de trois mois (…) ;
2) Une amende pécuniaire d'un million à cent millions de Franc CFA.

le retrait provisoire de l'autorisation pour une durée limitée (trois mois) ou définitive à l'encontre du Responsable du traitement.

En outre, dans le cadre du traitement des données personnel qui ne sont pas susceptibles de porter atteinte à la vie privée ou aux libertés, dans leur mise en œuvre, la Commission des données Personnel, établit et publie des normes destinées à simplifier ou exonérer l'obligation de déclaration. Ainsi, le non-respect de ces procédures de simplification ou d'exonération dans le traitement de ces données personnelles est passible de sanction pénale.

Les atteintes aux données informatisées, peuvent consister aussi, à un traitement de données personnelles comportant de numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, sans une autorisation préalable de la loi sur les données à caractère personnel.

Le traitement des données personnelles doit se faire dans le respect des mesures prévues à l'article 71 de la loi sur les données à caractère personnel[42] sous peine de sanction. Est également sanctionnée la collecte des données à caractère personnel par les moyens frauduleux, déloyaux ou illicites.

De même est considéré comme une atteinte aux données à caractère personnel, Le fait pour une personne de mettre ou de conserver dans un support ou mémoire informatiques, les données à caractère personnel faisant apparaitre directement ou indirectement l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuse ou les appartenances syndicales ou relatives à la santé ou à l'orientation sexuelle sans le consentement expresse de la personne concernée. Cette hypothèse est également valable pour des données portant sur des infractions, des condamnations ou des mesures de sûreté.

En sus de cela, la conservation les données à caractère personnel doit se faire dans le respect de la durée prévue par l'article 35 de la loi sur les données à caractère personnel[43], sous peine de sanction, à l'exception des données ayant un caractère historique, statistique ou scientifique. Est également considéré comme une atteinte aux donnes à caractère personnel, le détournement de ces données du but prévu par la disposition législative, de l'acte

[42] ART. 71 de la loi sur les données à caractère personnel, *op. cit.* « Le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

[43] Les données doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.

règlementaire ou de la décision de la Commission des Données Personnel, lors de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement.

De même, toute personne qui même par imprudence ou négligence porte à la connaissance d'un tiers, n'ayant pas la qualité de les recevoir, des données à caractère personnel, lors de leur enregistrement, leur classement, leur transmission ou d'une autre forme de traitement[44] est considérée comme ayant fait une atteinte aux données à caractère personnel. De même, le traitement des données à caractère personnel ayant une fin prospective, sans de consentement préalable de la personne concernée, est considéré comme une atteinte aux données à caractère personnel.

En plus, la loi sur la cybercriminalité sanctionne l'entrave fait à la Commission des Données Personnels, soit en empêchant à ses membres ou aux agents chargés d'appliquer la loi, soit en refusant de donner à ces derniers les renseignements ou documents utiles pour accomplir leur mission, soit enfin, en les donnant de fausses informations ou de s'abstenir de présenter le contenu de ces documents ou enregistrements sous une forme directement accessible[45].

La peine applicable pour ces genres d'infractions est d'un an à 7ans d'emprisonnement et d'une amende de 5.000.000 à 10.000.000 francs. Sauf en cas de divulgation par imprudence ou négligence, où la peine prévue est de six mois à 5ans d'emprisonnement et une amende de 300.000 à 5.000.000 francs. Il en est de même de l'entrave à la mission de la CDP. Pour ce derniers cas les peines sont dé six mois à deux ans d'emprisonnement et d'une amende de 200.000 à 1.000.000 francs.

Les atteinte aux données à caractère personnel se manifeste aussi, dans la production, la vente, l'importation, la diffusion , l'offre, la cession ou la mise à disposition d'un équipement, d'un programme informatique, de tout dispositif ou donne établie spécialement adaptée pour commettre une ou plusieurs infraction prévues par les articles 431-8, 431-16 de la loi sur la cybercriminalité. Il en est ainsi, de la production, de la vente, de l'importation, de la diffusion, le l'offre, de la cession ou de la mise à disposition d'un mot de passe, un code d'accès ou des données informatisées similaires dans le but d'accéder à tout ou partie d'un système informatique. Toute personne qui procèdera à de tel agissement sera puni des même peine prévue pour infraction concernées ou à une peine plus grave. De même sera puni des peines prévues pour chaque infraction ou à la peine la plus sévère, toute association ou

[44] ART.431-18 de la loi sur la cybercriminalité, *op. cit*.
[45] ART. 431-31.

entente dans le but de commettre une infraction portant sur une atteinte aux données à caractère personnel.

S'agissant des infractions se rapportant au contenu, nous pouvons citer la pornographie infantile et les infractions telles que le racisme, l'xénophobe, la menace l'insulte etc.

La pornographie infantile vise *« toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicitement ou des images réalistes représentant un mineur se livrant à un comportement sexuelle explicite* »[46]. En plus, sont sanctionnés les comportements relatifs à la production, à l'enregistrement, à l'offre ou à une mise à disposition, à la diffusion, à la transmission d'images ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique[47]. Est aussi sanctionne, la procuration pour soi-même ou pour autrui, le fait d'importer ou de faire importer, d'exporter ou de faire exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique[48]. Cette loi vise également des comportements concernant la possession d'image ou de représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées[49]. De même est sanctionnée ; la personne qui facilitera l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie infantile.

Le législateur Sénégalais en incriminant la pornographie infantile fait référence à la convention européenne sur la cybercriminalité à son article 9, intitulé « Infractions se rapportant à la pornographie enfantine ». Le droit pénal considère le mineur comme toute personne âgée de moine de 18ans. Le mineur est aussi défini par l'article 1 de la convention des Nations unies relative aux droits de l'enfant comme « tout être humain âge de moins de dix-huit ans, sauf si ma majorité est atteinte plus tôt en vertu de la législation qui lui est applicable »[50]. Ces personnes de par leur immaturité nécessitent une protection de la part des Etats contre toute forme d'exploitation sexuelle. Et c'est ce qui justifie l'interdiction de la

[46] Définition de la pornographie infantile par la loi sur la cybercriminalité, *op. cit.*
[47] ART. 431-34.
[48] ART. 431-35
[49] ART. 431-36
[50] Convention des Etats Unies relative aux droits de l'enfant du 20 novembre 1989.

pornographie infantile par le législateur Sénégalais. Ces actes sont punis d'une peine d'emprisonnement de 5ans à 10ans et d'une amende de 5.000.000 à 15.000.000 francs.

A côté de la pornographie infantile, la loi incrimine les comportements de nature raciste ou xénophobe commis par le biais d'un système informatique, ils consistent à « *un téléchargement, une diffusion ou une mise à disposition sous quelque formes que ce soit des écrit ; des messages ; des photos dessin ou toute autre représentation d'idée ou de théories de nature raciste ou xénophobe ». Aussi, le fait l'approuver, de nier intentionnellement ou de justifier des actes de génocide ou le crime contre l'humanité par le biais d'un système informatique* »[51], est constitutif d'infraction. De même, les actes qui servent à menacer une personne de commettre un crime ou un délit en raison de son appartenance à un groupe quelconque sont constitutifs d'infraction. Il peut s'agir des menaces de mort ou n'importe quelle menace pouvant exercer chez une personne la crainte sur sa vie. Selon Frédéric Chopin, « *les menaces peuvent parfois être dirigées contre les biens tout en étant dangereuses pour les personnes* »[52] Les peines prévues sont de six mois à sept ans d'emprisonnement à de 1.000.000 à 10.000.000 francs.

Les activités des prestataires techniques de services de communication au public par voie électronique. Elles englobent à la fois le rôle des intermédiaires techniques tels que les fournisseurs d'accès et les fournisseurs d'hébergement ainsi que le rôle des éditeurs, etc. Les activités exercées par ces derniers peuvent faire l'objet d'une atteinte. Ces atteintes sont sanctionnées par la loi sur la cybercriminalité. En effet cette loi mentionne les comportements tel que : la présentation mensongère faite aux personnes désignées au 2° de l'article 3 de la loi sur les transactions électroniques[53], d'un contenu ou d'une activité comme illicite afin d'en obtenir le retrait ou d'en faire cesser la diffusion, tout en sachant que ces informations sont fausses[54]. Cette présentation mensongère est punie d'une peine d'emprisonnement de six mois à 1an et d'une amende de 200.000 à 1.000.000 francs. De même, l'exercice d'une activité relative aux transactions électroniques obéit à certaines obligations dont la violation est passible de sanction pénale par la loi sur la cybercriminalité. Il s'agit de l'accomplissement les obligations prévues au quatrième alinéa du point 5 de l'article 3 de la loi sur les

[51] ART. 431-38 de la loi sur la cybercriminalité, *op. cit*.

[52] FREDERIQUE COPIN « Cybercriminalité », Répertoire de droit pénal et de procédure, juillet, 2013, p.61.

[53] Il s'agit les personnes physiques ou morales qui assurent, même à titre gratuit, par la mise à disposition au public des biens et services, le stockage de signaux, d'écrit, d'image, de sons ou de messages de toute nature fournis par des destinataires de services.

[54] ART. 443-43 de loi sur la cybercriminalité, *op. cit.*

transactions électroniques[55], de l'obligation de conserver les éléments d'information prévues à l'article 4 alinéa 1 de la loi sur les transactions électroniques[56] et enfin l'obligation s'il en existe de déférer à la demande d'une autorité judiciaire imposant la communication des éléments prévus à l'article précèdent. Ici, c'est le refus par ces personnes de communiquer aux autorités publiques les données qu'ils ont sollicité qui est sanctionné. Ces obligations pèsent sur les personnes physiques ainsi que les dirigeants de droit ou de fait exerçant une activité relative aux transactions électroniques. La violation de l'une de ces obligations est sanctionnée par la loi sur la cybercriminalité d'une peine d'emprisonnement de six mois à 1ans et d'une amende de 100.000 à 500.000 francs. Ces derniers sont également tenus de respecter les prescriptions prévues à l'article 3 et par l'article 5 de la loi sur les transactions électroniques, sous peine respectivement de six mois à 1ans d'emprisonnement et d'une amende de 200.000 à 1.000.000 francs et de six mois à 1an et une amende de 200.000 à2.000.000 francs.

Selon l'article 6 de la loi sur la transaction électronique, « toute personne nommée ou désignée dans un service de communication au public utilisant les technologies de l'internet dispose d'un droit de réponse »[57]. En effet, la demande s'exercice du droit de réponse est adresser au directeur de publicité. La loi sur la cybercriminalité met à la charge du directeur de publicité d'obligation de publier la demande d'exercice du droit de réponse dans les 24heures après la réception sous peines de sanction d'une peine d'emprisonnement de six ans à 1an et d'une amende de 200.000 à 20.000.000 francs . Est également sanctionnée le fait pour un fournisseur électronique de bien ou de service de refuser le remboursement d'un consommateur qui exerce son droit de rétraction, de la même peine citée précédemment. Enfin est sanctionnée d'une peine d'un mois à 1an d'emprisonnement et de 500.000 à 10.000.000 francs d'amende, la personne qui aura trompé l'acheteur sur l'identité, la nature ou l'origine du bien vendu, tout en lui livrant frauduleusement un bien non sollicité.

[55] Loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, quatrième alinéa du point 5 de l'art. 3. « A ce titre, elles doivent mettre en place un dispositif facile accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précèdent qui leur sont signalées et qu'exercent les destinataires de leurs services, et, d'autre part, de rendre public les moyen qu'elles consacrent à la lutte contre ces activités illicites.

[56] Art. 4 alinéa 1, *ibid.* « Les personnes mentionnes aux point 1 et 2 de l'article 3 de la présente loi détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu d'un service de communication au public en ligne ».

[57] ART.. 6, *ibid.*

B. *L'adaptation des infractions traditionnelles aux cyberdelinquances.*

Les infractions classiques commise par l'utilisation des TIC sont : les infractions liées à la publicité par voie électronique, les atteintes aux biens, à la défense national et celle commises par tous moyens de diffusion publique.

Les infractions liées à la publicité par voie électronique. La jurisprudence française définit la publicité comme « tout moyen d'information destiné à permettre à un client potentiel de se faire une opinion sur les résultats qui peuvent être attendus du bien ou du service qui lui est proposés »[58]. En sus, l'article 2 de la loi sur les transactions électroniques définit la communication par voie électronique comme « toute mise à disposition au public ou d'une catégorie de public, par un procédé de communication électronique ou magnétique, de signe, de signaux, d'écrits, d'images, de sons ou de messages de toute nature » Les conditions relatives à la publicité par voie électronique ne sont pas exempts de violation. C'est pour cette raison que la loi sur la cybercriminalité a établi les sanctions relatives à certains agissements. Ainsi, est sanctionnée, la personne qui enfreint les conditions prévues par l'article 15 de la loi sur les transactions électroniques[59] relatives à la possibilité de bénéficier d'offre promotionnelle ainsi que celles de participer à des concours ou jeux proposés par voie numérique. Les conditions dont il s'agit sont, l'exigence de précision et l'accessibilité. De même les publicités ; les offres ; les concours et les jeux promotionnels adressés par courrier électronique, doivent se faire conformément aux conditions prévues par l'article 14 de la loi sur les transactions électroniques[60]. Ces conditions ont sans doute pour but d'éviter les publicités trompeuses ou pratiques commerciales trompeuses qui peuvent enduire en erreur les consommateurs suite à de fausses publicités ou par des publicités imprécises. La peine est de six mois à 2ans d'emprisonnement et une amende de 100.000 à 500.000 francs.

Les atteintes aux biens. Les atteintes aux biens englobes, le vol d'information, l'escroquerie d'information le recel.

---

[58] Cass.Crim, 12novembre 1986, Bull. Crim. n° 335, p.861, https ://www.legifrance.gouv.fr consultée le 29/10/2019 à 13h 06.

[59] ART. 15 de la loi sur les transactions électroniques, *op. cit*. « Les conditions auxquelles sont soumises la possibilité de bénéficier d'offres promotionnelles ainsi que celles de participer à des concours ou à des jeux promotionnels, lorsque ces offres, concours ou jeux sont proposés par voie électronique doivent être clairement précisées et aisément accessibles ».

[60] cet article dispose que « les publicités et les offres promotionnelles telles que les rabais, les primes, ou les cadeaux ainsi que les concours ou les jeux promotionnels, adressés par courrier électronique, doivent pouvoir être identifiés de matière claire et non équivoque sur l'objet du courrier dès leur réception par leur destinataire ou en cas d'impossibilité technique dans le corps du message »

S'agissant du vol d'information. Aux termes de l'article 364 du code pénal Sénégalais *« le vol c'est la soustraction frauduleuse de la chose d'autrui* » L'admission du vol d'information en droit Sénégalais, aussi bien qu'en droit Français, n'est pas évidente. En effet à la question de savoir si une information, bien incorporel pouvait être volée, notamment dans l'hypothèse où une personne prend connaissance d'une information qu'elle utilise ensuite, la jurisprudence française semble avoir répondu par la négative à cette question, ne retenant l'existence d'un vol que lorsqu'il y a vol des originaux au temps nécessaire à leur reproduction.[61] En absence de vol de support l'usurpation d'information ne peut donc être sanctionnée sous la qualification de vol. Mais dans autre arrêt, la jurisprudence française, admet le vol d'information indépendamment de son support[62]. En outre, c'est à travers une loi intégrée dans le code pénal de 1994 que le vol d'information est prévu et réprimé de façon générale par ses articles 323-1 à 323-7. Le droit Sénégalais est également allé dans le même sens en réprimant de vol d'information. L'article 431-53 de la loi sur la cybercriminalité dispose que « la soustraction frauduleuse d'information au préjudice d'autrui est assimilée au vol[63] ». A la lecture de cette disposition nous pouvons déduire que le législateur Sénégalais sanctionne le vol d'information par assimilation au délit le vol classique. Ainsi le législateur a eu recours à ce système de l'assimilation qui marque sa volonté de saisir pénalement l'immatériel.[64]

Concernant les peines applicables, la loi sur la cybercriminalité prévoit une aggravation de la peine lorsque l'infraction a été commise par le biais d'un système informatique. La

[61] Cass. Crim. 8 janvier 1979 : bull. Crim. N° 13 p. 32. ; puis Cass. Crim. 12 janvier 1989 : Bull crim. N¨° 14, p. 38, https//www.legifrance.gouv.fr consultée le 29/10/2019 à13h15 pour le vol de disquettes et de leur contenu informatique le temps nécessaire à leur reproduction.

[62] Chambre criminelle de la cour de cassation, Crim. 1er mars 1989, bull. crim. 1989 n°100 p. 269, https://www.legifrance.gouv.fr, consultée le 29/10/2019, à 13h 16.

[63] TR Thiès, du 18 septembre 2012 affaire de l'Agence New Looks Business, bull. d'information de la cours suprême n°7-8 p. 134 note de PAPA ASSANE TOURE Dans cette affaire le juge condamne un ingénieur informaticien qui charge du service de la clientèle de l'Agence New-Look Business, avait pendant son service, copié dans sa clef USB des données de l'agent relatives aux clients et aux actes de cession. Apres sa cession de travail dans l'agence, il propose aux responsables de l'agent, la remise de la clé USB en échange d'une somme d'argent de 1.500.000 francs CFA. Le juge estime qu'il s'agit d'un vol parce que l'ingénieur informaticien *« a copié des données relatives à l'activité de l'Agence ; à sa clientèle ; à sa patrimoine et ce, à l'insu de son employeur lequel a soutenu, sans être contredit par le prévenu, qu'il avait interdit aux employés de faire des copies des informations allant jusqu'à installer un système de sécurité des activé à chaque fois par celui-ci ».*

[64] PAPA ASSANE TOURE, *Le traitement de la cybercriminalité devant la juge, l'exemple du Sénégal*, l'Harmattan Sénégal 2014, P. 163.

peine sera le double de la peine applicable en matière de vol simple[65]. De même, la loi prévoit l'impossibilité de prononcer un sursis d'exécution des peines prononcées.

Pour de délit d'escroquerie. L'article 379 du code pénal définit l'escroquerie comme « *l'emploi de moyens frauduleux en vue de se faire remettre un bien appartement à autrui* ».Ce délit pour sa constitution nécessite l'utilisation des moyens frauduleux.[66] Cette forme de délinquance est prise en compte par la loi sur la cybercriminalité qui incrimine « quiconque aura reçu des informations personnelles, confidentielles ou celles qui sont protège par le secret professionnel, usant de manœuvres frauduleuses quelconques soit, en faisant, usage de faux noms ou de fausse qualité ».L'escroquerie n'est pas une infraction nouvelle puisqu'ayant déjà été consacrée par le code pénal en son article 379.[67] Cette incrimination sanctionnant les comportements portant sur une chose matérielle se trouvent inadaptées face aux comportements commis par d'utilisation des TIC. Ainsi, pour des soucis de protection du droit de propriété, qui se trouve violé par plusieurs actes sur des réseaux sociaux, le législateur érige certains actes en infraction d'escroquerie[68]. L'escroquerie n'est incriminé que si elle porte sur des « informations personnelles, confidentielles, ou celles qui sont protégées par le secret professionnel »[69].

Le recel d'information. Selon l'article 430 du code pénal « ceux qui sciemment, aurait recelé en tout ou en partie des choses enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit seront punies des même peines prévues par l'article 370 du code pénal[70]. Le

[65] Double des peines prévues à l'alinéa 1 de l'article 379 du code pénal, c'est-à-dire d'une peine d'emprisonnement de 2ans au moins et de 10 ans au plus et d'un amende de 200.000 à 2.OOO.OOO francs.

[66] tels que l'usage qui estime que « quiconque, soit en faisant usage de faux noms ou de fausse qualité, soit en employant des manœuvres frauduleuse quelconques, se sera fait remettre ou délivrer des fonds, des meubles ou aura tenté de se faire remettre ou délivrer des fonds, des meubles ou des obligations, billets, promesses, quittances ou décharges et aura, par un de ces moyens, escroqué ou tenté d'escroquer la totalité ou partie de la fortune d'autrui », usage de faux noms ou de fausse qualité ou des manœuvres frauduleuse qui peut se manifester soit par l'intervention d'un tiers, soit par la production d'une pièce ou d'un document écrit soit par la mise en scène ou ma machination.

[67] qui estime que « quiconque, soit en faisant usage de faux noms ou de fausse qualité, soit en employant des manœuvres frauduleuse quelconques, se sera fait remettre ou délivrer des fonds, des meubles ou aura tenté de se faire remettre ou délivrer des fonds, des meubles ou des obligations, billets, promesses, quittances ou décharges et aura, par un de ces moyens, escroqué ou tenté d'escroquer la totalité ou partie de la fortune d'autrui ».

[68] C'est l'exemple de la décision rendue par de TRHC, Dakar du 29mars 2009 dit, affaire Riad Mouhamed Zayatte, bull. d'information de la cours suprême, n°7-8 p.142 note de PAPA ASSANE TOURE. Dans cette affaire les auteurs avaient utilisé les cardes falsifiées pour opérer des retraits d'argent au guichet automatique du Café de Rome et des paiements pour l'achat de bijoux et de matériels informatiques. Le juge les condamne pour escroquerie au motif qu'ils « ont retiré de l'argent ou se sont paye des biens à partir des cartes frauduleusement acquises ; qu'ils se sont faits remettre des fonds grâce à l'usage de moyens frauduleux ».

