Global Partner
Second Home, 68-80 Hanbury Street
London, E1 5JL
https://www.gp-digital.org/

Digital JONCTION
HLM Grand Médine N° 512
Dakar-Sénégal
http://jonction.e-monsite.com

ÉTUDE SUR « *L'ETAT DES LIEUX DE LA CYBERSECURITE ET DE LA CYBERCRIMINALITE AU SENEGAL* »

Consultant
Dr. Thierno Amadou NDIOGOU
Enseignant-chercheur à la FSJP-UCAD
thiernonndiogou@gmail.com

Mars 2019

SOMMAIRE

ABREVIATIONS ii
I. INTRODUCTION 1
1. Rappel du contexte de termes de référence de l'étude 1
a. Définition de « *cybersécurité* » et de « *cybercriminalité* » 1
b. Objectif stratégique global de l'étude 2
2. Méthodologie 3
II. L'ETAT DES LIEUX ET ANALYSES 4
1. Stratégies sénégalaises en matière de cybersécurité et de cybercriminalité 4
1. a. Stratégies sénégalaises en matière de cybersécurité 4
1. b. Stratégies sénégalaises en matière de cybercriminalité 4
2. Traitement et réponses du phénomène de la cybercriminalité et de la cybersécurité 5
2. a. Réponses étatiques 5
2. b. Réponses judiciaires 8
2. c. Réponses administratives 8
3. Inventaire des manquements au respect des normes des droits de l'homme dans la lutte contre la cybercriminalité et en matière de politiques de cybersécurité 9
3. a. Par rapport à la recherche de preuve 10
3. b. Par rapport à la présomption d'innocence 10
3. c. Par rapport au droit de la défense de l'inculpé 11
4. Exploration des atteintes aux droits numériques notamment la liberté d'expression sur internet et les données à caractère personnel 11
4. a. Sur la liberté d'expression 11
4. b. Sur les données à caractère personnel 12
III. RECOMMANDATIONS 14
1. Leçons apprises 14
2. Recommandations 14

ABREVIATIONS

JORS	Journal Officiel de la République du Sénégal
P (pp)	Page (pages)
n°	numéro
OSC	Organisation de la Société Civile
TIC	Technologies de l'Information et de la Communication

I. INTRODUCTION

1. Rappel du contexte de termes de référence de l'étude

Le cyberespace[1], considéré comme le cinquième champ de bataille, est un terrain d'opérations militaires au même titre que la terre, la mer, l'air et l'espace. C'est pourquoi, le monde militaire et le monde civil sont appelés à maîtriser les cybers risques, que cela soit dans un but de sécurité et de défense nationale, soit à des fins de lutte contre la cybercriminalité[2].

Dès lors, toute réponse pragmatique à la criminalité générée par le numérique se base sur une approche stratégique, qui fixe le cadre d'un plan d'action.

Cette vision est nécessaire pour gouverner, piloter et assurer la cohérence et la complémentarité des mesures stratégiques et opérationnelles. Cela autorise également leur efficacité et efficience. Sous ce prisme, toute stratégie passe nécessairement par une approche préventive qui consiste à rendre le cyberespace moins favorable à l'expression de la criminalité et à réduire les opportunités criminelles.

a. Définition de « *cybersécurité* » et de « *cybercriminalité* »

« *Cybersécurité* ». Le terme « *cybersécurité* » est une réalité difficile à appréhender en raison de son caractère intangible et fortement technique, et d'un grand flou sémantique dans la littérature. Il n'existe en effet pas de définition objective et consensuelle.

Cependant, pour les besoins de la présente étude, nous avons choisi de nous référer à la définition proposée par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) français[3] : « *La cybersécurité est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cyber sécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ». A travers cette définition, la cybersécurité comprend les trois composantes : les mesures de protection contre les menaces et les attaques, les mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels » et la cybercriminalité.