[69] ART. 431-56 de la loi sur la cybercriminalité, *op. cit.*

[70]Délit de vol.

receleur étant considère comme étant le complice de l'auteur qui a procuré la chose, il est donc normal que la peine applicable à l'auteur de l'acte délictuel soit la même que celle applicable au receleur. C'est le système de « l'empreinte de criminalité ». La loi sur la cybercriminalité a également sanctionné ce type de comportement. En effet, aux termes de l'article 431-57 du code pénal *« ceux qui auront recelé des informations enlevées, détenues ou obtenues à l'aide d'un crime ou d'un délit, seront punis des peines prévues à l'aide d'un crime ou d'un délit*, »[71].

Les peines applicables en matière d'escroquerie et de recel sont celles prévues par l'article 379 alinéas 1 du code pénal.

Les infractions commises par tous moyens de diffusion publique. Il s'agit plus précisément des infractions de presse. La loi sur la cybercriminalité cite parmi les moyens de diffusion publique : « 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 réunion publics, tout procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique ». Les moyens de diffusion, lorsqu'ils sont utilisés à des fins contraires aux bonnes mœurs, sont sanctionnés par la même loi. L'utilisation de ces moyens de diffusion n'est pas, en soi, une infraction. Ici la loi tente de protéger la dignité humaine et le respect de la personne en interdisant toute diffusion contraire aux bonnes mœurs[72]. Mais la loi s'abstient de déterminer les actes considérés comme contraires aux bonnes mœurs, ce qui peut être source de difficulté dans l'application de cette disposition. Le caractère de bonnes mœurs étant relatif d'un endroit à un autre. L'incrimination de ces comportements se justifie ainsi par le souci de protéger certaines valeurs sociales en relation avec l'honneur, la respectabilité ou la tranquillité des personnes. C'est une façon de réprimer, la diffamation ou des injures publiques, la diffusion de fausse nouvelles commis par l'utilisation des TIC. Les peines prévues sont de six mois à 7ans d'emprisonnement et d'une amande de 500.000 à 10.000.000 francs.

[71] D'après la jurisprudence, le recel peut prendre trois formes : La détention de la chose, la simple réception de la chose, ou en fin le seul fait de tirer profit de la chose. C'est ces différentes formes qui sont sanctionnées par le législateur.

[72] TGHC Dakar, n°2715 du 19 juin 2012, affaires des jeunes filles de Grand Yoff, bull. d'information ce la cours suprême n°7-8, p. 145 note de PAPA ASSANE TOURE. Le juge dans cette affaire estime que « les représentations montrant les jeunes filles se livrant à les agissement sexuellement explicites, impliquant des personnes du même sexe, constituent des images contraires aux bonnes mœurs au sens de l'article 431-59 du code pénal ».

Les atteintes à la défense nationale. L'Etat du fait de son importance et de sa puissance, nécessite une grande protection. Ainsi, sa sécurité et sa stabilité constituent les principales préoccupations des autorités publiques. En effet, vu la dangerosité de la cybercriminalité qui peut même porter atteinte à la stabilité ou la sécurité de l'Etat, certains comportements jugés inappropriés ont été incriminés. Il s'agit d'abord du fait « de livrer à une puissance étrangère ou à ses agents sous quelque forme ou par quelque moyen que ce soit ; de s'assurer, par quelque moyen que ce soit ; de posséder en vue de le livrer à une puissance étrangère ou à ses agents ; de détruire ou laisser détruire en vue de favoriser une puissance étrangère, un renseignement, objet, document, procède données numérisée ou fichier informatisé » La peine prévue est la perpétuité. Ensuite le fait pour une personne, de rassembler des renseignements, des objets, documents, procédés, données ou fichiers informatiques, en ayant conscience que leur réunion ou leur exploitation peut compromettre la défense nationale est un comportement blâmable, il sera punit du maximum des travaux forces à temps. Enfin le « fait pour un gardien ou un dépositaire d'un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui sans intention de trahison ou d'espionnage détruit ; ou laisser détruire ; soustrait ou laisser soustraire ; reproduit ou fait reproduire ; porté ou laisser porter à la connaissance d'une personne non qualifier ou au public alors que ces informations doivent être tenu secret dans l'intérêt de la défense nationale ou que l'accès de ces informations pourrait conduire à la découverte d'un secret de défense nationale » Il sera punit de la détention criminelle de dix à vingt ans. En cas de maladresse ou d'imprudence, d'inattention, de négligence ou d'inobservation des règlements, par le gardien ou le dépositaire, la peine est réduite de la détention criminelle de cinq à dix ans.

L'adaptation du droit pénal à la cybercriminalité, ne se limite pas au seul droit substantiel, elle s'applique aussi au droit procédural.

Paragraphe II : La mise en œuvre de la responsabilité pénale des personnes morales.

En droit, la personne morale est une entité dotée de la personnalité juridique. Cette personnalité juridique permet à la personne morale d'avoir les droits et obligations tels que le droit d'ester en justice, d'avoir les biens, mais aussi des dettes etc. Sur cette base, la personne morale peut voir sa responsabilité engager lorsqu'elle cause un préjudice à autrui. La loi sur la cybercriminalité a prévu les règles visant à sanctionner certains comportements les personnes morales. Ainsi, il convient d'étudier d'abord la responsabilité pénale spécifique

des acteurs de l'Internet (A) et enfin la responsabilité des personnes morales autres que les acteurs de l'internet. (B).

A : Responsabilité spécifique des acteurs de l'Internet.

Les acteurs de l'internet dont il s'agit dans cette partie, sont les intermédiaires techniques tel que les fournisseurs d'accès et les fournisseurs d'hébergement et les éditeurs.

Le fournisseur d'accès est définit comme étant : « *une société qui fournit l'accès à un utilisateur, particulier ou personnes morale, désirant se connecter au réseau internet, ainsi que les moyens matériels et techniques permettant de bénéficier des services s'appuyant sur ce réseau* »[73]. Les fournisseurs d'accès ont pour préoccupation « *d'offrir un accès à des services de communication au public* [74]». Par ailleurs, il faut préciser que les fournisseurs d'accès peuvent cumuler ce service avec d'autres services. En effet, Ils peuvent effectuer divers services comme, les services de connexion, de fax ou de téléphonie par Internet etc. De plus ils peuvent agir simultanément en tant que fournisseurs d'hébergement.

Quant aux fournisseurs d'hébergement ou fournisseurs de services, ils offrent diverses prestations à l'utilisateur, qui va au-delà de la simple mise à disposition de l'accès à Internet. Selon Léon Patrice Sarr, *« l'hébergement consiste à conserver en mémoire des information et à connecter un site à internet. Il définit le fournisseur d'hébergement comme un fournisseur de service de stockage et de gestion de contenus permettant à un fournisseur de contenu de rendre ses pages accessibles au public* »[75]. Ainsi, le point 2 de l'article 3 de la loi sur les transactions électroniques décrit les fournisseurs d'hébergement comme « Les personnes physiques ou morales qui assurent même à titre gratuit, par la mise à disposition au public des biens et services, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services »[76] .

Leur responsabilité peut être engagée. L'engagement de leur responsabilité peut se justifier par le fait que l'auteur de l'infraction n'est pas toujours facile à localiser, et c'est souvent le

[73] LEON PATRICE SARR « La répression de la cybercriminalité en droit Sénégalais à l'épreuve de l'anonymat dans le cyberespace », consulté le 27/ 05/ 2019, à 13h50.
[74] FREDERIC CHOPIN, *op. cit* .p. 112.
[75] LEON PATRICE SARR, *op.cit.*
[76] ART. 3, point 2 de loi sur les transactions électroniques, *op. cit*.

fournisseur qui héberge le site qui se fait poursuivre en premier par le lésé, sur la base d'une responsabilité extracontractuelle. On parle de la responsabilité du fait d'autrui.

Toutefois, il faut signaler qu'en principe, les fournisseurs d'hébergement *« ne peuvent voir leur responsabilité pénale engagée en raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicite ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible* »[77]. Cette exonération de responsabilité est limitée « lorsque le destinataire du service agit sous l'autorité ou le contrôle du fournisseur d'hébergement »[78]. Elle se justifie par le fait qu'aux termes de l'article 3 au point 5, les fournisseurs d'accès et les fournisseurs d'hébergement *« ne sont pas soumises à une obligation générale de surveillance les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicite*s ».[79] Mais ces derniers ainsi que les fournisseurs d'accès peuvent exercés une surveillance ciblée et temporaire à la demande les autorités judiciaires dans le cadre d'une enquête. De même, l'article 4 de la loi sur les transactions électroniques met à la charge des fournisseurs d'accès et d'hébergement l'obligation de collecter et de conserver toute information permettant l'identification de « *quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ».

En plus, pour des besoins de protection des internautes, contre *« l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie infantile* »[80], la loi sur les transactions électronique met à la charge des fournisseurs d'accès et d'hébergeurs, trois types d'obligation, qui ont avant tout pour objectif de lutter contre certaines infractions commis sur internet. Il s'agit entre autres de :

L'obligation de mettre en place un dispositif facilement accessible et visible, une obligation d'information envers les autorités publiques compétentes de toute activité illicite et une obligation de rendre public les moyens qu'elles consacrent à la lutte contre ces activités illicites[81].

---

[77] ART. 3, point 3, de la loi sur les transactions électroniques, *op.cit.*
[78] *Ibid*em
[79] ART. 3, point 5 *ibid.*
[80] *ibidem.*
[81] *Ibidem.*

Par ailleurs, il faut noter qu'en France, les fournisseurs d'accès et les hébergements n'ont pas le même régime juridique. En effet, depuis la loi du 21 juin 2004[82], les fournisseurs d'accès ont bénéficié d'une exonération de leur responsabilité pénale. Ainsi en vertu de l'article L 32 3- 3 du code des postes et communications électronique, « *toute personne assurant une activité de transmission de contenu sur un réseau de communication électroniques ne peut voir sa responsabilité civile ou pénale engager à raison de ces contenus que faisant l'objet de la transmission* ». Cependant, la responsabilité du fournisseur d'accès peut être engagée en cas de manquement aux obligations mis en place par la loi. De même il peut être aussi, condamné au cas où il n'a pas « *accomplie, les diligences normales* » pour faire cesser un contenu illicite.

Tandis que les fournisseurs d'hébergement ont une responsabilité autonome. La loi met à leurs charge « *une présomption de connaissance des faits litigieux par l'hébergeur lorsqu'il reçoit une notification de différents éléments énumérés par la loi, à savoir, la date de la notification, d'identité du notifiant(personne physique ou morale), les noms ou dénomination et domicile ou siège social du destinataire, la description des faits litigieux et localisation précise, les motifs pour lesquels le contenu doit être retiré comprenant la mention des dispositions légales et des justification de faits, la copie de la correspondance adressée à l'auteur ou à l'édition des informations ou activité litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou éditeur n'a pu être contacté* »[83] .

A côté des fournisseurs d'accès et d'hébergement, il y a enfin les fournisseurs de contenu ou éditeur. Ces derniers sont définis par la jurisprudence française comme étant *« la personne qui détermine les contenus qui doivent être mis à la disposition du public sur le service qu'il a créé ou dont il a la charge* »[84]. Ils peuvent également être définis comme « les personnes physiques ou morales qui prennent la responsabilité de mettre à la disposition du public un contenu qu'ils créent et/ou organisent »[85]. De cette définition nous pouvons noter que d'éditeur peut être une personne physique.

Il faut cependant opéré une distinction entre des éditeurs professionnels et les éditeurs non professionnels. Les éditeurs professionnels sont, selon certains auteurs « *les personnes qui*

[82] Loi n°2004-575 du 21 juin 2004 pour la confiance dans d'économie numérique.
[83] FREDERIC CHOPIN,*op. cit.,* p. 120.
[84] TGI, Paris, du 3juin 2008, https://www.legifrance.gouv.fr, consulté le 29/10/2019 à 13h26.
[85] LEON PATRICE SARR, *op. cit.*

éditent sur Internet à des fins professionnelles, soit parce qu'il s'agit de leur activité ou d'une victime de celle-ci »i[86] ce sont des sites d'informations en ligne et « *des sites de marchand ou encore des associations qui éditent sur Internet dans un cadre purement professionnel* »[87].

Les éditeurs professionnels ont une obligation d'identification à l'égard des tiers en mentionnant un certain nombre d'informations sur leurs sites. Mais les conditions d'identifications sont différentes selon qu'il s'agit d'une personne physique ou morale.

La loi sur les transactions électroniques met à la charge des éditeurs une obligation d'identification[88].

Les fournisseurs de contenu, s'ils agissent de manière illicite, répondent du contenu des informations qu'ils mettent sur Internet. La problématique est cependant de localiser la personne responsable, puisqu'il grâce de l'anonymat qui règne dans les réseaux sociaux, il est effectivement facile de se procurer une fausse identité virtuelle ou d'utiliser un serveur situé dans des pays avec lesquels une entraide n'est pas envisageable et rend complexe d'identification de l'auteur de l'infraction.

Enfin le fournisseur de contenus peut aussi facilement et rapidement déplacer son information illicite d'un serveur à un autre et ainsi ralentir ou rendre impossible les poursuites engagées.

---

[86] BENOIT TABAKA, « Le rôle de l'internaute depuis la loi pour la confiance dans l'économie numérique », Legipresse, 2006, p. 2.

[87] CHRISTIANE FERAL-SHUHL, *Le droit à l'épreuve de l'internet*, 7eme édition Dalloz, 2018, p. 551.

[88] ART.5 de la loi sur les transactions électroniques, *op. cit*. dispose que « Les personnes dont d'activité est d'édicter un service de communication au public par le biais des technologies de l'internet mettent à disposition du publique, dans un stand ouvert :

- S'il s'agit de personnes physiques, leur nom, prénom ; domicile et numéro de téléphone, et si elles sont assujettis aux formalités d'inscription au registre du commerce et du crédit mobilier(RCCM), le numéro de leur inscription ;
- S'il s'agit de personnes morales, leur dénomination ou leur raison social et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et du crédit mobilier(RCCM) ou au répertoire national des entreprises et associations, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;
- Le nom du directeur ou du codirecteur de la publication du service de communication au public par voie électronique et, le cas échéant, celui du responsable de la rédaction ;
- Le nom ; la dénomination ou la raison social, d'adresse et le numéro de téléphone du prestataire mentionne au point2 de l'article3 de la présente loi »[88].

[88] *Ibidem*.

Selon un auteur « *Les actes illicites les plus fréquents du créateur de contenus sont les violations du droit d'auteur, dans un cadre purement professionnel* »[89].

A côté des éditeurs professionnels, il y a ce que l'on appelle les éditeurs non professionnel. Les personnes qui éditent à titre non professionnels sont définies par la doctrine comme *« des particuliers qui réalisent un site, sous la seule réserve qu'ils n'agissent pas dans un cadres professionne*l »[90] il peut également s'agir de blogueurs qui dans la majorité des cas, n'exercent pas leur activité à titre professionnel (journaliste, avocat, magistrat, etc.)[91]. Ces éditeurs non professionnels bénéficient d'une « faculté d'anonymat »[92] prévues par la loi sur les transactions électroniques.

Ils bénéficient d'une l'exonération d'identification par opposition aux éditeurs professionnels, car leur identification est faite de façon limitée. Toutefois, ils doivent communiquer à l'hébergeur « *des éléments d'identification personnelles* », prévue pour les éditeurs professionnels conformément à l'article 5-2 de la loi précitée. Soumis à une obligation de secret professionnel, l'hébergeur ne peut en aucune cas les révèles sous peine de sanction.

A. ***B- Responsabilité pénale des personnes morales autres que les acteurs d'Internet.***

En général, le droit pénal a vocation à s'appliquer à tous. Mais le législateur Sénégalais est un peu réticent quant à l'admission de la responsabilité pénale des personnes morales[93]. Cette réticence se justifie par un principe fondamental du droit pénal. Il s'agit du « principe de personnalité des peines », en vertu duquel, seule la personne auteur de l'infraction peut être poursuivie. L'infraction ne peut être imputée qu'à la personne qui réunit sur sa tête les éléments constitutifs de cette dernière. « *Or, la personne morale de par sa nature est*

[89] FERAL-SHUHL, *opt.cit*. p.551.

[90] BENOIT. TABAKA, *op. cit*. p. 2.

[91] S. RAMBAUD, « Le blog, objet de multiples responsabilité », Légipresse, n°225, octobre 2005, p. 104, cité par PAPA ASSANE TOURE dans, Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal, *op. cit*.

[92] Puisque selon l'article 5 au point 2 de la loi sur les transactions électroniques, *op. cit*. ils « peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et adresse sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus par la présente loi » de leurs fournisseurs d'hébergement

[93] DIEUNEDORT NZOUABETH « Cours de droit pénal General », Université Cheikh Anta Diop de Dakar, 2018-2019, p. 134.

incapable de commettre une infraction parce qu'elle n'a aucune emprise sur les choses et est dépourvue de volonté et d'intelligence. L'idée d'associer ces deux notions parait donc étrange »[94].

L'irresponsabilité des personnes morales a fait l'objet de plusieurs justifications à travers les théories de la fiction, de principe de spécialité et l'atteinte au principe de la personnalité des peines[95].

Malgré, le rejet de la responsabilité la personne morale par le législateur Sénégalais, ce dernier a prévu quelques cas spécifiques dans lesquels, la personne morale peut voir sa responsabilité engagée. Le législateur Sénégalais a opté pour une responsabilité sectorielle. En effet, la responsabilité des personnes morale ne peut être engagée que de façon exceptionnelle à savoir en matière le blanchiment de capitaux, de financement du terrorisme et de la cybercriminalité. En sus, les articles 270, 271et 272 du code pénal, relatifs aux personnes responsables en matière d'infractions commise par des moyens de diffusion publique, vise la personnalité des personnes ayant la qualité de directeur de publication, de co-directeur, de producteur éditeur gérant, de directeur d'entreprise d'impression, de reproduction ou de diffusion de quelque nature que ce soit, de vendeur, afficheur, distributeur, importer, explorateurs, et leurs complices[96]. Contrairement au droit Sénégalais, en droit français, il y a une généralisation de la responsabilité pénale des personnes morales, à travers une évolution du code pénal, depuis la loi du 9mars 2004, dite Perben II entrée en vigueur à partir du 31decembre 2005.

---

[94] V. K. SALL, La responsabilité pénale des personnes morales en droit sénégalais, Mémoire Master2, FSJP, UCAD ; 2016, pp. 12 et S. cité par DIEUNEDORT NZOUABETH,*op.cit.*, p. 134.

[95] Il y a d'abord la théorie de la fiction selon laquelle la responsabilité pénale se concilie mal avec la nature propre de la personne morale, puisque cette dernière ne peut parler, agir ou s'exprimer que sur le biais des personnes qui la composent, elle ne peut donc voir sa responsabilité engagée sur le plan pénal parce que dépourvue de volonté et d'intelligence95. Ensuite le principe de « spécialité » des personnes morales, qui implique que leur responsabilité juridique en droit civil passe par l'existence d'un objet social qui « ne peut en aucun cas consister en la commission d'une infraction ». L'infraction fait sortir du groupement de son objet social et lui fait perdre la personnalité juridique qui lui avait été conférée. De même, il a été soutenu que les peines prévues étaient inadaptées et donc inapplicables aux êtres moraux parce que consistant en des peines privatives et restrictives de liberté : « l'amende est une peine et toute est personnelle, sauf les exceptions prévues par la loi ; elle ne peut donc être prononcée contre un être moral, lequel ne peut encourir qu'une responsabilité civile »95.Enfin on a soutenu que l'engagement de la responsabilité des personnes morales porterait atteinte au principe de la personnalité des peines parce qu'elle a pour effet de punir indistinctement tous membres du groupe y compris ceux qui n'ont pas voulu la commission de l'infraction95.

[96] DIEUNEDORT NZOUABETH*, ibid.*,p.136.

Pour que la responsabilité des personnes morales soit engagée, il faut que l'infraction soit commise par l'un de ces organes ou représentants. N'étant pas définie par le législateur français, la doctrine à tenter de donner une définition de l'organe, en assimilant cette notion à la *« structure de gestion dont le groupement est doté en vertu de ses statuts ou de la loi »*[97]. S'agissant du représentant, il désigne en principe, une personne physique titulaire d'un pouvoir de direction, tel qu'un administrateur ou toute autre personne dotée d'un mandat de représentation de la personne morale en vue de l'accomplissement d'actes juridiques.[98]

De même, l'organe ou le représentant doivent agir pour le compte de la personne morale. De cette dernière condition, suscite des interrogations doctrinales »[99]. Certains auteurs ont pu considérer que la condition revenait à limiter le champ d'application de la responsabilité des personnes morales aux seules infractions susceptibles de leur procurer un avantage ou de permettre la réalisation d'une économie. Ce qui exclut du champ de cette responsabilité les infractions qui ne procurent pas un avantage matériel aux personnes morales tel que la discrimination en raison de l'appartenance à une ethnie, une nation ou une race ou encore des infractions de nature sexuelle. Tandis que d'autres préfèrent une approche mixte en fonction de la nature de l'infraction en retenant non seulement le profit ou l'économie réaliser pour les infraction lucratives et du dysfonctionnement de la personne morales ayant permis la réalisation de l'infraction dans les autres cas [100]. Tandis que d'autres soutiennent d'idée selon laquelle « l'expression n'implique ni gain, pour l'entreprise ni dysfonctionnement. C'est cette dernière approche qui a été consacrée par la cours de cassation française qui rejette la théorie de faute et n'exige pas que soit établit l'existence d'un avantage au profit de la personne morale pour que soit retenus sa culpabilité »[101]. Pour le juge, la responsabilité des personnes morales découle automatiquement de celle de l'organe ou représentant, dès lors que ce dernier a commis l'infraction dans l'exercice de ses fonction de représentation.

En outre, si d'autre peines peuvent être prononcées contre la personnes morale du fait qu'il dispose un patrimoine, les peines comme l'emprisonnement, l'accomplissement d'un travail d'intérêt général, la suspension ou le retrait du permis de conduite ou de chasse ne

[97] ALAIN COEURET et ELISABETH FORTIS, *Droit pénal du travail*, Paris, 4eme Ed.Lexis Nexis Litec, 2008, p.187.
[98] *Ibid*.
[99] *Ibid*.
[100] JACQUES-HENRI Robert, *op. cit*., p. 357 à 358.
[101] Crim. 2 decembre1997, n°408 p. 1350, https://www.legifrance.gouv.fr, consultée le 29/10/2019 à 13h33.

peuvent en aucun cas être prononcées contre une personne morale [102]. En effet, à l'exclusion les sanctions précitées, qui ne peuvent frapper que les personnes physiques, la personne morale peut être sanctionnée à d'autres peines. Il s'agit selon l'article 431-62 de la loi sur la cybercriminalité de l'amende, de la dissolution de la personne morale , de la fermeture définitive ou temporaire d'une durée de 5ans au plus, de l'interdiction définitive ou temporaire d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales, l'exclusion définitive ou temporaire du marché public, la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, l'interdiction définitive ou temporaire d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement, l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique. En plus de ces peines principales, le juge peut prononcer des peines complémentaires telles que l'interdiction d'émettre des messages de communication numérique, l'interdiction à titre provisoire ou définitive de l'accès au site ayant servi à commettre l'infraction, en couper l'accès par tous moyens techniques disponible ou même en interdire l'hébergement[103].

Section II : Les règles de procédures applicables en matière de cybercriminalité.

Les règles de procédure applicables au cyber-délinquance sont relatives aux actes de poursuites Paragraphe (I). Il existe en outre d'autres règles de procédure applicable à la cybercriminalité (II).

Paragraphe I : Les actes de poursuites.

En droit pénal, lorsqu'une infraction a été commise, il est se pose le problème de rechercher des preuves, d'identifier la personne auteur de l'infraction et de la juger afin de la condamner. En sus, en droit pénal, *« la personne suspectée ou poursuivie doit être présumée innocente jusqu'à ce que sa culpabilité ait été légalement démontrée* »[104]. C'est ce que l'on appelle la présomption d'innocence. Cette présomption dont est bénéficiaire la personne soupçonnée, a pour conséquence que la recherche de preuve de l'infraction et de la culpabilité de ce dernier

[102] GASTON STEFANI, GEORGES LEVASSEUR, BERNARD BOULOC, *Droit pénal général*, 15 Edition, Dalloz, p.402.
[103] Loi sur la cybercriminalité, *op. cit.* Art.431-64.
[104] THIERRY GARE, CATHERINE GINESTET, *Droit pénal Procédure pénale*, 8edition Dalloz, 2014, p.249.

incombe au ministère public ou à la partie lésée. Cette procédure fait intervenir plusieurs organes. Il s'agit d'abord de l'organe de police judicaire. Son rôle consiste dans la recherche des infractions et l'identification de leurs auteurs. La police judiciaire est composée d'officier de police judiciaire (articles 15 du code de procédure pénale) et d'agents de polices judicaires (article19 du code de procédure pénale). Ces organes interviennent souvent dans de cadre de l'enquêtes réglementées par les articles 45 à 69 du code de procédure pénale. Il s'agit de l'enquête sur infraction flagrante et de l'enquête préliminaire.

L'enquête sur flagrance délit. Selon l'article 45 du code de procédure pénale, il y a trois hypothèses de fragrance. L'infraction qui se commet actuellement ou vient de se commettre, c'est aussi de cas lorsque l'individu soupçonne est poursuivi par clameur publique ou s'il porte d'objets, de traces ou d'indices rendant vraisemblables sa participation à l'infraction et enfin le cas lorsque l'infraction a été commise à l'intérieur d'une maison et que le légitime occupant demande de la constater.

A côte de l'enquête de flagrance, il y a l'enquête préliminaire qui est aussi menée par la police judiciaire. La recherche et la constatation des infractions ainsi que l'identification de leurs auteurs font intervenir d'autres organes tels que le juge d'instruction sans oublie le rôle du Procureur de la République.

Le juge d'instruction est un juge chargé d'ouvrir une information concernant un crime ou certains délits à la demande du Procureur de la République par un réquisitoire introductif d'instance ou à la demande de la partie lésée par une plainte avec constitution de partie civile. Et enfin le procureur de la République est la personne chargée de la mise en mouvement et de l'exercice de l'action publique.

L'avènement de la cybercriminalité ne reste pas sans conséquence majeurs sur les actes d'investigation menés par des organes cités ci-dessus. Ainsi, « *la lutte contre la criminalité organisée nécessite que les enquêteurs disposent de prérogatives plus coercitives et plus rapides, surtout dans l'environnement numérique. Les méthodes traditionnelles de recherche des preuves y sont certes applicables, mais elles sont parfois limitées face aux modes opératoires employés par les cybercriminels* »[105]. Face à cette situation, les investigations dans ce domaine se font sur la base de la perquisition informatique, et de la saisie

[105] PAPA GUEYE, *criminalité organisés, terrorisme et cybercriminalité : Réponse de politiques criminelles*, l'harmattan, 2018 P.376.

informatique (A) mais aussi d'autres actes de poursuites spécifiques aux cyberdelinquances sont applicables(B)

A- Les actes de procédures classiques adaptés à la cybercriminalité.

Il s'agit dans cette partie d'étudier d'une part la perquisition informatique et d'autre part de la saisie informatique.

« La perquisition a pour objectif la recherche, à l'intérieur d'un lieu, d'indices ou d'objets pouvant établir l'existence d'une infraction[106]. Elle constitue la *« recherche policière et judiciaire des éléments de preuves d'une infraction* »[107]. « *Elle n'est pas une simple présence de l'enquêteur sur les lieux mais consiste en « une instruction, une pénétration* »[108] à l'intérieur du domicile d'une personne privée ou dans les locaux appartenant à une personne morale en vue de la recherche d'objets relatifs aux faits poursuivis. Ainsi, « *les perquisitions peuvent s'effectuer dans tous les lieux où il est possible de trouver des objets dont la découverte serait utile à la manifestation de la vérité*[109].

Les organes chargés de l'enquête peuvent procéder à des perquisitions en cas d'enquête de flagrant délit, en cas d'enquête préliminaire ou lorsqu'une information est ouverte.

En droit commun l'article 48 du code de procédure pénale dispose que « *l'officier de police judiciaire, a le pouvoir, dans le cadre de sa mission, de procéder à une perquisition au domicile des personnes qui paraissent avoir participé au crime ou détenir des objets ou pièces relatifs au crime afin de récolter la preuve du crime ». Il doit dresser un procès-verbal de cette perquisition* ». Ce pouvoir de perquisition obéit à des conditions bien déterminées. Afin de préserver le respect des droit de la défense, *« les perquisitions et saisies de l'OPJ doivent être effectuées en présence des personnes soupçonnées d'avoir participé au crime et de la personne au domicile de laquelle la perquisition a lieu*[110] ». De même les perquisitions et visites domiciliaires ne peuvent être effectuées avant 5heures et après 21heures sauf disposition contraire[111]. Sous peine de nullité, les perquisitions doivent être mentionnées dans un procès-verbal dressé et signés par les personnes citées ci-dessus.

---

[106] JEAN PRADEL, *Procédure pénale*, 17eme édition, Cujas, 2013, p.374.
[107] SERGE GUINCHARD et THIERRY DEBARD, *Lexique des termes juridiques*, 25eme édition 2017-2018 p.833.
[108] JEAN PRADEL, *op. cit* p. 374.
[109] THIERRY GARE ET CATHERINE GUIESTET, *op. cit*. p.345.
[110] Article 49 alinéa 1 du code de procédure pénale du Sénégal. (CPPS)
[111] ART. 51 al. 1, *ibid.*

Dans le cadre de la cybercriminalité, en raison du caractère immatériel des infractions, les perquisitions s'effectuent en ligne. C'est ce qui justifie qu'on les appelle « les perquisitions informatiques ». Les *« perquisitions en ligne » ou « informatiques » sont des procédures permettant d'accéder à des systèmes informatiques, notamment le disque dur d'une ordinateur, les clés USB CD-Rom et aussi à des données qui peuvent être stockées dans un autre système très éloigné du lieu de la perquisition* »[112].

Aux termes de l'article 677-36 de la loi sur la cybercriminalité, « *lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatique sur le territoire Sénégalais, sont utiles à la manifestation de la vérité ; le juge d'instruction peut opère une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou autre système informatique des lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial* »[113] . Ainsi, le juge d'instruction saisit sur requête du procureur de la République ou sur demande de la victime pour ouvrir une information, peut si la nécessité de l'enquête d'exige procéder à la perquisition. Les perquisitions ne sont possibles que s'ils tendent vers la manifestation de la vérité. Ce qui exclut des perquisitions n'ayant aucun rapport avec la manifestation de la vérité. Ces actes sont en principe exercés par le juge d'instruction, mais rien ne s'opposent à ce qu'ils puissent être exercés par les officiers de police judiciaire, qui à travers leur mission d'enquête ou sur commission rogatoire, recourir à cette pratique. Par ailleurs pour ce qui concerne l'enquête de flagrant délit, les officiers de police ou sous leur responsabilité les agents de police judiciaire peuvent, « *au cours d' une perquisition effectuée dans les conditions prévues à article 51-1 du CPP ; accéder par un système informatique, implanté sur les lieux où se déroule la perquisition, à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, des lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial sans le consentement du propriétaire du système* »[114] .En sus, en ce qui concerne l'enquête préliminaire, les perquisitions de système informatique ne peuvent avoir lieu qu'avec le consentement expresse de la personne chez qui l'opération aura lieu.

En ce qui concerne la saisie, le code de procédure pénale estime que les officiers de police judiciaire peuvent dans le cadre d'une enquête de fragrant délit saisir toute arme ou

[112] PAPA GUEYE, *op. cit.* p. 377.
[113] ART. 677 de la loi sur la cybercriminalité, *op. cit.*
[114] ARTS. 677-36 à 677- 37. *Ibid.*

instrument ayant servi à commettre de crime ou dont l'utilisation été prévue pour le commettre et préserver tout indice trouvé sur les lieux. Ils peuvent saisir tous papiers, documents ou objets relatifs aux faits incriminés. Ces papiers et documents ou objets doivent être immédiatement inventoriés et placés sous scellés[115].

La saisie informatique, quant à elle est possible, dans tous les cas où elle permet une manifestation de la vérité aux organes chargés de l'enquête. Tout comme la saisie classique, la saisie informatique également peut porter sur tous les objets, papiers, documents, ou données informatique qui ont servi à l'infraction ou qui en constituent le produit. La saisie consiste à faire ou conserver une copie de données informatique, y compris en utilisant l'équipement sur site ; et rendre inaccessible, ou en supprimant, les données informatiques dans le système informatique accédé ; ou faire sortir sur imprimante les données informatiques. Il en est ainsi de la saisine les cédéroms, les clés USB ou des téléphones mobiles. Le juge d'instruction ou les officiers de police judiciaire conformément à l'article 677-37 de la loi sur la cybercriminalité peuvent procéder à cette opération si l'objet ou le document ou les données saisis serviront éventuellement à apporter des informations nécessaires dans le cadre de leur enquête. « *La saisie des données consiste à placer sous mains de justice soit leur support physique soit une copie en présence des personnes qui assistent à la perquisition »*[116].Par ailleurs, en cas d'enquête préliminaire, les perquisitions et saisies ne peuvent être effectuées sans le consentement expresse de la personne chez qui l'opération a lieu[117]. Cela étant dit, il convient de voir dans ensuite les actes de procédure spécifique à la cyber-délinquance.

B : Les actes de procédure spécifique à la cyber-délinquance.

Il s'agit, ici, de l'interception de correspondance et de la conservation des données. Ce sont les actes de procédure qui peuvent être utilisés quand l'infraction est commise par l'utilisation des TIC. Mais l'interception de données peut être utilisée par les enquêteurs pour écouter les conservations d'une personne soupçonnée afin de prouver sa culpabilité ou son innocence, dans une enquête portant sur une infraction classique.

[115] Art. 48 CPPS.
[116] Dr. PAPA GUEYE, *op. cit.* P. 379.
[117] ART. 68, CPPS, *op. cit.*

L'interception de correspondances ou de données informatisées émises par la voie des TIC en matière de police judiciaire consiste à des écoutes téléphoniques. Il peut également porter sur tout échange de correspondance par voie électroniques tels que les mails, messagerie instantanées, etc.[118]. Aux termes de l'article 677-38 « *si les nécessites de l'information l'exige, le juge d'instruction peut utiliser les moyens techniques appropries pour collecter ou enregistrer en temps réel les données relatives au contenu de communication spécifiques transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existant ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées* ». L'interception des données informatisées est caractérisée par le secret professionnel.

L'utilisation de la technique d'interception de données par les enquêteurs, en cours les enquêtes, est dérogatoire au droit commun, car comme nous le savons, interception de correspondance est une infraction en vertu de la loi sur la cybercriminalité. En effet ; seules les personnes autorisées par la loi peuvent procéder à cette pratique sans que leur responsabilité pénale ou civile ne soit engagée.

Par ailleurs, il convient de signaler que le principe général de confidentialité des communications est protégé par la Convention européenne des droits de l'homme qui précise que « *le secret des correspondances émise par la voie de télécommunications est garanti par la loi. Il ne peut être porte atteint à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêts publics prévus par la loi* ». Ce souci de protection qu'apporte la convention, n'empêche en rien à ce que les Etats prévoient des procédures d'interception de données dans le cadre des enquêtes en matière de cybercriminalité.

En effet, «*La loi devrait permettre aux autorités chargées de l'enquête d'appliquer toute mesure technique permettant la collecte de données de trafic dans la poursuite des infractions pénales. Elle devrait être révisée en vue de rendre possible l'interception de télécommunication et la collecte de données de trafic dans le cadre d'enquête sur des infractions graves contre la confidentialité, l'intégrité et la disponibilité des systèmes de*

[118] L'accès des autorités publique aux données chiffrées, 30 Aout 2017, https://www.cnil.fr consulté le 25septembre 2019 à 17h 24.

télécommunications ou informatiques »[119] Toutefois les pouvoirs des organes charges de l'enquête devraient être limités dans le cadre de l'interception des données, du fait que ce procède entraine des immixtions clandestines dans la vie privée les individus. En outre, certains auteurs considèrent que *« l'absence de limitation de la durée de l'interception des données par l'autorité et sur de droit de recours contre la décision judicaire d'interception constituent de réels dangers susceptibles de favoriser des atteintes à la vie privée des citoyens* »[120]. Pour concilier la protection de la vie privée et la protection de l'intérêt général, le législateur devrait admettre d'interception de données que pour les infractions portant atteintes à la sécurité de l'Etat et les atteintes à la vie.

La conservation rapide des données. Aux termes de l'article 677- 35 du code de procédure pénales « *si les nécessite de l'information l'exigence ,notamment lorsqu'il y a des raison de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou modification, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaire* ».Les personnes chargées de les conserver ne doivent en aucun cas les communiquer à une autre, elles sont tenues par le secret professionnel. Elles engagent leur responsabilité pénale en cas de violation du secret professionnel.

En outre, « *cette conservation des données de connexion est dérogatoire au droit commun qui pose, au contraire un principe d'effacement des données de communication dès la fin de la communication* »[121].

Si les données sont stockées dans un serveur qui se trouve hors du territoire national, les pays poursuivantes peuvent, en vertu de l'article 29 de la convention, demander une entraide en vue d'obtenir la conversation rapide de données stockées au moyen d'un système informatique.

La conservation des données par les différents opérateurs et prestataires de services de communication électronique fait l'objet d'un débat en France. « *En effet dans sa décision du*

[119] Problème de procédure pénale lies à la technologie de l'information, Recommandation N°R(95) 13 adoptée par le comité des Ministres du Conseil de l'Europe le 11 septembre 1995 P.59, https://rm.coe.int, consultée le 28/10/2019 à 20h30.

[120] THIERNO AMADOU NDIOGOU, « Etude sur L'Etat des lieux de la cybersécurité et de la cybercriminalité au Sénégal », Global Partner Digital Jonction, mars 2019 p. 10.

[121] MARTINE EXPOSITO « Prévenir des cybercriminalité dans un contexte professionnel, https://cours.unjf.fr, consultée le 13/06/ 2019 à 12h15.

8 avril 2014 ; la Cour de Justice de l'Union Européenne à invalider la directive 2006/24/CE du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de service de communication électroniques accessibles au public ou de réseaux publics de communication. De même dans un arrêt conjoint, la cour de Justice de l'Union Européenne affirme que le droit de l'Union européenne ne s'opposait pas à une règlementation nationale imposant une conservation ciblée des données pour lutter contre la « criminalité grave » sous certaines conditions :

- *Limiter clairement et précisément, « au strict nécessaire » les catégories de données à conserver, les moyens de communication vises, les personnes concernées ainsi que la durée de conservation et offrir des garanties suffisantes à cet égard ;*
- *Se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux donnes doit être accordé aux autorités nationales compétentes ;*
- *Respecter les droits fondamentaux que sont le respect de la vie privée et la protection des données à caractère personnel ;*
- *Soumettre l'accès aux données à certain garde-fous (notamment : un contrôle préalable par une autorité indépendante) ;*
- *Conserver les données sur le territoire de l'Union européenne* »[122].

A votre avis, ces conditions posées par la jurisprudence montrent que la conservation des données est une méthode strictement encadrer et constitue une exception en matière d'enquête. Par ailleurs, il convient d'analyser les autres règles de procédure applicables en matière de cybercriminalité.

Paragraphe II : Les autres règles de procédures applicables en matière de cybercriminalité.

Il s'agit d'examiner la spécificité de la prescription de l'action publique en matière de cybercriminalité (A) et les modes de preuves(B)

[122] Rapport sur « La procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique : proposition pour une efficacité juridique renforcée », présentés par ERIC FREYSINETET ET CORINE THIERACHE, enregistré dans code pénal et cybercriminalité, le 24 juin 2014 p. 21 à 22.

A : La spécificité de la prescription de l'action publique en matière de cybercriminalité.

En droit pénal, la poursuite des auteurs d'une infraction ne peut se faire à tout moment. Il existe des délais au-delà desquels, une personne ne peut être poursuivie. On parle de prescription de l'action publique. La prescription de l'action publique peut être définie comme l'extinction du droit d'action par l'écoulement d'un délai.

La prescription se justifie pour plusieurs raisons : d'abord, on a pensé à l'idée d'amendement et d'expiation chez le délinquant. C'est la conception morale de la prescription. Ensuite, on a invoqué qu'au bout d'un certain temps, il est inutile de raviver les souvenir d'une infraction déjà tombée dans l'oubli[123]. En effet, *« la paix et la tranquillité publique commanderait, après un certain délai, d'oublier l'infraction et non d'en raviver le souvenir, mais aussi la contrepartie de l'inquiétude dans laquelle vit l'auteur des faits aussi longtemps qu'il échappe à la poursuite* »[124]. C'est la conception socialiste de la prescription. Enfin on a soutenu qu'il y a prescription à cause du dépérissement des preuves. On parle de la conception technique de la prescription. En sus, *« avec les années, les traces ou les indice disparaissent et les témoignages devient fragiles. Le risque de l'erreur judiciaire conduit logiquement à renoncer à exercer l'action publique* »[125]. La mise en place de la prescription par le législateur a pour objectif de rappeler au Ministère Publique et la partie lésée que les poursuites ne peuvent être engagées que dans les délais normaux de l'action publique, dans ce cas la prescription peut être analysée comme une sanction de la négligence du ministère publique ou de la partie lésée. On parle également de la conception technique Selon Mme Dominique-Noelle Commaret, *« tout temps mort excessif laisse présumer le désintérêt de la victime ou du ministère public et leur renoncement, dans un système marqué par le principe d'opportunité des poursuites, la prescription apparait comme une réponse procédurale apportée à l'inaction ou l'oubli, volontaire ou involontaire* »[126].

Toutefois ; ces justifications n'échappent pas aux critiques : d'abord on a fait remarquer que l'idée d'une expiation résultant de l'angoisse imposée au délinquant n'est pas très convaincante car le temps n'a pas le même effet chez tous les délinquants[127]. Ensuite, on a

---

[123] BERNARD BOULOC, *Procédure Pénale*, Dalloz, Coll. Précis, 22eme édition, 2010, p.173.
[124] Pour un droit de la prescription moderne et cohérent, https://www.senat.fr, consultée le O2/07/2019 à 15h13.
[125] *Ibid.*
[126] DOMINIQUE-NOELLE COMMARET, Point de départ du délai de prescription de l'action publique : des palliatifs jurisprudentiels faute de réforme législative d'ensemble, Revue de science criminelle, 2004, cité dans Pour un droit de la prescription moderne et cohérent, *ibid*.
[127] JEAN. PRADEL, *Procédure Pénale*, Cujas, 15eme édition, 2010 p.184.

soutenu que la prescription nuit à la protection de la société dans la mesure où elle profite aux grands délinquant comme aux petits délinquants alors que le temps ne saurait atténuer les dangers des premiers. Ainsi, la prescription suppose une impunité de l'auteur de l'infraction et ne garantit pas à cet effet l'absence de récidive de la part de ce dernier[128]. De même il s'avère aujourd'hui plus difficile d'invoquer le dépérissement les preuves avec l'évolution de la science qui peut détecter les empreintes génétique pou les traces ADN.