---

[1] L'on peut retenir que le cyberespace constitue pour les États de faire valoir les frontières et la sécurité dans cet espace virtuel mondialisé, et d'assurer aux citoyens, aux entreprises et aux institutions un État de droit dans le cyberespace (Note conceptuelle « Conférence internationale sur le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone ». OIF. Abidjan, Côte d'Ivoire ; 8 — 10 février 2016. : francophonie.org/IMG/pdf/note_conceptuelle_conference_cybersecurite_abidjan_2016.pdf

[2] L'on pourrait même convoquer d'autres aspects notamment économiques.

[3] Document cité par F. AJINA, « cadre juridique de la cybersécurité dans l'espace francophone » disponible sur le lien suivant : http://ific.auf.org/sites/default/files/IFIC-AUF-EtudeJurid-Cybrsecurite.pdf

En scrutant par ailleurs, la Stratégique nationale de la cybersécurité du Sénégal (SNC2022), l'on peut retenir que la cybersécurité renvoie à un « *ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes* ».

Cette acception intègre des solutions d'ordre éducatif, juridique, managérial et technique orientées vers l'objectif de sécurisation du cyberespace. Bref, la cybersécurité procède d'une approche holistique et pluridisciplinaire des réponses de politique criminelle à la cybercriminalité.

« *Cybercriminalité* ». Relativement au mot « *cybercriminalité* », les rédacteurs de la loi sénégalaise n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité semblent le définir comme *« toute infraction qui implique l'utilisation des technologies de l'information et de la communication »*[4].

Cette définition renvoie à celle retenue par le droit pénal camerounais : « *l'ensemble des infractions s'effectuant à travers le cyberespace par les moyens autres que ceux habituellement mis en œuvre et de manière complémentaire à la criminalité classique* »[5].

b. Objectif stratégique global de l'étude

Facilitation de l'engagement de la société civile dans les processus décisionnels nationaux clés en matière de cybersécurité et de cybercriminalité. L'objectif stratégique global consiste à la capacitation des organisations de la société civile du Sénégal à s'engager efficacement dans les principaux processus d'élaboration des politiques en matière de cybersécurité et de cybercriminalité.

Cette situation de référence permettra d'établir un renforcement de la liberté de l'internet au Sénégal en facilitant la participation de la société civile aux principaux processus nationaux en matière de cyber décision.

Les objectifs de l'étude. Ils tournent autour des points ci-après :

- *Explorer la stratégie sénégalaise en matière de cybersécurité et de cybercriminalité ;*
- *Traiter le phénomène de la cybercriminalité et de la cybersécurité et les réponses étatiques (législatives ; judiciaires ; administratives) et sociétales (sensibilisation ;*

[4] Exposé des motifs de la loi n° 2008- 11 du 25 janvier 2008 portant sur la cybercriminalité, JORS, n°6406 du 03 mai 2008, p. 419.

[5] Loi n° 2010-12 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun, J.O. de la République du Cameroun du 21 décembre 2010, p. 3 et s..

éducatives ; plaidoyer) apportées à ces phénomènes nouveau de l'environnement des technologies de l'information et de la communication ;

- *Faire l'inventaire des manquements au respect des normes des droits de l'Homme dans la lutte contre la cybercriminalité et en matière de politiques de cybersécurité ;*
- *Explorer les atteintes aux droits numériques notamment la liberté d'expression sur internet ; les données à caractère personnel, etc. ;*
- *Faire des recommandations pour la prise en compte du respect des droits de l'homme dans l'élaboration de la stratégie nationale de cyber sécurité.*

2. Méthodologie

Elle repose essentiellement sur trois (3) phases :

1. Une phase de recherche documentaire ;
2. Une phase de collecte de données par interview[6] ;
3. Une phase de traitement des données.

[6] Il n'est pas inutile de souligner que le consultant a été appuyé par trois (3) facilitateurs durant l'exercice de sa mission ; il s'agit de deux (2) de ses étudiants qui travaillent sur ce thème et une doctorante membre de son Laboratoire d'Etudes et de Recherches en Droit privé et Sciences criminelles (LER'DP-SCRIM).

II. L'ETAT DES LIEUX ET ANALYSES

Conformément à ce qui précède, la présente étude vise à procéder à l'état des lieux tout en l'analysant.