Le régime juridique de la prescription de droit commun, se manifeste par la détermination du délai de prescription et par l'interruption de la prescription.

Ainsi, le délai de prescription de droit commun varie selon la nature de l'infraction. Il est de dix ans pour les crimes ; de trois ans pour les délits et de un an pour les contraventions. Toutefois, en dehors les délais de prescription de droit commun, la loi à prévue dans certains cas des délais de prescriptions distinctes. Il en est ainsi en cas le détournement de derniers publics ou l'action public se prescrit pour sept ans.

Le délai de prescription commence à courir à partir du moment où l'infraction est définitivement réalisée et non au jour où l'agent est entrain de la commettre .Pour les infractions instantanées le point de départ est fixé au jour de l'acte délictueux ; pour celles continue le délai commence à courir à compter du jour de la cessation de l'acte délictueux et enfin pour l'infraction à élément multiples, la prescription commence à courir à compter du jour du dernier acte matériel.

La loi sur la cybercriminalité a également prévu les délais de prescription qui présentent une particularité d'interruption de la prescription par rapport au droit commun de la prescription, lorsque l'infraction est commise par le biais de réseaux informatiques en fixant le point de départ de la prescription « à compter de la cessation de l'activité délictueuse en ligne ».[129]

Il faut signaler que le cours de la prescription peut être interrompu ou suspendu.

On parle, lorsque le délai déjà partiellement écoulé se trouve anéanti et qu'il faut en recommencer un autre. La loi a prévu quelques causes d'interruption de l'action publique. Il s'agit des actes d'instructions et ceux de poursuite. Les actes de poursuite sont la citation directe, la réquisition, la plainte avec constitution de partie civile. Autrement dit, les actes de

[128] VALERIAN FORMY « Le désordre de la prescription de l'action publique », Mémoire pour l'obtention du diplôme d'Etude Approfondie, 2010-2011. P.22
[129] ART. 677-34, de la loi sur la cybercriminalité, *op.cit.*

poursuite sont les actes de mise en mouvement de l'action publique. Quant aux actes d'instruction, ce sont des actes accomplis par un juge d'instruction ou par un officier de police judiciaire et qui ont pour objet la recherche ou la réunion des preuves à partir du moment où une information est ouvert[130].

L'interruption de l'action publique entraine des conséquences qui varient selon qu'il s'agit de la personne ou le l'infraction. Pour les personne, l'interruption est absolue et joue à l'égard de tous, qu'ils soient auteurs, coauteurs ou complices. Pour l'infraction, l'interruption a un effet relatif car elle se limite aux faits délictueux visés dans l'acte d'instruction ou dans la poursuite. L'interruption de la prescription anéantit le délai déjà écoulé et marque le point de départ d'un nouveau délai.

La suspension de la prescription, quant à elle, a pour objectif d'arrêter de façon temporaire le cours de la prescription sans effacer le délai déjà couru. La loi prévoit deux causes de suspension de l'action publique. Il s'agit les obstacles de droit et des obstacles de faits. Concernant les obstacles de droit, ce sont des évènements dressés par le législateur qui empêchent la prescription de courir. Il y a obstacle de droit lorsque l'action publique ne peut être exercée qu'après un jugement préalable. C'et les problèmes des questions préjudicielles à l'action publique. Il en est ainsi du délai de suspension d'état[131].

S'agissant des obstacles de faits, ce sont les difficultés résultant d'évènements accidentels qui, dans une affaire déterminée, empêchent de déclencher ou d'exercer l'action publique. C'est l'exemple de la guerre. Lorsqu'il y a suspension de l'action publique, la prescription commence à courir après la disparition de cet obstacle. Contrairement à l'interruption, la suspension n'anéantit pas les délais déjà écoulés. Ces derniers viendront s'ajouter aux délais restant pour à courir pour le décompte du délai de prescription.

En somme, la prescription de l'action publique, empêche la mise en mouvement ou l'exercice de l'action publique, que ce soit à l'égard du Ministère publique ou à l'égard des parties civiles en cas d'existence. Par ailleurs, la prescription se manifeste par son caractère l'ordre public. Par conséquent, elle s'impose à tous même au Ministère Public qui est le défenseur de l'intérêt général. De même, le juge a le devoir de la soulever d'office, au cas où les parties au procès ne s'en prévalent pas.

[130] Un interrogatoire, une audition de témoin, un transport sur les lieux, une perquisition.

[131] Ce délit pour être poursuivi pénalement nécessite qu'un faux soit commis dans l'acte de naissance d'un enfant pour modifier sa filiation. C'est après la décision du juge civile saisi préalablement de la question que l'action publique pourra être intentée.

La loi sur la cybercriminalité, n'a pas traité les questions concernant la durée de la prescription selon de nature de l'infraction cybercriminelle, ni parlée de l'interruption ou de la suspension de l'action publique. Cela laisse croire que dans ces questions, il n'existe pas une différence selon qu'il s'agit de la prescription de droit commun ou les règles de prescription applicables à la cybercriminalité. Si c'est le cas, la seule différence résulterait dans la détermination du point de départ du délai de prescription.

Bien que la loi sur la cybercriminalité ne mentionne que les délais de prescriptions et le point de départ de la prescription de l'action publique en matière de cybercriminalité, nous pouvons déduire que le régime juridique concernant l'interruption et la suspension des délais de prescription sont identiques à ceux du droit commun. A côté de la prescription de l'action publique, il existe des modes de preuve applicable à la cybercriminalité.

B. B : Les modes de preuve applicable à la cybercriminalité.

En vertu du principe de la liberté des preuves en manière de procédure pénale, les infractions peuvent se prouver par tout moyen[132]. Cela se justifie non seulement dans le fait que les infractions ne sont pas des actes juridiques mais des faits juridiques, mais aussi par le souci de garantir la célérité du procès pénal ; car les délinquants peuvent dissimuler leurs actes rendant ainsi difficile de les découvrir si la preuve était préconstituée.

Le droit pénal n'a pas exclu l'écrit parmi les modes de preuve. Toutefois, « il ne peut avoir un rôle aussi important qu'un droit civil. En effet, il existe en droit commun plusieurs modes de preuve qui ont tous la même force probante car laissés à l'appréciation du juge.

Parmi ces modes de preuve nous pouvons citer :

Le témoignage. C'est une déclaration faite par une personne(le témoin) concernant des faits ou évènements dont elle a eu personnellement connaissance. Selon Bentham les témoins sont « *les yeux et les oreilles de la justice* »[133]. Le témoin est destiné à donner une information sur les faits ou évènements faisant l'objet de l'enquête. Le témoignage est recevable dans toutes les étapes de la procédure, allant de l'enquête, ou de l'instruction jusqu'au jugement.

L'aveu, quant à lui, est une reconnaissance, par une personne soupçonnée ou poursuivie, de l'exactitude de tout ou partie des faits qui lui sont reprochés. L'aveu peut être

[132] ART. 414 CPPS.
[133] THIERRY GARE, CATHERINE GUINESTET, *Droit pénal procédure pénale*, Dalloz, 2010, p.243.

judiciaire ou extrajudiciaire. Il est dit judicaire lorsque la personne concernée le fait devant le juge. Dans cette hypothèse, le juge est tenu de prendre en compte cet aveu. L'aveu est dit extrajudiciaire lorsqu'il est fait en absence du juge.

La preuve par présomption de fait. C'est un mécanisme qui consiste pour le juge de tirer une conséquence d'un fait connu lorsqu'il existe un fait inconnu. Les présomptions de fait ou judicaire sont laissées à l'appréciation du juge, qui ne doit les admettre que si elles sont graves, précises et concordantes. Il existe d'autres modes de preuve en matière pénale non énumérés. Ce qui revient à dire que la liste n'est pas exhaustive.

En plus de ces mode de preuve qui relèvent du droit commun de la preuve en matière pénale, nous constatons que l'utilisation des TIC pour commettre une infraction a une incidence sur l'élaboration des éléments de preuves afin d'appréhender l'auteur de l'infraction.

En effet, la présomption d'innocence prévue par plusieurs textes internationaux exige, en ce que la personne poursuivie ou soupçonnée soit présumée innocente jusqu'à ce que sa culpabilité soit légalement établie par un jugement définitif. Ces textes sont entre autres la Déclaration des droits de l'homme et du citoyen de 1789, qui en son article 9 qui dispose que « tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable »[134] . Il en est de même de la Déclaration universelle des droits de l'homme qui à son article 11 dispose que « toute personne accusée d'un acte délictueux est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie au cours d'un procès public ou toutes les garanties nécessaires à sa défense lui auront été assurées »[135]. D'où l'importance de la preuve.

En matière de cybercriminalité, du fait de l'immatérialité de l'infraction, la recherche ou la collecte des éléments de preuve doit être différente de celle traditionnelle. En effet, « *les preuves numériques ont été acceptés comme nouvelles sources de preuve*[136]. Elles constituent *« une modalité particulière d'établissement de la vérité qui consiste à avoir recours à des moyens numériques varies qui vont de l'étude des contenus dans la mémoire d'un disque dur, aux messages électroniques, en passant par l'enregistrement numérique* »[137]. En effet, Les éléments de preuves numériques sont d'importance nécessitée dans plusieurs phases du travail

[134] ART. 9 de la Déclaration des droits de l'homme et du citoyen de 1789.
[135] ART. 11 de la Déclaration Universelle des droits de l'homme du 10decembre 1948.
[136] Rapport sur « comprendre la cybercriminalité : Guide pour les pays en développement », élaboré à partir d'un ouvrage intitulé, comprendre la cybercriminalité : Guide pour les pays en développement, présenté par MARCO GERCHE, UIT 2012, p.239.
[137] MELANIE CLEMENT-FONTAINE « De l'information numérique à la preuve numérique », colloque du 13 Avril 2010 à la Première Chambre de la Cour d'Appel de Paris, p.11.

d'enquête sur la cybercriminalité. Parmi ces phases nous pouvons citer *: « la phase d'identification des éléments de preuves pertinents ; la phase de collecte et d'archivage des éléments de preuve ; la phase d'analyse de la technologie informatique et des éléments de preuve numérique ; la présentation des éléments de preuve au tribunal »*[138].

Ce procédé qui constitue la collecte numérique des preuves est issu de la « criminologique informatique ». Ce terme désigne *« l'analyse systématique des équipements informatique et télécommunication dans le but de trouver des éléments de preuve numériques* »[139].

Le recours à la preuve numérique se justifie par le fait que l'auteur de l'infraction, en utilisant les TIC pour la commettre, laisse des traces derrière lui. Ces traces laissées par ce dernier serviront de preuves pour son inculpation. Tel est le cas lorsqu'un suspect a recours à de moteurs de recherche pour trouver des documents de pédopornographie, sa recherche, puis ses adresses IP et dans certains cas, des informations supplémentaires relatives à son identité (comme son nom d'utilisateur Google) sont enregistrés.[140]Ainsi, les experts en criminalistiques informatique peuvent analyser le matériel et logiciels informatiques utilisés par un suspect, restaurer des fichiers effacés, décrypter des fichiers ou identifier des internautes en analysant les données relatives au trafic[141].Les traces laissées par l'auteur de l'infraction permettent la célérité de l'enquête car elles orientent les enquêteurs, qui au lieu de perdre leur temps à rechercher des preuves dans plusieurs secteurs géographiques, se dirigent directement vers les lieux où se trouvent ces traces.

Toutefois, la liberté de la preuve en matière pénale, ne signifie pas que toutes les preuves sont recevables. En effet, la recherche et l'administration de la preuve doivent se faire dans le respect de certains principes qui tournent autour du principe de la légalité de la preuve.

Le principe de la légalité interdit d'usage de certains moyens de preuve qui portent atteinte à la dignité de l'homme tels que les pratiques de l'ordalie, l'aveu obtenu par la torture, les procédés scientifiques modernes comme l'utilisation de narcotiques ou de détecteur de mensonge[142]. Selon l'article 3 de la convention européenne des droits de l'homme « nul ne peut être soumise à la torture ni à des peines ou traitements inhumaines ou dégradants ». Cet article marque l'interdiction de toute pratique inhumaine quelle que soit la cause. La

[138] . MARCO GERCKE, *op. cit.,* p. 240.
[139] *Ibidem.*
[140] *Ibidem*.
[141] *Ibidem*.
[142] THIERRY GARE ET CATHERINE GINESTET, *op. cit*. p.757.

procédure pénale n'est pas à l'abri de cette interdiction, qui doit respecter les principes défendus par cette convention.

En dehors du respect de la dignité humaine, la recherche et l'administration de la preuve doivent être effectuées par des procédés loyaux. Il est admis qu'il serait contraire à la dignité de la justice que la ruse et le stratagème soient à l'origine de l'obtention des preuves[143].

En plus de ces principes il y a le principe de la proportionnalité. Ce principe impose à ce que des moyens employés dans la recherche de la preuve, soient proportionnels à la protection des libertés individuelles et collectives. Selon un auteur, « *la collecte de preuves numériques peut conduire à porter atteinte aux libertés individuelles ou collectives. Il doit donc être opère un équilibre entre la légitimité de pouvoir se constituer une preuve afin de faire valoir un droit et le respect des libertés individuelles et collectives des autres* »[144]. A notre avis, cette exigence peut être justifiée par le fait que, le droit pénal a pour principale préoccupation la protection de l'individu contre toutes atteintes de quelque nature qu'elle soit. Et la protection de l'individu n'est rien d'autre que la protection de sa liberté individuelle. Par ailleurs, il convient de signaler que le dispositif de la répression de la cybercriminalité, présente des insuffisances.

Chapitre II : L'insuffisance du dispositif de la répression de la cybercriminalité.

Les textes mis en place par les autorités étatiques, pour lutter contre la cybercriminalité constituent une réelle solution. Mais, face à la montée et à l'évolution de la cybercriminalité, cette solution s'avère insuffisante. Il convient dans cette partie de mettre l'accent sur l'insuffisance du dispositif de la cybercriminalité (section I) avant de proposer un renforcement du dispositif dans le but de l'améliorer (Section II)

Section I : L'insuffisance du cadre juridique du dispositif de la cybercriminalité.

Le dispositif de la répression de la cybercriminalité, présente des insuffisances aussi bien en droit substantiel (paragraphe I) qu'en droit procédural (paragraphe II).

[143] THIERRY GARE ET CATHERINE GINESTET, *op.cit.* p. 757.
[144] MELANIE CLEMENT-FONTAINE, *op. cit*. p. 17.

Paragraphe I : Les difficultés relatives au droit substantiel.

Les insuffisances du droit substantiel se caractérise par l'imprécision de la loi par rapport à certaines infractions(A) et par le silence de la loi sur la cybercriminalité face à certains comportements (B).

A. L'imprécision du dispositif par rapport à certains aqissements.

On a pu remarquer que depuis d'adoption de la loi sur la cybercriminalité, il y a une forte évolution des techniques de cette délinquance. En effet, **le délit d'escroquerie** a vu une évolution considérable au fil des temps. L'escroquerie ne se limite pas au seul fait de soutirer une information confidentielle ou caractérisée par le secret professionnel, mais s'étend à une remise de fonds qui consiste souvent à une utilisation de ces informations escroquées, pour soutirer de l'argent aux victimes. Ainsi nous pouvons citer l'exemple de l'escroquerie à la nigériane ou 419. « *L'escroquerie à la nigériane consiste à envoyer un mail informant la société destinataire d'un changement de cordonnées en raison de dysfonctionnement. Les auteurs y expliquent que le paiement des prochaines factures devra s'effectuer sur un nouveau compte bancaire, mieux sécurisé. Elle touche principalement les entreprises exerçant dans le secteur du commerce, ou les escrocs se font passer pour leurs sous-traitants asiatiques* »[145]. En plus de l'escroquerie à la nigériane, il y a l'escroquerie au président qui consiste à obtenir un virement en se faisant passer pour le PDG de l'entreprise, en justifiant d'une quelconque urgence pour qu'il soit immédiat. En effet, « *une personne de l'entreprise est appelée par le prétendu PDG expliquant qu'il est en déplacement et a besoin d'un virement pour une opération confidentielle* »[146].

Il y a aussi l'escroquerie appelé, l'escroquerie à la norme single Euro Payements Area qui signifie en français l'espace unique de paiements en euro (SEPA). *« Cette nouvelle forme d'escroquerie exploite les failles de la norme SEPA* ». Autrement dit les faiblesses de la norme SEPA. Il s'agit pour ces délinquants de contracter une entreprise en se faisant passer comme un informaticien pour leur convaincre, de se connecter sur un site pour des mises à jour ou des tests de sécurité. « *Ce faux site leur permet de prendre le contrôle à distance du*

[145] PAPA GUEYE, *op.cit*. P. 300.
[146] PAPA GUEYE *Ibid*. P.301.

réseau interne de l'entreprise. Des ordres de virement[147] *sont alors passes sans surveillance puisque les banques ne vérifient plus si l'ordre émane bien de l'entrepris*e »[148].

En fin, existe une autre forme d'escroquerie qui consiste à tromper l'internaute, en faisant semblant de lui envoyer un courriel en cadeau, composé de divers choses comme les vêtements, les chausseurs, des ordinateurs ou portables, sacs etc. Ces escrocs demanderont ensuite au destinataire du courriel de payer un prix de dédouanement. Et ce prix de dédouanement sera versé à une tierce personne, avec qui ils lui mettront en rapports. Cette tierce personne jouera le rôle d'un contrôleur de douane. Une fois que l'internaute versera le prix du dédouanement, il coupe tout contact avec ce dernier.

Face à cette évolution du délit d'escroquerie, nous trouvons nécessaire que le législateur Sénégalais puisse étendre le domaine de l'escroquerie en prenant en compte ces formes d'escroquerie pour mieux répondre à la protection des atteintes aux biens via Internet.

La loi sur la cybercriminalité doit être adaptée à cette tournure des techniques d'escroquerie. Il serait difficile pour une victime d'escroquerie portant sur les informations suivie d'un vol de fond, suite aux informations reçues, soit qualifié comme étant une simple escroquerie commise par l'utilisation des TIC, cela risque de lèse la victime qui non seulement à livrer les informations secrètes à une personne qui n'a pas la qualité de les recevoir, mais aussi se faire appauvrir par cette personne, qui se livre à lui soutirer de l'argents.

A notre avis, la loi doit procéder à une aggravation des peines lorsqu'il y a cumule de ces deux actes afin d'équilibrer les dégâts que ces actes ont causé.

En sus de cela, nous pouvons noter une imprécision de la loi sur la cybercriminalité concernant l'interception des données. En effet, le législateur Sénégalais, en autorisant l'interception des données en matière l'enquête, s'obtient de déterminer des conditions visant à sauvegarder la vie privée imposées dans le rapport explicatif de la Convention de Budapest sur la cybercriminalité[149]. Autrement dit, il n'a pas prévue de condition de protection de la vie privé tel que prévue dans la Convention de Budapest sur la cybercriminalité. Les conditions de protection dont il s'agit, sont : *« la limitation de la durée de l'interception, l'exigence de*

[147] Un virement SEPA est un virement international dans la zone européenne : un transfert de font d'un compte vers le compte d'un bénéficiaire situé dans cette zone européenne. https://www.bluenote-systems.com, consulté le 25/04/2019 à 9h13.

[148] PAPA GUEYE, *op.cit.*, p. 301

[149] PAPA ASSANE TOURE, *op.cit.*, p. 382.

la détermination des infractions concernées par la mesure et du droit de recours contre la décision judiciaire d'interception »[150]. Loi n'a pas donné de précision sur les limites de la durée des interceptions, ni sur les catégories d'infractions pouvons faire l'objet d'une interception de données, ou encore sur la possibilité d'exercice d'une recours contre une décision d'interception[151].

Toutefois les insuffisances du dispositif de la répression de la cybercriminalité ne se limite pas à la seule imprécision de la loi par rapport à certains comportements, mais se manifeste également à travers le caractère transnational de la cybercriminalité.

B: Le silence du dispositif de répression de la cybercriminalité du Sénégal face à certains comportements.

Le dispositif de la répression de la cybercriminalité comporte des limite qui se manifestent par l'omission de certains types de cyber délit tels que :

L'abus de confiance. Le législateur Sénégalais n'a pas prévu ce type l'infraction parmi les atteintes aux biens. L'abus de confiance peut se définir comme étant le fait de porter atteinte à la fortune d'autrui en détournant ou en dissipant tout bien susceptible d'être soustrait et qu'on a reçu à charge de restitution de le conserver, de le représenter, de le rendre ou d'en faire un usage déterminé. En droit positif Sénégalais, le détournement d'une information « reçue » en vertu d'un des contrats énumérés par l'article 383 du code pénal peut-il être admis sans une défiguration du délit d'abus de confiance ? Selon le professeur Lucas de Leyssac *« le vol d'une information seule est possible, en ce sens que cette valeur peut être considérée comme « marchandise » au sens de l'ancien article 408 du code pénal. Ce texte ne précise pas que la chose doit être matérielle. Ce qui serait de nature à ouvrir de nouvelles perspectives à l'abus de confiance d'information* »[152].La jurisprudence Sénégalais a rejeté le cas l'abus de confiance portant sur une information car selon lui « *ce délit suppose pour sa constitution l'existence un contrat en vertu de l'article 383 du code pénal, et la remise d'une chose corporelle ayant une valeur juridique au motif que l'article 383 du code pénal Sénégalais ne*

[150] PAPA GUEYE, *op.cit*., p. 382.
[151] *Ibidem*.
[152] M.P.LUCAS DE LEYSSAC, « une information seule est-il seule susceptible de vol d'une autre atteinte juridique aux bien », D. 1985. Chron. P. 51, n° 48 et 49.

vice dans son contenu que les chose corporelles »[153]. Cet arrêt bien qu'étant antérieur à la loi sur la cybercriminalité n'a pas suscité une prise de conscience du législateur, dans la nécessité d'incriminer ce comportement comme un abus de confiance portant sur une information. Et jusqu'aujourd'hui l'abus de confiance portant sur une information reste impuni au Sénégal faute de base légale

De même nous pouvons citer des comportements comme l'apologie de crime de guerre. L'apologie de crime de guerre consiste dans la justification, la publication sur le net les crimes concernés.

Cyber- blanchiment. Le blanchiment d'argent est l'activité de dissimiler la provenance d'argent acquis par des manières illégales tels que les activités mafieuses, trafic de drogue, d'armes, extorsion, corruption ; fraude fiscales etc. en le réinvestissant dans des activités légales. Grâce au blanchiment, l'argent semble propre c'est-à-dire prend une apparence honnête. Cette forme de criminalité, n'a pas été prévue de façon précise comme une infraction cybercriminelle par le législateur Sénégalais, alors qu'elle peut constituer bel et bien une infraction cybercriminelle, dans la mesure où le délinquant peut utiliser les TIC pour effectuer un blanchiment d'argent. Cet argument a été approuvé dans un article qui estime que « *Le blanchiment d'argent connait de nouveaux développement depuis l'avènement d'internet. Pour cet auteur, les plateformes de jeu et de paris en ligne, qui sont vulnérables pour le blanchiment de capitaux et d'autres crimes financiers par la nature de leurs opérations, peuvent servir comme facilitateurs de blanchiment* »[154]. En effet, à l'appui de cet argument, un auteur estime que « *le blanchiment de capitaux ou d'argent est une activité en développement sur Internet* »[155].

A côte des infractions ci-dessus, le dispositif marque des insuffisances, dans l'omission de la responsabilité de certains acteurs d'Internet. Il s'agit entre autres, des exploitants de forums de discussion. Un forum de discussion peut être défini comme « *un service permettant à un individus de s'exprimer et de débattre librement sur un thème donné* »[156]. Le législateur

[153] TRHC Dakar du 19 juillet 2007, affaire résidence Saint James.com inédit. In bull. d'information de la cours suprême, n°7-8 p.137. note PAPA ASSANE TOURE.

[154] Cybercriminalité et blanchiment de capitaux sur internet, https://creobis.eu./blog/20015/08/07aml/, consultée le 29/06/2019 à 16h 12

[155] CRISTOPHE GUILLEMIN « Blanchiment des capitaux, nouvelles tendance de la cybercriminalité en 2006 », https://www.zddnet.net.fr, consultée le 15/10/2019 à 12h20

[156] PIERE PEREZ, « Forum de discussion et responsabilité », 2013 www.esen.education.fr, consultée le 29/06/2019 à 16h10.

Sénégalais n'a pas règlementé des conditions d'engagement de leur responsabilité. Une omission qui laisse apparaitre des doutes sur le régime juridique de leur responsabilité. Ce silence du législateur Sénégalais quant au régime de la responsabilité des exploitants de discussion, s'observe également en France où la jurisprudence est divisée sur la question. En effet, cette jurisprudence applique tantôt de régime juridique les fournisseurs d'hébergement, tantôt elle opte pour de régime juridique des éditeurs[157]. Face à ces difficultés d'identification du régime juridique applicables aux exploitants de discussion, le TGI de paris dans une décision rendue le 11 février 2003 a estimé que ces derniers « étaient à la fois éditeurs et hébergeurs »[158]. Là encore, cette décision ne permet pas de régler le problème car le régime de la responsabilité des fournisseurs d'hébergement et les éditeurs sont distinctes. Ce qui permet de revenir au même résultat, c'est-à-dire le choix entre le régime des éditeurs et celui des hébergements.

Ensuite nous pouvons citer, les créateurs de lien hypertexte ou d'hyperlien. Ici aussi le législateur n'a pas prévu de textes applicable aux conditions de la responsabilité de ces derniers. Toutefois l'imprévision des conditions de responsabilité des créateurs de lien hypertexte ou hyperlien ne fait pas obstacle à ce que leur responsabilité pénale soit engagée. Ils peuvent être poursuivis pénalement ou civilement pour atteinte au droit de la propriété intellectuelle notamment aux droits d'auteurs et aux droits des marques ou si leurs œuvres renvoient à des contenus illicites[159].

Enfin, le régime juridique de la responsabilité des fournisseurs d'outils de recherche (la responsabilité des moteurs de recherche**)** ne figure pas dans le dispositif de lutte contre la cybercriminalité du Sénégal. Le législateur semble ne pas aborder cette question, ni la jurisprudence Sénégalaise. Contrairement en France où cette dernière, qui dans une affaire qui a soulevé la question du régime de la responsabilité des moteurs de recherche, estime « *qu'ils peuvent être assimilés à des fournisseurs d'hébergement dès l'instant ou l'activité a un caractère purement technique, automatique et passif impliquant que ledit prestataire n'a pas la connaissance, ni le contrôle des informations transmises ou stockées* »[160].

[157] Affaire Père Noel, TGI Lyon du 28 mai 2002, https://www.legalis.net, consultée le 29/10/2019 à 13h58.
[158] TGI de paris, Affaire Yahoo du 11 février 2003, https://www.legalis.net, consultée le 29/10/2019 à 17h 09.
[159] LEON PATRICE SARR, *op. cit*.
[160] Cours de justice des communautés européennes(CJCE), arrêt du 23mars 2010 dans l'affaire dite Google AdWords, https://www.legalis.net, consultée le 29/10/2019 à 14h12

De même, le législation n'a pas envisagé les hypothèses des infractions sexuelles et de proxénétisme commises sur le net comme c'est le cas de la France où le législateur érige en infraction le cas où « la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication ». Il s'agit ici du délit de viol dont l'auteur de l'infraction a connu sa victime par l'utilisation du net. L'utilisation du net pour connaitre la victime constitue pour le législateur français une circonstance aggravante du viol.

Paragraphe II : Les difficultés relatives au cadre procédural.

Les difficultés relatives au cadre procédural se présentent d'une part au caractère transnational de la cybercriminalité (A) et d'autre part dans l'insuffisance des moyens humains et matériels pour faire face à la cybercriminalité(B).

A- Les difficultés lies au caractère transnational de la cybercriminalité.

Les difficultés s'observent non seulement dans l'application de la loi compétente en cas de conflit comportant un élément d'extranéité, mais aussi dans la recherche de la preuve.

Concernant l'application de la loi, notons que, La particularité de la cybercriminalité est le fait qu'elle ne touche pas seulement un pays bien déterminé car ses effet peuvent se sentir dans plusieurs Etats. La cybercriminalité *« a pour cible un territoire sans limite puisque la ou Internet est accessible, la criminalité l'est également* »[161]. Ainsi, la cybercriminalité est devenue aujourd'hui une délinquance transnationale, c'est pour cette raison qu'un auteur affirme que *« c'est dans l'espace en apparence virtuel, immatériel, universel, sans frontières, que des infractions pénales sont susceptibles d'être commises et qu'elles le sont effectivemen*t »[162]. Le critère transfrontalier de la cybercriminalité peut se justifie du fait que les auteurs, ou complices de l'infraction peuvent se trouver dans différents pays, et réalisés ensemble une infraction. Il en est ainsi, du fait que les éléments de preuve permettant d'inculper l'auteur de l'infraction peuvent se trouvent les divers pays. En sus, l'Internet est un réseau international qui fait intervenir plusieurs législations nationales qui sont susceptibles de s'appliquer à un conflit déterminé. Cela pose le problème de la compétence juridictionnelle des différentes Etats concernés par ce conflit.

[161] ROMAIN BOSS, *op.cit*., P.44.
[162] CHRISTIANE FERAL-SCHUHL, *Cyberdroit : le droit à l'épreuve de l'Internet*, Dalloz, 6e éd., 2011-2012, cité par ROMAIN BOSS, *ibid*. p.143.

Par ailleurs, *« le principe de la souveraineté interdit en principe, à la juridiction saisie du procès pénale d'exercer ses attributions en dehors de ses frontières et de recueillir elle-même dans un Etat étrangère les preuves* ».[163]En effet, les infractions commises en dehors du territoire d'un Etat ne sont pas en principe de la compétence du juge de cet Etat.

Beaucoup des pays ont opté pour le principe de la territorialité lorsqu'il existe un élément d'extranéité. On parle d'élément d'extranéité quand une infraction fait intervenir plusieurs pays entrainant par la suite un conflit de lois.

Le droit pénal Sénégalais n'est compétent que lorsque l'infraction est commise au Sénégal, on parle du principe de la territorialité. Ce principe s'appuie sur le lieu de la commission de l'infraction pour déterminé la loi compétente. En outre, « *Les règles nationales attributives de compétence législatives et juridictionnelles en matière pénale répondent en apparence aux nécessités de la répression, le principe étant celui de la solidarité de ces compétence* ».[164] « Il en est ainsi plus particulièrement *en cas d'application du critère de compétence territoriale, dès lors que l'infraction peut être localisée sur le territoire nationale, en totalité, ou en partie seulement* ».[165]C'est dans cet optique que, le droit sénégalais est compétent dans des cas où l'infraction est éclatée dans l''espace. Sont réputées commises sur le territoire de la République les infractions dont l'un des éléments constitutifs a lieu sur ce territoire.

Cet élément d'extranéité se manifeste également en matière de cybercriminalité grâce à l'universalité du réseau internet. « *L'universalité suppose l'accès universel à l'Internet, aux téléphones et en somme aux TIC »*[166].

En outre, il est à noter que l'internet est assujetti au respect des droits humains dont il constitue la base. *En effet « l'universalité de l'Internet permet de mettre en évidence l'harmonisation perpétuelle liant la croissance avec l'utilisation de l'Internet et l'application des droits de l'homme »*[167]. *Ce respect des droits humains a pour conséquence d'accès*

[163] OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME (UNODC), « La coopération internationale en matière pénale contre le terrorisme », New York, 2011, p.87.

[164] Ce principe signifie que le juge pénal saisi applique sa propre loi étatique, à l'exclusion de toute loi pénale étrangère. Voir : HENRI DONNEDIEU DE VABRES, Les principes modernes du droit pénal international, éd. Paris Sirey,1928, Editions Panthéon-Assas. Cité par ROMAIN BOSS dans la lutte contre la cybercriminalité au regard de l'action des Etats p.147.

[165] JACQUES FRANCILLON, «cybercriminalité aspects de droit pénal international », XIXe Congres International de Droit Pénal, Société de l'Information et du Droit Pénal, Colloque Préparatoire- Section 4, p.5

[166] UNESCO « UNISERVALITE DE L'INTERNET » : un outil pour la construction des sociétés du savoir et de l'agenda pour le développement durable post-2015, 2 septembre 2013 p. 1

[167] *Ibid*. p. 7.

librement de chaque personne à l'Internet[168]. En effet, selon un auteur, *« La cybercriminels, dans le cadre de leurs activités, sont liés entre eux par les supports informatiques et sont constitués en réseaux pouvant agir à partir de territoires différents*[169] ».

Aujourd'hui, la criminalité sur internet est étudiée en droit pénal international comme une manifestation de la criminalité transnationale, donc transfrontalière, malgré le fait qu'une infraction commise sur les réseaux ne peut présenter qu'un caractère national. C'est ce caractère national de l'infraction qui face au caractère transfrontalier de la cybercriminalité, pose un problème de compétence des différentes normes concernées par la même infraction. Et La recherche de la preuve dans l'Etat du lieu de commission de l'infraction peut poser de sérieuses difficultés.

Ainsi le fait que le droit pénal repose sur le principe de la présomption d'innocence, exige que la culpabilité du prévenu soit établie par des preuves suffisantes. Selon un auteur, « *la répression des infractions commises sur Internet, qui sont souvent à caractère internationale, est loin d'être satisfaisante à l'heure actuelle puisque des règles du droit pénal international classique déduits du principe de la souveraineté nationale en matière pénale et du principe de territorialité, constituent des entraves à l'efficacité de la répression* »[170]. L'élément l'extranéité rend complexe voire impossible, l'identification des auteurs de l'infraction ou l'application de la loi pénale.

Un autre problème survient lorsque l'infraction commise dans un pays déterminé n'a pas fait l'objet d'une règlementation dans le pays où se trouve l'auteur de l'infraction. En outre, du fait de la théorie de la souveraineté des Etats, ces derniers sont libres dans l'organisation de leur système répressif. Il y a donc *« une cohabitation au niveau international d'une multitude de règles propres à chaque pays* »[171].

En droit international, un comportement ne peut être jugé comme délictueux que s'il fait l'objet d'une répression bien établie et codifiée. En ce sens, le pouvoir de légiférer est un pouvoir exclusivement réservé au domaine étatique. Il émane d'une autorité unique qui est la seule à même de pouvoir déterminer les comportements répressibles. Le droit pénal

[168] UNESCO « Universalité de l'internet: un outil pour la construction des sociétés du savoir et de l'agenda pour le développement durable post-2015 », *op.cit*. p.7.
[169] PAPA GUEYE, *op. cit*. p.275.
[170] NICOLAS RONTCHEVSKY, « revue Internationale de Droit Economique », ed.de boeck, 2002, pp. 523-528.
[171] ROMAIN BOSS, *op. cit*. p. 144.

international peut être défini comme *« la branche du droit criminel ayant pour objet la répression des infractions présentant un caractère d'extranéité »*[172] Au nom de la souveraineté nationale, l'Etat se présente alors comme « *le seul maitre dans l'application de ses intérêts et dans l'élaboration des infractions punissables dont il entend assurer la protection ».*[173]*Ainsi, selon le droit pénal international, le juge répressif n'applique que sa propre loi nationale »*[174].Comme le précise un auteur « *En droit pénal international, le juge n'applique jamais que sa propre loi et il l'applique toujours comme loi normalement applicable au rapport de droit. Le juge d'un Etat quelconque ne sera jamais saisi de la répression du fait incriminé que si ce fait constitue un délit au regard de l'Etat au nom duquel il punit et au regard de la loi qu'il a pour mission d'appliquer : dans ces conditions, il ne frappera jamais son auteur que des peines que cette loi y attache* »[175].

Pour ce qui est de la recherche de la preuve, précisons que l'avènement de la cybercriminalité a pour conséquence le bouleversement des moyens traditionnels. Ceux-ci semblent inaptes, dans la recherche de la preuve des infractions immatérielles. Or, comme le dit Aloysins Bertrand *« Il y a pas de serrure dont le crime n'ait pas la clef* » Cette citation illustre l'interdiction fait aux juges de condamner une personne sans preuve de sa culpabilité. Ainsi, les difficultés dans la recherche de la preuve soulevées par la cybercriminalité se manifestent avant tout dans l'inadéquation de certaines dispositions du code de procédure pénale à la délinquance commise sur Internet. En effet, *« Les instruments dont disposent les officiers de police judiciaire dans la recherche des preuves des infractions n'ont pas été conçu au temps de l'univers numériques et dématérialisé, ni même adaptes à celui –ci* »[176]. Hors la cybercriminalité ne peut être combattue efficacement que lorsqu'il existe une adaptation des moyens d'investigation au numérique.

Le législateur Sénégalais a tenté d'apporter les réponses à ces besoins pour adapter les enquêtes à la cybercriminalité. Cette adaptation se manifeste, par la précision de la perquisition et de la saisie informatique, de l'interception de données, de l'admission de la preuve numérique, de la conservation rapide les données. Mais ces efforts semblent

---

[172] DIDIER REBUT, *Droit pénal international*, Précis Dalloz, 2e édition, 2014, p. 726.

[173] FANNY BINOIS, « La solidarité des compétences législatives et juridictionnelles en droit pénale international »,mem. université Jean-Momet, paris, 2012,p. 13.

[174] CLAUDE LOMBOIS, *Droit pénal international*, Précis Dalloz, 2eedition, 1979, p.478.

[175] ETIENNE-ADOLPHE BARTIN, « *Etude de droit international* », paris 1899, p.214, cité par ROMAIN BOSS, *op. cit*., p.184.

[176] TABAROT (M), rapport n° 608 (2ere partie) sur le projet de loi n 528 pour la confiance dans l'économie numérique,(2013), cité par ROMAIN BOSS, *ibid*.., p. 202.

insuffisants face au caractère international de la cybercriminalité, car les acteurs chargés des enquêtes ont une compétence nationale. En sus, « *les nombreuses possibilités techniques facilitant l'anonymat sur le réseau Internet, l'effacement des données, la complexité des faits, soulèvent de réelles difficultés pour les enquêteurs en matière d'établissement des preuves* »[177]. Par ailleurs, M Jean Domat définissait la preuve comme suit « *on appelle preuve ce qui persuade l'esprit de la vérité. (…).On appelle preuves en justice les manières réglées par les lois pour découvrir et pour établir la vérité d'un fait contesté* »[178]. Elle est également définie comme étant, « *une modalité particulière d'établissement de la vérité qui consiste à avoir recours à des moyens numériques divers et variés qui vont de l'étude des contenus dans les données d'un disque dur, aux messages électroniques, en passant par l'enregistrement numérique* »[179]. Pour faire face à ces difficultés liées à la souveraineté des Etats, il est nécessaire voire indispensable que les pouvoirs des organes chargés de l'enquête soient élargis au-delà des frontières nationaux. Cela peut être possible si l'on procède à un développement des moyens d'investigations numériques permettant de surmonter les limites frontalières.

Elargir cette possibilité de recherche au-delà les frontières des Etats semble être bénéfique pour lutter contre la cybercriminalité.

Malgré ces innovations en matière d'investigation, les difficultés sont toujours présentes. En effet, les difficultés peuvent être liées à la distance qui peut séparer l'Etat des poursuites et celui de l'arrestation[180].

De même, les difficultés peuvent être liées à la poursuite. Elle se manifeste par le fait que les cybercriminels utilisent les techniques d'anonymat et les techniques de cryptage pour masquer leurs identités et dissimiler leurs actes délictuels. De plus l'anonymisation qui caractérise en grande partie le réseau Internet, ne garantit en rien l'identité de celui qui est derrière le mail, la vidéo ou le site Internet, qui complique nécessairement la tâche des enquêteurs. L'anonymat et le cryptage qu'utilisent les cyberdelinquants laissent des conséquences dans la célérité en matière de collecte des preuves numériques.

---

[177] ROMAIN BOSS, *op. cit.* p.202.

[178] JEAN DOMAT, *Les lois civiles dans leur ordre naturel* paris, éd. cavalier, t1 1771, p.204, cité par ROMAIN BOSS, ibidem.

[179] MELANIE CLEMENT-FONTAINE, *op.cit.* p.11.

[180] ROMAIN BOSS, *op.cit*. p.203.

Par ailleurs, aux termes de l'article 51 du code de procédure pénale « *sauf réclamation faite de l'intérieur de la maison prévues par la loi, les perquisitions et visites domiciliaires ne peuvent être commencées avant cinq heures et après vingt- et- une heure* ». Cet article qui limite les heures de perquisitions et de visites domiciliaires peut entrainer une conséquence néfaste dans la collecte des preuves, car plus que le temps passe, plus l'infraction est difficile à prouver. De même la limitation des heures de perquisitions et de visites à domicile « *interdit la mise en œuvre des mesures tendant à la cessation du trouble à l'ordre public qu'elle constitue, quand bien même les autorités répressives compétentes en seraient informées, ce qui n'est guère satisfaisant* ».

Les difficultés procédurales dans la répression de la cybercriminalité se manifestent également dans l'insuffisance de moyens humains et matériels.

En somme, du fait de son caractère transnational, le cyber délinquance pose une difficulté aux enquêteurs qui se trouvent parfois dans l'impossibilité de rassembler des preuves contre les prévenus. Le principe de la souveraineté fait obstacle à l'intervention des enquêteurs hors lieu de compétence ou hors du territoire national sans autorisation de la part les autorités compétentes. Pour faire face à cette impuissance, il faut une coopération entre Etats. Ceci étant dit, il convient de mettre l'accent ensuite sur les insuffisante de moyens humains et matériels

B-L 'insuffisance de moyens humains et matériels.

La police judiciaire ainsi que le juge d'instruction ont vocation à perquisitionner et à saisir en ligne, au cours des investigations dont l'objet porte sur une infraction cybercriminelle. Ils doivent dans ce cas agir vite du fait que les indices et autres éléments de preuves à recueillir sur le réseau sont très volatiles[181]. Or c'est les mêmes acteurs qui sont chargés de mener des investigations aussi bien pour des infractions traditionnelles que pour les infractions cybercriminelles. Le manque de compétence spécialisée peut avoir pour conséquence, la lenteur dans la procédure d'investigation. Et souvent, plus l'investigation dure, plus on a une faible possibilité d'appréhender l'auteur de l'infraction car les preuves risques de disparaitre, autrement dit de dépérir. Ainsi la lutte contre la cybercriminalité, nécessité la disposition

[181] 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 pour l'obtention du Diplôme d'Etude Approfondie(DEA), 2006-2007. https://www.memoireonline.com. Consultée le 13/ 10/2019 à 10h11.

d'une importante force en capital humain, c'est-à-dire en ressource humaine dans le cadre des investigations.

Les pays sous-développés de par leur manque de moyens matériel et humains n'ont pas les capacités pour combattre la cybercriminalité vue qu'elle constitue un phénomène délicat et qui nécessite un certain moyen matériel. Par régler ce problème, il faut un renforcement des ressources humaines dans le cadre de la lutte contre la cybercriminalité. Renforcement qui selon Monsieur Adama Ouane doit avoir pour objet de «*construire des parcours professionnels associés à de l'expertise de haut niveau. Ces expertises devront remplir plusieurs fonctions :*

- *Participer à la connaissance et à l'anticipation de la menace cyber et à la maitrise des risques ;*
- *Soutenir la lutte contre les cyberattaques, notamment dans le contexte de la lutte contre la cybercriminalité, la protection des infrastructures critiques et des équipements, des structures d'importances vitale ;*
- *Offrir les outils et les connaissances nécessaires à toute la chaine des acteurs de la justice pénale dans le domaine de la lutte contre la cybercriminalité ;*
- *Collaborer au développement et à l'évaluation de produits et de solution de cybersecurité et de cyberdefense ;*
- *Participer à l'ingénierie de la cybersécurité, en particulier dans le domaine de la conception et lors de la mise en œuvre de moyens techniques (chiffrement, pare-feu, détection d'incidents,…) ;*
- *Apporter les processus, procédures et contrôles nécessaire à la gouvernance, à la gestion opérationnelle l'évaluation et à l'optimisation des mécanismes de sécurité ;*
- *Proposer le soutien nécessaire à la prise en compte et à la satisfaction des besoins juridiques et managériaux et d'intelligence économique*
- *Encourager des actions de sensibilisation et de formation de la population*
- *Contribuer à l'animation et au développement de la recherche et de la formation : en assurant le lien entre les centres de formation et de la recherche et les entités de l'économie numérique, pour innover, créer de la valeur et contribuer à résoudre les problèmes auxquels la société est confrontée*

- *Organiser des exercices de simulations bilatérales et régionales de réponse aux menaces et aux attaques dans les secteurs de la cyberpolice, de la cybersecurité et de la cyberdéfense*
- *Développer les cursus de formation académique et professionnelle afin de mettre rapidement sur le marché les compétences indisponibles* »[182].

Cette proposition faite par Adama Ouane nous semble intéressante. En effet, pour améliorer cette insuffisance, il a été créé au Sénégal une Ecole à vocation régional(ENVR) située à Dakar et inaugurée le 6 novembre 2018, dans le but de former les organes chargés de l'enquête. Mais cela s'avère insuffisant, en effet, la cybercriminalité est présente partout dans le pays, et il est nécessaire de former un nombre considérable de personnes. Pour cela il faut les moyens matériels et financiers. Or le Sénégal à l'heure actuelle, ne semble pas disposer de ces moyens. La cybercriminalité implique un tout nouveau mode de travail, sur lequel les saisies sont très souvent au format numérique. En ce sens, les agents qui opèrent en tant que police investigateur en cybercriminalité doivent être particulièrement familiarisés avec l'outil informatique et le maitrise à la perfection.

Pour atteindre cet objectif, les Etats et surtout les Etats Africains en particulier le Sénégal, doivent favoriser une coopération avec les Etats en développement pour plus d'expérience dans la lutte. En effet, le manque de coopération entre les Etats développés et Les Etats en voie de développement aggrave la situation de ces derniers. Ainsi, les Etats en voie de développement doivent bénéficier d'appui matériel et de partage d'expérience par voie d'assistance et l'appui technique de la part les Etats développés leurs permettant de mener à bien leurs enquêtes[183]. C'est dans ce contexte que les Etats-Unis ont mis en place un groupe d'expert intergouvernemental ayant un contrat à durée indéterminée, lors du 13eme congrès sur le crime[184].Selon Mme Loide LUNGAMENI, «*l'objectif principal du programme est de répondre aux besoins identifiés dans les pays en développement en soutenant les Etats membres à prévenir et à combattre la cybercriminalité* »[185]. Ces congres ont pour vocation le

[182] ADAMA OUANE, *op. cit*. p.53 à 54.
[183] ROMAIN BOSS, *op cit*.p.355.
[184] 13eme congre des Etats-Unis pour la prévention du crime et la justice pénale, Doha(qatar),12-19 Avril 2015.
[185] DOHA : l'ONU et ses partenaires mettent l'accent sur leurs efforts pour combattre la cybercriminalité : Disponible sur : https://.news.un.org, consultée le 23/10/2019 à11h10.

prolongement et l'amélioration de la coopération internationale pour lutter contre la criminalité transnationale organisée[186].

Dans cette même optique, le Sénégal, a mis en place une Brigade spéciale de lutte contre la cybercriminalité, qui est l'équivalent de la plateforme de lutte contre la cybercriminalité en Côte-d'Ivoire[187]. La mission de la brigade consiste essentiellement dans la conduite d'enquêtes judiciaires portant sur les infractions visant ou utilisant des systèmes informatiques. Cette brigade est spécialisée dans des affaires portant sur la cybercriminalité. Cette spécialisation constitue un avantage considérable dans la recherche des preuves et l'identification des auteurs de ces infractions, en favorisant la célérité des enquêtes. Mais pour plus de rigueur, il serait préférable que plusieurs brigades spéciales de lutte contre la cybercriminalité soient construites. Au moins une pour chaque région du Sénégal et de décentraliser les tâches.

Vu l'évolution de la cybercriminalité, une seule brigade s'avère insuffisante.

La cybercriminalité trouve de plus en plus d'ampleur dans le pays, et pour cela il faut renforcer les personnes chargées de la recherche des preuves et de l'identification des auteurs, pour la création au niveau de toutes les régions du Sénégal, une brigade spécifique en la matière. Face aux difficultés ainsi soulevées, il est nécessaire qu'une solution soit mise en place pour renforcer le dispositif.

Il est nécessaire pour une meilleurs lutte contre la cybercriminalité de décentraliser la brigade spécifique en la matière à travers le pays pour faciliter la rapidité dans l'investigation. Une brigade spécifique dont le siège se trouve à Dakar, n'est pas mal, mais ne suffit pas.

Agir sur les réseaux suppose que les services de police judicaire disposent d'une connexion à Internet[188], Or la situation actuelle de l'Afrique marque une insuffisance de ressources financières pouvant combler ce besoin.

Section II : La nécessite de renforcer de dispositif

Le dispositif doit être renforcé en tenant compte aussi bien le cadre substantiel (paragraphe I) que le cadre procédural (paragraphe II).

[186] ROMAIN BOSS, *op.cit.* p.356.
[187] ANMONKA JEANINE-ARMELLE TANO-BIAN « « La répression de la cybercriminalité dans les Etats de l'Union Européenne et de l'Afrique de l'Ouest, Thèse, Université de Paris Descartes, 28mai 2015, p.268
[188] KABORE ANATOLE, *op.cit.*

Paragraphe I : Une amélioration du cadre substantiel.

En raison du caractère transnational et délocalisé de la cybercriminalité, le Sénégal a besoin d'un instrument juridique à la fois sous régional (A) et international (B) pour mieux lutter contre la cybercriminalité. C'est dans ce sens qu'un auteur déclare que « la criminalité sur Internet est un problème mondial (…) qui nécessite les mesures mondiales, un travail international mieux coordonne et surtout, des normes minimales obligatoires »[189].

A- La nécessité de renforcer de dispositif par une coopération sous-régionale.

La lutte contre la cybercriminalité nécessite pour son efficacité une collaboration d'Etats. C'est ainsi que l'Union africaine, étant consciente de cette exigence, les ministres en charge des TIC ont proposé un Projet de Convention de l'Union africaine sur la confiance et la sécurité dans le cyberespace, intégrant des dispositions relatives à la lutte contre la cybercriminalité .Selon ces ministres, « *la criminalité transnationale organisée, et notamment la cybercriminalité, entravent sérieusement le développement économique de l'Afrique* ». D'où la nécessité pour ces Etats africaines de trouver des solutions permettant de neutraliser ce phénomène. L'expression de cette volonté de lutter contre la cybercriminalité a évolué grâce à plusieurs déclarations, que sont la Déclaration d'Abidjan du 22fevrier 2012[190], la Déclaration d'Addis-Abeba du 22 juin 2012[191] adoptant le projet de loi sur l'harmonisation des cyber-sécurité en Afrique et la déclaration de Khartoum AU/CITMC-4/MIN/Décl. (IV) du 06 septembre 2012.[192]La mise en œuvre de ces directives a permis d'appréhender la répression de la cybercriminalité sous la forme d'une convention sur la cyber-sécurité, d'où le projet de l'Union africaine sur la cyber-sécurité. Ce projet a pour objectifs principaux « l'élaboration d'une politique d'adaptation des incriminations nouvelles spécifiques aux TIC, la mise en place des sanctions et l'adaptation du régime de responsabilité en vigueur[193].En outre, maitre Lionel Kalina a envisagé l'élaboration d'une politique régionale adéquate de prévention et de lutte contre la cybercriminalité[194]. Selon lui, cette démarche passe par une « *convocation d'un sommet africain de prévention et de lutte contre la cybercriminalité,*

[189] GERHARG SCHÖDER, cite par Romain BOSS, *op. cit.* p. 215
[190] Déclaration d'Abidjan du 22 février 2012.
[191] Déclaration d'Addis-Abeba du 22juin 2012.
[192] Déclaration de Khartoum du 06 septembre 2012.

[194] LIONEL KALINA « Cybercriminalité : quels outils pour l'Afrique ?- Cybzercriminalité.blogg.org, consultée le 13/10/2019à 16h30.

lui seul disposerait de l'autorité et la légitimité nécessaire pour fédérer les différentes initiatives concurrentes et imposer une démarche collective ».[195] Ainsi selon l'avocat Patrick Amazou « *la cybercriminalité transcende les frontières et les régions. Apporter des réponses pays par pays sera vain. Il faut des solutions régionales* »[196].Face à la nécessité d'une union pour combattre la cybercriminalité, l'union Africaine a signé une convention sur le cyber sécurité et la protection des données à caractère personnel le 27juin 2014. Cette convention prévoit que « chaque Etats partie s'engage à adopter des mesures législatives et/ou règlementaires pour identifier les secteurs considères comme sensibles pour sa sécurité nationale et le bien-être de l'économie ». La convention vise à « renforcer et harmoniser les législations actuelles des Etats membres et des communautés économiques régionales(CER) en matière de TIC, dans le respect des droits libertés fondamentales et des droits de l'homme et des peuples, ainsi qu'à créer un cadre normatif approprié correspondant à l'environnement juridique, culturel, économique et social africain »[197].

Malgré cette initiative, la convention de l'Union africaine est passée à l'échec du fait que beaucoup de pays africains se sont abstenus de la ratifier. Sur 55 pays, seulement14 pays l'ont ratifié. Il s'agit du Benin, Tchad, Comores, Congo Ghana, Guinée-Bissau, Mauritanie, Sierra Leone, São Tomé-et-Prince, Zambie, Sénégal, et l'Ile Maurice. Cette méfiance de la part des Etats Africains fait obstacles à la lutte contre la cybercriminalité, car selon Patrick Amadou *« pour la lutte contre les cyber attaques, la solution doit être globale »*[198]. Pour lui l'abstention des Etats Africains quant à la convention se justifie par le fait que « *une coopération régionale laisse entendre une perte d'influence pour ls Etats et cela est dur à accepter pour la plupart d'entre eux* ». « *Les Etats ont peur de perdre leurs souveraineté* ». A notre avis nous pensons que la convention de l'union africaine bien que pouvant heurter la souveraineté des Etats membres est indispensable pour mettre fin aux cyberattaques. Vue son caractère transnationale. Il est donc plus cohérent de perdre une partie de sa souveraineté pour garantir sa sécurité que de garder toute sa souveraineté et vivre dans l'insécurité. Les Etats doivent faire beaucoup plus d'effort allant dans ce sens. D'abord en ratifiant la convention, ensuite en respectant tous les engagements pris par la convention. Pour un auteur, *« un*

[195] LIONEL KALINA, *op.cit*.

[196] Cybercriminalité : comment l'Afrique essaie de se défendre-Le point, http : //www. Le point.fr, consultée le 23/07/2019 à10h 30.

[197] L'Afrique se met en ordre de bataille contre la cyberveillance et de la cybercriminalité : http://cio-mag.com, consultée le23/07/2019 à 15h12.

[198] PATRICK AMAZOU, Cybercriminalité: comment l'Afrique essaie de se defender, www.osiris.sn. Cybercriminalité-com, consultée le 28/10/2019 à 19h35.

instrument africain de prévention et de lutte contre la cybercriminalité présente le mérite de favoriser l'harmonisation des stratégies de lutte contre la cybercriminalité dans les Etats membres et d'impulser une coopération juridique et judiciaire entre les Etats. Ce projet aura eu le mérite « politique » de constituer un instrument juridique contre la cybercriminalité élaboré et mis en œuvre par des Africains »[199]. Cette solution nous semble favorable.

A côté de l'Union Africaine, la CEDEAO a elle aussi à travers une directive c/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espèce de la CEDEAO, envisagé des incriminations ainsi que des sanctions visant à lutter contre la cybercriminalité dans cet espace. Pour la CEDEAO « la cybercriminalité est un phénomène nouveau qui nécessite la définition des infractions spécifiques, lesquelles doivent être rattachées consubstantiellement aux infractions classiques, tels que le vol, l'escroquerie, le recel, le chantage en raison de la nature du préjudice cause au moyen de l'utilisation de l'Internet »[200]. C'est ce qui a motivé la CEDEAO à avoir l'idée « d'adopter un cadre de répression pénale en vue de lutter efficacement contre la cybercriminalité, ainsi que de permettre une coopération appropriée en raison de la gravité des préjudices qu'ils engagent »[201]. Cette directive s'applique dans le domaine tels que les atteintes aux systèmes informatiques, les atteintes aux données informatiques, atteintes portant sur le contenu, les atteintes portant sur les logiciels et programmes informatiques, infractions de presse commises par des moyens de communication électronique, la responsabilité des personnes morales autre que publiques, l'usage de données falsifiées, disposition d'un équipement pour commettre des infractions, participation à une association formées ou à une entente en vue de commettre des infractions informatique. Cette directive va s'appliquer dans tous les pays membres de la CEDEAO, ce qui aura pour conséquence une identité dans l'incrimination de certains comportements. De même, la CEDEAO à mise en place un acte additionnel portant sur la protection des données à caractère personnel[202].

En fin, dans l'espace UEMOA, on note à des efforts tentant à lutter contre la cybercriminalité. Il s'agit de loi uniforme relative à la répression des infractions en matière de chèque, de carte bancaire et autres instruments et procédés électroniques de paiement[203]. Cette loi régit le système de paiement dans l'ensemble des pays membres de l'UEMOA. Les systèmes de

[199] PAPA ASSANE TOURE, *op. cit.* P. 473.
[200] Directive C/DIR/08/11 du 19 Aout 2011portant lutte contre la cybercriminalité dans l'espèce CEDEAO.
[201] *Ibidem.*
[202] Acte Additionnel du 2 octobre 2009 relative à la protection des données à caractère personnel dans l'espace CEDAO
[203] Loi uniforme n° 2008-48 du 3 septembre 2008 relative à la répression des infractions en matière de chèque, de carte bancaire et autres instruments et procédés électroniques de paiement.

paiement sont encadrés par des normes qui ont un lien direct avec la cybercriminalité. Il en est ainsi de la fraude aux cartes bancaires, interception frauduleuses des données bancaires, escroquerie en ligne etc.

Malgré ces dispositions favorables à la répression de la cybercriminalité, on note certaines difficultés liées à l'harmonisation des incriminations et des peines. Ces difficultés trouvent leur source dans le retard de l'édiction des normes coercitives. Cette lenteur se justifie par un manque de coordination des politiques de lutte contre la cybercriminalité. En effet *« les Etats de Afrique de l'ouest ne mènent pas la recherche de solution à la cybercriminalité de manière coordonnée car laissant chaque Etat l'avancer à son rythme en privilégiant le domaine qui lui semble prioritaire par rapport à ses population aux demandes et aux réalités* »[204]. Cela peut entrainer un décalage temporel important entre les dates d'éditions, qui pouvaient être différentes d'un Etats membre à un autre. Il se peut aussi qu'il y ait des vides juridiques dans certains Etats entrainant par la suite une absence d'incidence des peines déjà prononcées par un juge. En effet, *« Cette absence d'incidence de condamnation d'un criminel à l'étranger sur une peine prononcée dans le nouvel Etat de commission d'une infraction donnée est une limite à l'efficacité des sanctions contre la cybercriminalité »*[205]. Ainsi, l'auteur estime que « *cette question soulevée peut être résolue par les procédures d'exéquatur qui favorisent la reconnaissance des décisions de justice généralement et peines en particulier rendues par le juge d'un Etat. Le problème pourrait également être règle avec les conventions multilatérales ou plus souvent bilatérales signes en matières de coopération de police judiciaire* »[206].

Par ailleurs, nous pouvons noter que l'hypothèse concernant l'exéquatur sera difficile à admettre, car droit pénal est gouverné par le principe de la légalité des délits et peines. Cela soulève la question de savoir est ce qu'il est possible pour un Etat d'accepter une décision de justice tentant à condamner un comportement, que cet Etat même n'a pas prévu et sanctionné pénalement ? Ou l'application d'une peine non prévue par la loi de l'Etat concerné ?

Face à la dimension de la cybercriminalité, il sera quasi- totalement impossibles pour lutter efficacement contre ce phénomène, de se limiter aux dispositions nationales ou sous-régionale. Vu sa dimension internationale, il est nécessaire, de mettre en place une coopération internationale dont l'objectif principale est de lutter contre la cybercriminalité.

---

[204] ANMANKA JEANINE-ARMELLE TANI-BIAN, *op. cit.* p.333.
[205] *Ibid*. p.334
[206] *Ibidem*.

B-La nécessité de renforcer le dispositif par une coopération internationale.

Etant un problème transnational, il est nécessaire, pour lutter contre ce phénomène une coopération des Etats. En effet, le caractère transnational de la cybercriminalité nécessite une réunion les forces, les différents Etats pour empêcher d'une infraction soit dans l'impunité occasionnée par les obstacles liés à leur souveraineté.

Dans le cadre de la coopération, certains Etats sont déjà sur le point, c'est le cas de la convention de Budapest[207]. Adoptée, le 23novembre 2001, elle constitue le premier traité international à avoir définie la cybercriminalité. Les infractions désignées dans cette convention sont : les atteintes à la propriété intellectuelle et aux droits connexes[208], les infractions informatiques tels que la falsification informatique et la fraude informatique[209], la pornographie enfantine[210], *« les atteintes à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques »*[211]. Son objectif est d'apporter une solution sur la compétence territoriale des Etats en matière de cybercriminalité. Cette convention a été ratifiée par 35pays membres de l'UE et par les Etats-Unis (à l'exécution de la Russie et de la chine qui ont refusé de l'adopter) Selon l'article 22 de la convention chaque Etat doit adopter des mesures législatives nécessaires pour établir sa compétence à l'égard des infractions prévues par ladite convention « *lorsque l'infraction est commise :*

- *Sur son territoire ;*
- *à bord d'un navire battant pavillon de cette partie ;*
- *à bord d'un aéronef immatriculé dans cette partie*

par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relevé de la compétence territoriale d'aucun Etat »,(ou) « pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, §1 de la présente convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre parties au seul titre de sa nationalité, après une demande d'extradition »[212]. En effet, « *La convention de Budapest a établi deux critères de*

[207] CONVENTION DE BUDAPEST sur la cybercriminalité du 23novembre 2001.
[208] ART. 10.
[209] ART.7 et 8.
[210] ART. 9.
[211] ART. 2, 3, 4, 5, et 6.
[212] ART. 22.

rattachement de la compétence à savoir : celui de la territorialité et le critère tiré de la nationalité de la victime »[213].

Toutefois, selon M. Papa Assane Touré, la convention de Budapest présente des difficultés d'application dans le cadre d'un conflit positif de compétence. Il y conflit positif lorsque plusieurs tribunaux revendiquent leur compétence sur une affaire bien déterminée. *Toutefois, il soutient que « l'article 22, §5 de la convention à tenter de résoudre ce problème en disposant que « lorsque plusieurs parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente convention, les parties concernées se concertent, lorsque cela est opportun, afin de décider quelle est celle qui est la mieux à même d'exercer les poursuites* »[214].

L'adhésion à la convention de Budapest présente un avantage pour les pays membre de lutter efficacement contre la cybercriminalité.

En outre, en France, il existe les organismes multilatéraux dont la finalité est basée sur la sécurité des systèmes d'information. Entre autres nous pouvons citer l'exemple de L'OTAN (Organisation du Traité de l'Atlantique Nord). Cet organe a pour objectif principale, de veiller sur le cyber défense. C'est une organisation qui a pour vocation d'organiser la sécurité d'une région géographique, elle regroupe 56Etats dont certains en Amérique du Nord, en Asie, et en Europe. En effet, il s'agit d'un moyen d'alerte précoce ; de prévention des conflits ; de gestion de crises et de relèvement post-conflit. Toutefois, il faut signaler que le Sénégal, dans le cadre des conventions internationales, à seulement adhère à la convention de Budapest. Nous estimons qu'il serait avantageux pour le Sénégal d'être membre de cette organisation pour bénéficier d'une sécurisation. Par ailleurs nous ne pouvons pas atteindre l'objectif recherché dans la répression de la cybercriminalité sans pour autant procéder à une amélioration du cadre procédural.

Paragraphe II : Un meilleur encadrement du cadre procédural.

Cette amélioration du cadre procédural doit se faire par l'élargissement des pouvoirs des organes chargés de l'enquête(A) et par une procédure de prévention qui se manifeste par la sensibilisation(B)

[213] PAPA ASSANE TOURE, *op. cit*. p.507.
[214]PAPA ASSANA TOURE, *ibid*. p.507.

A-Elargissement des pouvoirs des organés charges de l'enquête.

Le besoin d'élargir les pouvoirs des organes chargés de l'enquête se ressent aussi bien au niveau national qu'au niveau international.

Au niveau national, le législateur a trouvé la nécessité d'étendre les pouvoirs des organes par le rajout de certains actes de poursuites. En effet, c'est à travers la loi N°2016 du 08 novembre 2016, modifiant la loi n° 65-61 du 21 juillet1965 portant Code de procédure pénale, qu'il a procédé à « un renforcement des pouvoirs du juge d'instruction et des prérogatives de l'officier de police dans la collecte des preuves en cas d'infraction en matière de cybercriminalité[215]. Ce renforcement des pouvoirs des organes chargés de l'enquête se manifeste à travers les articles 90-4, 90- 10 et 90-11.

Aux termes de l'article90-4 « Le juge d'instruction ou l'officier de police judiciaire agissant sur délégation judiciaire, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la perquisition ou des services qui permettent de protéger ou de crypter des données qui sont stockées, ou transmise par un système informatique, de fournir des information sur le fonctionnement de ce système et sur la manière d'y accéder un d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compressible ».En plus, l'article 90-10 permet au juge d'instruction ou l'officier de police judiciaire sur délégation judiciaire ou pendent l'enquête sur autorisation ou sous le contrôle du procureur de la République d'utiliser un logiciel à distance et l'installer dans le système informatique du mis en cause afin de recueillir les éléments de preuve pertinents utiles à l'instruction ou à l'enquête. Ils peuvent également et si la nécessite de la recherche des preuves l'exige, utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu des communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou enregistrer, en application des moyens techniques existant, ou prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatiques[216].

De même l'article 10 de la loi n° 2016-33 du 14 décembre 2016 relative aux services de renseignement estime que « Les services spéciaux de renseignement peuvent, lorsqu'ils

---

[215] ASTOU DIOUF « Etude critique de la Stratégie Nationale de cyber sécurité du Sénégal », avril 2019, http://jonction.e-monsite.com, consultée le 13/09/2019 à 16h13.

[216] Article 90-11 issu de la loi n°2016-29 du 08 novembre 2016 modifiant la loi n°65-60du 21juillet 1965 portant Code de procédure pénale. (JORS n°6975).

disposent d'indices relatifs à l'une les menaces prévues à l'article 2 et à l'absence de tout autre moyen, recourir à des procèdes techniques, intrusifs, de surveillance ou de localisation pour recueillir les renseignements utiles à la neutralisation de la menace ». A travers ce texte, le législateur permet au service de renseignement de procéder à une infiltration, géolocalisation pour empêcher ou neutraliser une menace. « Ce renforcement se manifeste par le développement de nouvelles techniques mises à la disposition des investigateurs, inaugurées par les fameuses écoutes téléphoniques, la géolocalisation »[217].

En plus de ces dispositions nationales qui viennent renforcer les pouvoirs les organes chargé de l'enquête en matière de cybercriminalité, on peut ajouter comme moyen de renforcer la lutte contre ce phénomène, les conventions sous- régionaux et la coopération internationale sur la cybercriminalité

Pour ce qui est les conventions sous -régionaux, nous pouvons citer, la convention relative à l'extradition judiciaire en matière pénale[218]. Et celle relative à l'extradition signée à Abuja le 06 Aout 1994.

Concernant la coopération internationale, elle se manifeste à travers la Convention des Nations Unies contre la criminalité transnationale organisée(CTO). Toutefois, cette convention ne concerne que les crimes organisés, or la cybercriminalité n'a pas forcément un caractère de crime organisé. Il peut être le fruit d'une seule personne. Cette observation constitue une limite de la convention. Mais cette limite ne peut empêcher à ce que la convention soit bénéfique à la lutte contre la cybercriminalité, dans la mesure où elle peut revêtir un caractère de crime organisé. En effet, la plupart des infractions cybercriminelles sont perpétrées par plusieurs personnes qui forment un réseau. Ainsi, selon l'article 3 de la convention, « La présente convention s'applique, sauf disposition contraire, à la prévention, aux enquêtes et aux poursuites conservant : les infractions établies conformément aux articles 5, 6, 8 et 23 de la présente convention ; les infractions graves telles que définies à l'article 2 de la présente convention, lorsque ces infractions sont de nature transnationale et qu'un groupe criminel y est impliqué ». Elle constitue un avantage pour les Etats parties à travers la possibilité d'une demande d'entraide, « Les Etats parties s'accordent mutuellement l'entraide judiciaire la plus large possible lors des enquêtes, poursuites et procédures judicaires concernant les infractions visée par la convention et comme prévu à l'article 3 de la

[217] THIERNO AMADOU NDIOUGOU, *op.cit.,* p.8

[218] Convention relative à l'extradition judiciaire en matière pénale signé à Dakar, le 29juillet 1992.

convention s'accordent réciproquement une entraide (…) le produit, les éléments de preuves de ces infractions se trouvent dans l'Etat partie requis et qu'un groupe criminel organise y implique »[219].

L'adhésion de la Convention des Nations Unies contre la criminalité transnationale organisée permettra au Sénégal de se lancer plus efficacement dans la lutte contre la cybercriminalité.

A côté de la convention des Nation Unies, le renforcement des pouvoirs des organes chargés de l'enquête, peut se manifester à travers la convention du conseil de l'union Européenne sur la cybercriminalité encore appelée convention de Budapest. Cette convention ratifiée par le Sénégal en 2016, a prévu des cas d'entraide judicaire et d'extradition. L'article 23 de la convention dispose « Les parties coopèrent conformément aux disposition du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leurs droit national, dans la mesure la plus large possible les unes avec les autres, aux fins d'investigation ou de procédures concernant les infractions pénales liées à des systèmes et donnes informatiques ou pour recueillir les preuves sous formes électronique d'une infraction pénale[220]. L'extradition s'applique aux infractions prévues aux articles 2à 11 à conditions qu'elles soient punissables dans la législation des deux Etats parties, par une peine privative de liberté pour une période maximale d'un an au moins.IL y a là une exigence de la réciprocité des incriminations entre les Etats Parties comme condition préalable à l'extradition. Nous pouvons déduire à cet effet que l'absence de réciprocité de l'incrimination rendrait impossible toute demande d'extradition. Ces conventions d'extradition ci-dessus peuvent servir de complément à la loi Sénégalaise du 28decembre 1971 relative à l'extradition[221].

En ce qui concerne l'entraide elle est prévue par l'article 25 de la convention .Cet article prévoit à son alinéa 1 que « Les parties s'accordent l'entraide la plus large possibles aux fins d'investigation ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir les preuves sous formes électronique d'une infraction pénale ».

[219] ART. 18, de la convention relative à l'extradition judiciaire ; *op. cit.*
[220] ART. 23 de la convention du conseil de l'Europe sur la cybercriminalité.
[221] Loi n°71-73 du 28decembre 1971 relative à l'extradition.

Du fait de ces conventions, le Sénégal sera en mesure de se protéger plus efficacement contre des actes de malveillance commis à travers des TIC.

Les pouvoirs des organes chargés de l'enquête peuvent aussi être élargis par le renforcement des moyens d'investigations tels que la possibilité de faire des perquisitions de nuit et par le renforcement des techniques d'enquête par la possibilité de procéder, à côté de la géolocalisation, à une infiltration et à une captation de données informatiques comme c'est le cas en droit français, qui par la technique du captage de données prévoit la mise en place d' *« un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des donnes informatique, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatise de données ou telles qu'il les y introduit par saisie de caractères* »[222]. L'infiltration policière désigne *« le fait, pour un officier de police judiciaire spécialement habité et agissant sous la responsabilité d'un officier de police judiciaire de coordonner l'opération, de surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer auprès de ces personnes comme un de leurs coauteurs, complices ou receleurs* »[223]. Cependant des techniques de la géolocalisation et de l'infiltration ne doivent être utilisées que pour des infractions cybercriminelles les plus graves telles que des atteintes à la sécurité de l'Etat et les atteintes aux personnes comme dans le cas du cyberterrorisme.

Ces procédés de renforcement des pouvoirs des organes chargés de l'enquête que sont la géolocalisation, l'infiltration ou la captation de données informatiques ne, doivent à notre avis être possibles que dans les cas les plus dangereux à la sécurité des citoyens et de l'Etat. Cette proposition est due, au fait que ces procédés sont souvent attentatoires de la vie privée les personnes concernées.

B- La nécessité d'allonger les délais de prescription de l'action publique et de la garde à vue en matière de cybercriminalité.

Les difficultés dans la recherche de la preuve en matière de cybercriminalité, causées par l'anonymat et le caractère transnational de la cybercriminalité, font ressentir le besoin d'allonger les délais de prescription. Le silence de la loi sur la cybercriminalité concernant les

[222] ART. 23 du projet de loi d'orientation et de programme pour la performance et la sécurité intérieure, assemblée nationale du 27mai 2009, www.assemblee-nationale.fr, consultée le 29/A10/2019 à 15h46.
[223] ART. 706-81 du CPPF de la loi n°2004-204 du 9mars 2004, issue du projet de loi portant adaptation de la justice aux évolutions de la criminalité.

délais de prescription laisse présumer l'application des délais de prescription de droit commun à la cybercriminalité.

En effet, vu la spécificité de la cybercriminalité, il est nécessaire que des délais spécifiques soient prévues en la matière. Ainsi, les délais de droit commun semble être inadéquats dans un milieu où la procédure est dominée par le caractère immatériel des techniques de poursuites et de la preuve numérique. Cette adaptation du droit procédural devait s'étendre aux délais de prescription de l'action publique, par un allongement de ces délais. Cette proposition visant à allonger des délais de prescription de l'action publique en matière de cybercriminalité, serait un avantage pour les enquêteurs qui disposeront beaucoup plus de temps dans la recherche de l'infraction et dans d'identification de son auteur.

La prescription étant par définition, l'écoulement d'un délai au-delà duquel les poursuites ne peuvent être possibles, fait obstacle dans certaines circonstances, la répression de l'auteur de l'infraction. En effet, le caractère transnational de la cybercriminalité rend complexe l'exerce de certaine poursuites dans la mesure où le principe de la souveraineté n'accorde pas à un Etat de s'immiscer dans le territoire d'un autre Etat, dans le but de la recherche les preuves, sans le consentement préalable de l'Etat duquel les preuves doivent être collectées. Par conséquent, « *si la preuve pénale est impossible à établir, tout le droit pénal est alors voue* »[224] à l'échec et dans ce cas, la personne soupçonnée peut être poursuivie. En effet, la personne soupçonnée peut ne pas être poursuivie avant la prescription de l'action publique, si les organes chargées de l'enquête ne trouvent pas d'autres moyens de prouver son culpabilité.

Le but de la prescription qui consiste à garantir la paix et la sécurité, par l'oubli ou le pardon, n'éteinte pas toujours cette objectif si n'inertie les poursuites ne dépend pas de la personne poursuivante ou du Ministère publique, mais d'une impossibilité des poursuites indépendante de leur volonté.

Concernant la garde à vue, c'est une mesure qui permet à la police de « *retenir une personne contre laquelle il existe une ou plusieurs raison paisible de soupçonner qu'elle a commis ou tenté de commettre une infraction* »[225], à sa disposition pendant un temps bien déterminé par la loi. Elle a par objet de facilité des enquêtes et l'audition de la personne gardée à vue. Elle permet aussi de contrôler la personne en évitant qu'elle prenne la fuite.

En droit commun, la garde à vue se déroule dans des conditions fixées par la loi.

Ainsi, la garde à vue ne peut excéder en principe 24heures. Toutefois, ce délai peut être prolongé de 24 heures si les besoins de l'enquête l'exigence c'est-à-dire s'il existe chez la personne gardée à vue des indices graves et concordants de nature à motiver son inculpation.

De même, la garde à vue peut être allongée à nouveau pour un délai de 48ans sur l'autorisation du Président de la République, son délégué ou le juge. Mais cette mesure ne peut être possible que pour les infractions les plus graves tels que les atteintes à la sureté de

[224] ROMAIN BOSS, *op. cit*. p.183.
[225] ERIC OK « La preuve numérique, Un défi pour l'enquête criminelle du 21e siècle », article, publié dans « Cahiers du numérique », 2003/3 Vol. 4 p. 205 à 217.

l'Etats, pour des périodes exceptionnelles comme en période d'Etat de siège ou d'Etat d'urgence[226]. Le législateur Sénégalais n'a pas soulevé des délais de la garde à vue en matière de cybercriminalité. Ce qui veut dire qu'il s'agit des mêmes délais qu'en droit commun. Partant, la cybercriminalité est une nouvelle forme de délinquants qui est caractérisée par sa spécificité en matière d'enquête. En effet *« les enquêtes judiciaires sont aujourd'hui de pus n plus confrontées à des éléments de preuve qui se manifestent sous de document informatique* »[227], ces délais précités semblent à notre avis être insuffisants face aux délits cybercriminels, du fait de la possible fréquence des lenteurs dans les procédures d'investigation. D'où la nécessité de procéder à une extension de la garde à vue dans les questions portant sur la cybercriminalité, comme en matière de terrorisme ou la garde à vue est étendue au maximum d'un délai de 12jours, afin de permettre aux enquêteurs d'avoir le temps nécessaire pour la recherche des preuves suffisantes pouvant déterminer la culpabilité de la personne gardée à vue.

Toutefois, le recours à l'extension des délais de la garde à vue doit être nuancé. En effet, on ne saurait perdre de vue que la garde à vue est une mesure qui porte atteinte à la liberté individuelle. C'est pour cette raison que le législateur à prévue des règles visant à protéger toute personne se trouvant dans cette situation. L'officier de police judiciaire chargé de mettre en garde à vue effectuer une requête de garde à vue, il doit indiquer dans un registre les motifs de la garde à vue, la durée des interrogations, les heures de report qui ont séparés l'interrogation, la conduite devant le procureur[228]. De même, la personne gardée à vue dispose de la possibilité de demander un examen médical à tout moment. En cas de prolongement des délais de la garde à vue, la personne gardée à vue peut demander l'assistance d'un avocat[229].

Cette protection des libertés individuelles par l'encadrement de la procédure de la garde à vue est sans doute nécessaire, mais il faut signaler que les libertés individuelles ne peuvent être garanties s'il n'existe pas des mesures suffisantes tendant à faciliter d'identification de la personne auteur de l'infraction et à la collecte des preuves.

Le risque de porter atteinte à la liberté individuelle qui caractérise la garde à vue, nécessite une limitation de celle-ci à certaines infractions. Il en est ainsi des infractions contre la sureté de l'Etat et les infractions graves telles que les atteintes aux personnes commises par l'utilisation des TIC.

En somme les délais la prescription de l'action publique et de la garde à vue doivent être prolongés au double de ceux prévus pour chaque infraction ou prévus en fonction de la situation en cause, afin de meilleur garantir la protection les internautes.

[226] Art. 55 CPP
[227] ERIC OK , *op. cit*. p. 205 à 217
[228] ART. 57, CPPS.
[229] ART. 55 alinéa, *in fine*, *ibid.*

Conclusion.

Les nouvelles technologies de l'information et de la communication ont de nos jours, dominé le monde. L'internet transforme le monde en un village planétaire. Il présente des avantages considérables, surtout dans le monde des affaires en ce sens où, il améliore la production des entreprises, révolutionne le travail et rend possibles l'émergence de nouveaux modèles d'affaires permettant de communiquer, de négocier, d'échanger et de commercialiser en temps réel. Etant « *un mécanisme de distribution de l'information et un moyen de collaboration et d'interaction entre les individus et leurs ordinateurs à travers toute la planète* »[230], son accessibilité à tout individu à travers le monde, ne reste pas sans avoir de conséquences négatives vis-à-vis des internautes.

Les nouvelles technologies de l'information et de la communication ont favorisé l'émergence des nouveaux types d'infractions ou une évolution d'infractions existantes. Ces infractions liées aux TIC, dénommées sous le nom de cybercriminalité, peuvent porter atteinte aux systèmes informatiques, aux données informatisées. Elles peuvent aussi consister à une atteinte portant sur des contenus illicites, à une atteinte relative à la personne ou aux biens. Ainsi, « *le développement spectaculaire des TIC sur le continent avec la démocratisation de la téléphonie mobile et l'émergence de la banque et du paiement mobiles expose l'Afrique à des menaces* »[231].

Le Sénégal n'est pas en exempt de ces menaces. C'est pour cette raison que le législateur, à travers la loi n°2008-11 du 25 janvier 2008 sur la cybercriminalité, prévoit des incriminations et des sanctions spécifiques à la cybercriminalité. Il vise à neutraliser tous comportement portant atteintes aux systèmes informatiques, aux données informatiques, aux contenus illicites, et à adapter le droit pénal à la cyberdelinquance, portant sur, les atteintes aux biens, à la propriété telles que le vol, d'escroquerie, le recel etc.

Le législateur Sénégalais à procéder à une amélioration des techniques d'investigation dans le but l'adapter le droit procédural à la cybercriminalité. Il en est ainsi de l'admission de la preuve numérique, de la saisie informatique, de la perquisition informatique, etc. De mêmes,

[230] PAPA GUEYE, *op. cit*. p. 266.

[231] MOUHAMADOU LO, « La cybercriminalité et la protection des données personnelles au Sénégal », .https://www.francophonie.org, consultée le 12/ 08/2019 à13h50.

le législateur a envisagé la responsabilité pénale de certaines personnes afin de rendre plus efficace, la répression de la cybercriminalité. Il s'agit de la responsabilité des fournisseurs d'accès, les hébergements, des éditeurs et des personnes morales autres que l'Etat et les collectivités locales.

En sus, la loi n°2008-12 sur la protection des données à caractère personnel, la loi n°2008-8 sur les transactions électroniques et la loi n°2008-10 sur la société de l'information constituent autant de lois édictées, et qui ont pour but de combattre la cybercriminalité.

A côte des dispositions nationales permettant de lutter contre la cybercriminalité, nous pouvons noter des engagements aussi bien au niveau sous régional, continental, qu'international dans le but de lutter contre la cybercriminalité.

Au niveau sous régional, nous avons la Directive de la CEDEAO portant lutte contre la cybercriminalité dans l'espace de la CEDEAO[232]. Au niveau continental nous pouvons citer, la convention de l'Union Africaine sur la cyber-sécurité et la protection, des données à caractère personnel du 27 juin 2014.

Mais, il ne faut pas perdre de vu que le problème de la cybercriminalité ne se limite pas au niveau national ou sous régional. Le Sénégal aura besoin d'une collaboration au niveau international. C'est pour cette raison que le Sénégal a depuis 2016 signé la convention européenne sur la cybercriminalité encore appelé la Convention de Budapest. A travers cette convention, le Sénégal peut bénéficier d'une demande d'entraide pour toute infraction entrant dans le cadre de la convention. Cette entraide s'applique en matière d'investigation et de procédure dans le but de recueillir les preuves sous forme électronique d'une infraction pénale[233]. En matière d'investigation, l'entraide peut porter sur l'accès aux données stockées[234], sur la collecte en temps réel de données relatives au trafic[235], et sur d'interception de données relatives au contenu[236]. L'entraide peut également concerner des mesures provisoires, telles que la conservation rapide de données informatique stockées et la divulgation rapide de données conservées.

[232] Directive C/DIR/1/08111, portant lutte contre la cybercriminalité dans l'espace de la CEDEOA.
[233] Article 25 de la convention de Budapest
[234] Art. 31 et 32
[235] Art. 33
[236] Art. 34 de la convention de Budapest, *op.cit*.

A côté de l'entraide, le Sénégal a aussi à travers la convention, la possibilité le faire une demande d'extradition[237]. De même, le Sénégal aurait dû ratifier la convention des Nations Unies contre la criminalité transnationale organisée. Bien que la cybercriminalité ne soit pas toujours, le fait un groupe de personne, mais nous ne pouvons pas écarter la possibilité qu'elle soit le fait d'un groupe de personnes, qui agit de concert. D'ailleurs la plupart les délits cybercriminels sont perpétrés par un groupe de personnes.

Par ailleurs, ces différentes dispositions envisagées pour lutter contre la cybercriminalité sont d'un avantage considérable, mais elles ne sont pas suffisantes elles seules pour neutraliser ce phénomène. Vu son caractère transnational, il serait selon nous préférable, pour une lutte beaucoup plus efficace, que la cybercriminalité soit intégrée parmi les infractions à compétence universelle. Encore faudrait-il, pour ce faire, qu'il y ait une incrimination des comportements juges cybercriminel de façon universels. Dans ce cas, chaque pays peut se déclarer compétent pour juger une personne se livrant à des actes cybercriminels, quel que soit sa nationalité, ou le lieu de commission de l'infraction. En adoptant cette solution, il serait très difficulté de voir une infraction cybercriminelle être dans l'impunité. Ce qui entraine pour conséquence, de dissuader tout individu ayant l'intention de commettre un cyber-délit. Cette solution permet aussi de mettre fin à l'obstacle de compétence issue de la souveraineté des Etats.

Par ailleurs, la répression de la cybercriminalité nécessite pour plus d'efficacité qu'une procédure de sensibilisation soit mise en place. En effet, « *les cybercriminels tirent une grande partie de leur force du fait que leurs victimes ne se méfient pas d'eux. Il s'agit donc de mettre un terme à cette ignorance de l'existence de réseaux nuisibles* ».[238] D'où la nécessité de les sensibiliser. La sensibilisation consiste dans l'intérêt de susciter la curiosité de quelqu'un sur une question bien déterminée.

Cette idée est soutenue par Dr. Papa Gueye dans son ouvrage intitulé « Criminalité organisée, Terrorisme et Cybercriminalité : Réponses de politique criminelles », qui voit la sensibilisation comme un moyen de prévention de la cybercriminalité. Par lui, « *La sensibilisation consiste à informer les internautes de la nécessité d'instaurer des codes de conduites mais également à sensibiliser les différents auteurs sur le rôle qu'ils peuvent jouer pour éviter que des crimes informatiques soient commis, pour faire éviter aux internautes,*

[237] Art. 24, de la convention de Budapest, *op.cit.*

[238] CLEMENCE BOULANGER FRAFER FANNY, « Cybercriminalité : un aperçu du monde des criminels virtuels », Classe International, https:// classe-internationale.com, consultée le 13/07/2019, à 12h30.

surtout aux mineurs, des dommages ou des traumatismes »[239]. « *Elle doit être élargie à toutes les couches de la population, notamment les jeunes, les parents et les enseignants* ».

Le rôle des parents consiste à éduquer leurs enfants de bons principes et de valeurs, donc selon lui « *ils sont les mieux placés par informer et protèges leurs enfants des dangers que peut présenter l'Internet* »[240]. Cela se justifie par le fait que les parents jouent un rôle très important dans d'éducation de leurs enfants. C'est pour cette raison que le code de la famille leur donne un pouvoir considérable envers leurs enfants mineurs. Il s'agit du droit de garde, qui donne aux parents les prérogatives tel que les pouvoirs de direction et de contrôle sur les enfants mineurs. Et ce pouvoir de contrôle et de direction ne sont rien d'autre que le devoir d'éducation et de protection qui pèse sur chaque parent. Pour un auteur la présence les parents ainsi que l'intérêt qu'ils portent envers les activités de leurs enfants sur le Net sont non négligeables[241].

Concernant, le rôle des enseignants dans la prévention de la cybercriminalité, ils procèderont à expliquer aux élevés des dangers de la cybercriminalité ainsi que les techniques permettent d'éviter ce genre d'attaque. Ces idées semblent intéressantes, car ils englobent les différents moyens possibles que doit utiliser un Etat afin de sensibiliser ses citoyens des dangers de la cybercriminalité.

En sus de cela, nous pensons que la prévention de la cybercriminalité sera plus efficace, si cette forme de délinquance fait l'objet d'une matière spécifique qui sera enseignée dans les écoles et universités. Pour y parvenir, les enseignants doivent au préalable être formés, dans ce domaine, afin qu'à leur tour, ils puissent dispenser, leurs connaissances.

En plus de l'enseignement, la prévention de la cybercriminalité, doit procéder par la création d'une organisation chargée d'organiser des séances de sensibilisation annuelle dans toutes les régions du pays. Ces séances auront comme thèmes, la lutte contre la cybercriminalité, où ces associations exposeront, les différentes formes de la cybercriminalité existantes, les techniques utilisées par les cybercriminels ainsi que les moyens nécessaires pour y échapper.

---

[239] PAPA GUEYE, *op. cit*. p. 330.

[240] PAPA GUEYE, *Ibid*. P.333.

[241] V. KAISER, « La protection des mineurs sur Internet : la problématique de la pédopornographie et des contenus juges préjudiciables », mémoire présente à l'UCL en vue de l'obtention du grade de Maitrise en droit, Louvain-la-Neuve, 2009. Cité par PAPA GUEYE, *ibidem*. P.333.

En outre, la sensibilisation ne doit pas se limiter seulement dans la prévention de la cybercriminalité, elle doit être élargie aux victimes pour leur montrer, les voies à suivre pour obtenir réparation de leurs préjudices.

A côté de la sensibilisation, Dr. Papa Gueye a proposé, le recours aux techniques de contrôle pour prévenir la cybercriminalité.

Les techniques de contrôle consistent dans la vérification de l'Age des internautes et du contenu. La vérification d'âge est une technique qui permet de voir si l'utilisateur qui essaie d'accéder à un site web à effectivement l'âge requis pour en visionner le contenu. « Le système émet une décision qui est soit « oui » soit « non » selon que le visiteur a atteint ou non l'âge programmé. C'est une technique qui existe déjà dans certaine sites. C'est l'exemple des sites pornographiques, qui exigent pour y accéder un âge minimal de 18ans. Cela revient à interdire aux mineurs la consultation de ces sites. Le but de cette vérification est de protéger les mineurs qui ne peuvent accéder à n'importe quels sites sur Internet.

En plus, de la vérification d'âge, selon Dr. PAPA GUYE *« les pays devraient penser à la mise en place d'une plateforme d'échange permettant de vérifier l'authenticité des informations fournies et contenues dans les pièces d'identification »*. Et à ce titre, *« un partenariat solide et sur devra être noue entre les services publics et prives, permettant un accès certifie aux différentes bases de données ». IL est aujourd'hui nécessaire de créer au Sénégal cette plateforme d'échange entre le ministre de l'Intérieur, les hébergeurs, les fournisseurs d'accès et les opérateurs par exemple* »[242].

Le recours à la technique de filtrage de contenu quant à lui consiste à un filtrage sur la base de « listes blanches », qui ne permet l'accès qu'aux sites préalablement identifiés et qui par conséquence, bloque l'accès à tous les sites qui ne se retrouvent pas dans la liste[243].

[242] PAPA GUEYE, *op. cit.* p. 341.

[243] Communication de la commission sur le contenu illégal et préjudiciable sur Internet, C. O. M. (96) 487 final, p. 19/24.

Bibliographie

I-Ouvrages généraux, manuels et traités.

- ALAIN COEURET et ELISABETH.FORTIS, Droit pénal du travail, Paris, 4eme Ed. Lexix Nexis Litec, 2008,463 pages.
- BERNARD BOULOC, Procédure Pénale, Dalloz, Coll. Précis, 22eme édition, 2010, 1122 pages

- CLAUDE LOMBOIS, *droit pénal international*. Précis, Dalloz, 2^{e}edition, 1979, p.478.
- DIDIER REBUT, *Droit pénal international*, Précis Dalloz, 2^{e} édition 2014, p. 726.
- GASTON STEFANI, GEORGES LEVASSEUR, BERNARD BOULOC, *Droit pénal général*, 15 éd. Dalloz, 1994, 628 pages.

- HENRI DONNEDIEU DE VABRES, *Les principes modernes du droit pénal international*, éd. Paris Sirey, 1928, *470 pages*.
- JACQUES-HENRI Robert, *Droit pénal général*, Presses Universitaire de France, 3eme édition, 1998, 520 pages.
- JEAN CARBONNIER, « sociologie juridique », éd. Presse Universitaire de France, 1978, 415 pages.

- JEAN PRADEL, Procédure pénale, CUJAS, 17éme édition, 2013, 975 pages.
- SERGE GUINCHARD et THIERRY DEBARD, *Lexique des termes juridiques*, 25eme édition 2017-2018, 1199 pages.

- THIERRY GARE ET CATHERINE GUIESTET, *Droit pénal procédure pénale*, Dalloz, 8eme Edition, 473 pages.

II-Ouvrages spéciaux.

- ALI AZZOUZI , « La cybercriminalité au Maroc », préface de M. CHAWKI, 2010, 156 pages.
- CHRISTIANE FERAL-SCHUHL, Cyberdroit, Le droit à l'épreuve de l'internet, Dalloz 7eme édition, 2018/2019,1884 pages.
- PAPA GUEYE, criminalité organisée, terrorisme et cybercriminalité : Réponses de politique criminelles, l'Harmattan, 2018, 436 pages.

- PAPA ASSANE TOURE, Le traitement de la cybercriminalité devant le juge, L'exemple du Sénégal, l'Harmattan, 2014, 618pages

III-Articles, documents et dossiers.

- ABDOULLAH CISSE « Exploration sur la cybercriminalité et la sécurité en Afrique : Etat des lieux et priorité de recherche », Synthèse des rapports nationaux, 2011,77pages.
- CHRISTIAN AGHROUM, « police judiciaire et nouveaux territoires de l'information, numériques », campagne nationale des experts de justice en informatiques et techniques associées .Colloque du 13 Avril 2010 à la 1ere chambre de la cour d'appel de paris, entre 40 à 42 pages.
- Dixième Congrès des Nations Unies pour, « La prévention du crime et le traitement des délinquants », Vienne, 10-17 avril, 2000, 17pages.
- FREDERIQUE CHOPIN, « La cybercriminalité », Répertoire de droit pénal et de procédure pénale, Université AIX-Marseille CDS EA 901, 153 pages.
- JACQUES FRANCILLON, «cybercriminalité aspects de droit pénal international », XIXe Congres International de Droit Pénal, Société de l'Information et Droit Pénal, Colloque Préparatoire –Section4, 37pages.
- MELANIE CLEMENT-FONTAINE, « De l'information numérique à la preuve numérique », colloque du 13 avril 2010, entre 9 à 19eme pages.
- MOHAMED CHAWKI, « Essai sur la notion de la cybercriminalité », IEHEI, juillet 2006, 36 pages
- NICOLAS RONTCHEVSKY, « revue Internationale de Droit Economique », ed.de boeck, 2002, entre 523à 528, pages.
- Rapport sur Comprendre la cybercriminalité : Guide pour les pays en développement, élaboré à partir d'un ouvrage intitulé, Comprendre la cybercriminalité : Guide pour les pays en développement, représenté par Marco Gercke, UIT 2012, 374pages.
- Rapport sur la procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique : proposition pour une efficacité juridique renforcée, présenté par ERIC FREYSSINET et CORINNE THIERACHE, enregistré dans le code pénal et lutte contre la cybercriminalité, juin 2014, 46pages.
- OFFICE DES NATION UNIES CONTRE LA DROGUE ET LE CRIMES (UNODC), « La coopération internationale en matière pénale contre le terrorisme », 2011,156 pages.
- THIERNO AMADOU NDIOGOU « Etude sur L'état des lieux de la cybersécurité et de la cybercriminalité au Sénégal », Global Partner Digital Jonction, mars 2019, 15pages
- UNESCO « Universalité de l'internet: un outil pour la construction des sociétés du savoir et de l'agenda pour le développement durable post-2015 », 2 septembre 2013, 14pages.

IV-Thèses et mémoires.

- ANMONKA JEANINE-ARMELLE TANO-BIAN « La répression de la cybercriminalité dans les Etats de l'Union Européenne et de l'Afrique de l'Ouest », Thèse, Université de Paris Descartes, 28mai 2015, 641 pages.
- EMMANUELLE MATIGNON « La cybercriminalité : un focus dans le monde des télécoms » mémoire, Université de Paris1 Panthéon-Sorbonne, 2011-2012, 95pages.
- FANNY BINOIS, « La solidarité des compétences législatives et juridictionnelles en droit pénale international », mémoire, Master, université Jean-Monnet, paris, 2012-2013, 66pages.
- ROMAIN BOSS « La lutte contre la cybercriminalité au regard de l'action des Etats », thèse Université de Lorraine, 2016, 407 pages.

V -Législations

• Textes internationaux

- Convention internationale relatives aux droits de l'enfant du 20 novembre 1989, (ratifiée par le Sénégal le 31 juillet 1990)
- Convention de Budapest sur la cybercriminalité du 23novembre 2001.
- Convention des Nations Unies contre la criminalité organisée du 15 novembre 2000.
- Déclaration Universelle des droits de l'homme du 16 décembre, 1948.
- Déclaration des droits l'homme et du citoyen de 1789.

• Textes sous régionaux.

✓ Union africaine(UA)

- Projet de Convention de l'Union africaine sur la mise en place d'un cadre juridique de confiance pour la cybersécurité en Afrique.
- Convention sur la cybersécurité et la protection des données à caractère personnel du 27juin 2014.
- Déclaration d'Abidjan du 22fevrier 2012 pour une harmonisation des cyber-législation africaines.
- Déclaration d'Addis-Abeba du 22juin 2012, pour une harmonisation des cyber-législation africaines.
- Déclaration de Khartoum du 06 septembre 2012, relatif à la quatrième session de la conférence de l'union africaine des ministres chargés de la communication et des technologies de l'information.

✓ CEDEAO.

- Convention A/P1/8/94relative à l'extradition signée à Abuja(Nigeria) le 06 aout 1994.
- Convention A/P1/7/92 relative à l'extradition judiciaire en matière pénale signée à Dakar (Sénégal) le 29 juillet 1992.

- Acte additionnel du 2 octobre 2009 relatif à la protection des données à caractère personnel dans l'espace de la CDEAO.
- Directive C/DIR/08/11 du 19 aout 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

✓ UEMOA

- Loi uniforme n° 2008-48 du 3 septembre 2008, relative à la répression des infractions en matière de chèque, de carte bancaire et autres instruments et procèdes électroniques de paiement (JORS, n°6453, du 7 février 2009.

• Textes nationaux

- Loi n°65-60 du 21 juillet 1965 portant Code pénal, (JORS n° 3767 du 6 septembre 1965).
- Loi n°65-61 du 21 juillet 1965, portant Code de procédure pénale, (JORS n° 3777 du 25 aout 1965).
- Loi n°71-77 du 22decembre 1971, relative à l'extradition, (JORS n° 4207 du 05 février 1972).
- Loi n°2008-08 du 25janvier 2008, sur les transactions électroniques (JORS n°6404 du 26 avril 2008).
- Loi n°2008-11 du 25 janvier 2008, portant sur la cybercriminalité, (JORS, n°6406 du 3mai 2008).
- Loi n°2008-12 du 25janvier 2008, sur la protection des données à caractère personnel, (JORS, n°6406 du 29 novembre 2008).
- Loi n°2008-23 du 25 juillet 2008portant insertion d'un article 664 bis dans Code de procédure pénale, (JORS n° 6420, du 8 aout 2008).
- Loi n°2016-29 du 08 novembre 2016 modifiant la loi n°65-60 du 21 juillet 1965 portant Code de procédure pénale (JOSRS n°6975 du 27 mai 2016)
- Loi n°2004-575, du 21 juin 2004 pour la confiance dans l'économie numérique, (JOF n° 143 du 22 juin 2004). (Loi française)
- Loi n°2004-204 du 9mars 2004, issue du projet de loi portant adaptation de la justice aux évolutions de la criminalité, (JOF n° 59 du 10 mars 2004). (loi française).

VI-Jurisprudences.

- TR Thiès, du 18 septembre 2012 affaire de l'Agence New Looks Business, bull. d'information de la cour suprême, n°7-8, p134 note de PAPA ASSANE TOURE.
- TGHC Dakar, n°2715 du 19 juin 2012, affaires des jeunes filles de Grand Yoff bull. d'information de la cour suprême n°7-8, p.145 note PAPA ASSANE TOURE.
- TRHC Dakar du 19 juillet 2007, affaire résidence Saint James, inédit. In bull. d'information de la cour suprême, n°7-8, p.137 note de PAPA ASSANE TOURE.

- TRHC, Dakar, 29mars, 2009, dit Riad Mouhamed Zayatte, bull. d'information de la cour suprême, n°7-8 p.142 note PAPA ASSANE TOURE.

VII-Webographie.

- ABDOULLAH CISSE « Exploration sur la cybercriminalité et la sécurité en Afrique : Etat des lieux et priorité de recherche » Synthèse des rapports nationaux, 2011 p. 5. https://idl-idrc.dspacedirec.org, consultée le 3/ 9/ 2019 à 10h08.
- L'accès des autorités publique aux données chiffrées, 30 Aout 2017, https://www.cnil.fr consulté le 25septembre 2019 à 17h 24.
- ADAMA OUANE, « guide pratique de la cybersécurité et de la cyberdéfense, https://www.francophonie.org, consulté le 06/08/2019, à 15h07.
- L'Afrique se met en ordre de bataille contre la cyberveillance et de la cybercriminalité : http://cio-mag.com. visité le23/07/2019 à 15h12.
- ART. 23 du projet de loi d'orientation et de programme pour la performance et la sécurité intérieure, assemblée nationale. du 27mai 2009, www.assemblee-nationale.fr, consultée le 29/A10/2019 à 15h46
- ASTOU DIOUF « Etude critique de la Stratégie Nationale de cyber sécurité du Sénégal » avril 2019, http://jonction.e-monsite.com, consulté à 16h13.
- Définition de confidentialité, htrps://fr.m.wikipedia.org. Consultée le 2/07/2019 à 11h27.
- Définition de la répression, https://www.cnrtl.fr, consultée, le 29/10/2019 à 19h33.
- Cass.Crim, 12novembre 1986, Bull. crim., n°335 p.861, https://www.legifrance.gouv.fr, consultée le 29/10/2019 à 13h06.
- Cass. Crim. 8 janvier 1979 : bull. Crim. N° 13p.32, https://www.legifrance.gouv.fr, con sultée le 29/10/2019 à 13h15.
- Cass. Crim. 12janvier 1989 : Bull crim. N° 14, p.38, https://www.legifrance. gouv.fr, consultée le 29/10/2019 à 13h20.
- Chambre criminelle de la cour de cassation, Crim. 1er mars 1989, n°100 p.269, https://www.legifrance. gouv.fr, consultée le 29/10/2019 à 13h16.
- Crim. 2 decembre1997, https://www.legifrance.gouv.fr, consulté le 29/10/2019 à 13h33.
- Cours de justice des communautés européennes(CJCE), arrêt du 23mars 2010 dans l'affaire dite Google AdWords, https://www.legilis.net, consultée le 29/10/2019 à 14h12.
- CLEMENCE BOULANGER, FRAFER FANNY, « Cybercriminalité : un aperçu du monde des criminels virtuels », https:// classe-internationale.com., consulté le 13/07/2019 à 12h30.
- CRISTOPHE GUILLEMIN « Blanchiment des capitaux, nouvelles tendance de la cybercriminalité en 2006 », Janvier 2007, https://www.zdnet.fr. consulté le 15/10/2019 à 12h20.

- DOHA : l'ONU et ses partenaires mettent l'accent sur leurs efforts pour combattre la cybercriminalité : Disponible sur : https://.news.un.org. Consultée le 23/10/2019 à 11h10.

- JEAN-CLAUDE MOUSSOKI « Les moyens de communication traditionnels en zones rurale dans l'espace culturel Koogo : cas du département du Pool », Mémoire en vue l'obtention du Diplôme d'Etudes Approfondies (D.E.A), année 2003-2004, p.1. https://www.memoireonline.com. Consultée de 5/1O/2019à 10h30.
- 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 pour l'obtention de la maitrise en droit, 2007. https://www.memoireonline.com. Consultée le 13/ 10/2019 à 10h11.
- L'Internet ? Définition, Histoire et Application, https://wikimemoires.net. Consultée le 12/10/2019 à 10h20.
- L'Internet et la démocratie numérique- Cybercriminalité, ordre public économique et déstabilisation de l'Etat, https://books.penedition.org consulté le 06/08/2019 à 13H12.
- LAURIANE MPOUKI « Avantages et inconvénient d'internet chez les jeune », bantuhub.com. 12/10/2019 à 10h54.
- LEON PATRICE SARR « La répression de la cybercriminalité en droit Sénégalais à l'épreuve de l'anonymat dans le cyberespace », https://www.droit-technologie.org. Consulté le 27/05/2019 à 13h50.
- LIONEL KALINA, « Cybercriminalité : quels outils pour l'Afrique ? Cybercriminalitéblogg.org, consultée le 27/05/ 2019 à 16h30.
- MARTINE EXPOSITO « Prévenir des cybercriminalité dans un contexte professionnel, https://cours.unjf.fr. consultée le 13/06/2019 à12h15.
- Le Ministre de L'Intérieur français. Disponible sur http://www.interieur.gouv.fr/, consultée le 12/09/2019à 15h16.
- MOUHAMADOU LO, « La cybercriminalité et la protection des données personnelles au Sénégal ».https://www.francophonie.org, consultée le 12/08/2019 à 13h50.
- PATRICK AMAZOU, Cybercriminalité: comment l'Afrique essaie de se defender, www.osiris.sn. Cybercriminalité-com. 19h35
- PIERE PEREZ, « Forum de discussion et responsabilité », 2013 www.esen.education.fr, consultée le 29/06/2019 à 16h. déjà connu
- Problème de procédure pénale lies à la technologie de l'information, Recommandation N°R(95) 13 adoptée par le comité des Ministres du Conseil de l'Europe le 11 septembre 1995 P.59, https://rm.coe.int, consultée le 28/10/2019 à 20h30.
- Pour un droit de la prescription moderne et cohérent, https://www.senat.fr, consultée le O2/07/2019 à 15h13.
- STEPHANIE PERRIN, Cybercriminalité, https : //vecam.org, consultée le 12/09/2019 à15h17.
- Technologies de l'information et de la communication, https://fr.m.wikipedia.org. Consultée le 5/10/2019 à 11heures.
- TGI de paris, Affaire Yahoo du 11 février 2003, https://www.legilis.net, consulté le 29/10/2019 à 14h12.
- TGI Lyon du 28 mai 2002 dite affaire Père Noel, https://www.legalis.net, consultée le 29/10/2019 à 13h58.
- TGI, Paris, du 3juin 2008, n°350, https://legalis.net, consultée le 29/10/2019 à 13h26.
- Un virement SEPA est un virement international dans la zone européenne : un transfert de font d'un compte vers le compte d'un bénéficiaire situé dans cette zone européenne. https://www.bluenote-systems.com, consulté le 25/04/2019 à 9h13.

Table des matières