1. Stratégies sénégalaises en matière de cybersécurité et de cybercriminalité

1. a. Stratégies sénégalaises en matière de cybersécurité

Pour répondre aux cybermenaces auxquelles le Sénégal est confronté, l'approche du Gouvernement s'appuie sur une vision et des objectifs stratégiques précis. Cette approche renforce toutes les activités relatives à la cybersécurité entreprises au Sénégal par des particuliers, des organisations des secteurs public et privé et de la société civile ainsi que du monde universitaire.

La vision se décline comme suit : « *En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous* ». À ce sujet, voir la Stratégique nationale de la cybersécurité du Sénégal (SNC2022).

Afin de réaliser cette vision, le Gouvernement sénégalais s'emploiera à atteindre les cinq (5) objectifs stratégiques suivants :

- ✓ *Renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal ;*
- ✓ *Protéger les infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal ;*
- ✓ *Promouvoir une culture de la cybersécurité au Sénégal ;*
- ✓ *Renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs ;*
- ✓ *Participer aux efforts régionaux et internationaux de cybersécurité.*

1. b. Stratégies sénégalaises en matière de cybercriminalité

L'organisation de la réponse répressive méthodique contre la cybercriminalité[7], est passée par l'articulation d'un véritable mouvement d'expansion du champ de la politique criminelle, qui se décline sous forme de cyberstratégie de répression du phénomène. Elle s'articule autour de deux (2) points :

[7] A. CISSE, « Les déterminants juridiques à la promotion des technologies de l'information et de la communication (TIC) au Sénégal : enjeux, perspectives et méthodologie », Revue trimestrielle d'informations sur les télécommunications, la régulation et la recherche de l'ARTP, Octobre, novembre, décembre 2006, p.20 et s.

- ✓ *Elaboration d'une stratégie de modernisation des instruments de répression ;*
- ✓ *Articulation d'une stratégie d'amélioration du processus de répression.*

2. Traitement et réponses du phénomène de la cybercriminalité et de la cybersécurité

En politique criminelle[8], « *traiter* » un phénomène criminel consiste à y apporter une réponse « *organisée, voulue ou acceptée, en tout cas codée par la société* »[9].

Ainsi, dans un contexte de mutation et de bouleversement du champ pénal suscité par l'avènement des TIC, la problématique du traitement de la cybercriminalité renvoie à la stratégie de recherche d'une réponse adaptée à ce phénomène.

A côté des réponses étatiques (législatives, judiciaires et administratives), des réponses sociétales (sensibilisation, éducatives et plaidoyer) devront être apportées à ces phénomènes nouveau de l'environnement des technologies de l'information et de la communication.

2. a. Réponses étatiques

Il n'est pas inutile de rappeler qu'à côté des réponses étatiques, il en existe une panoplie de réponses extra étatiques. Ces réponses résultent de l'Union Africaine (UA), de la Communauté Économique des États de l'Afrique de l'Ouest (CEDEAO), de la Banque Centrale des États de l'Afrique de l'Ouest (BECEAO) et de l'Union Économique et Monétaire Ouest Africaine (UEMOA).

Conseil : Voir le site de l'Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal : http://www.osiris.sn/

❖ Sur la sécurité informatique

Outre le Projet de Loi portant Code des Communications Electroniques voté par l'Assemblée nationale du Sénégal le mercredi 28 novembre 2018, l'on peut citer notamment :

- **Loi** n° 2008-08 du 25 janvier 2008, sur les transactions électroniques, JORS, n° 6404 du 26 avril 2008, pp. 395 et s.
- **Loi** n° 2008-10 du 25 janvier 2008, portant loi d'orientation relative à la société de l'information, JORS, n° 6406 du 03 mai 2008, pp. 419 et s.

---

[8] Selon M. DELMAS-MARTY, la politique criminelle comprend « *l'ensemble des procédés par lesquels le corps social organise les réponses au phénomène criminel* ».
[9] M. DELMAS-MARTY, *Modèles et mouvements de politique criminelle*, Paris, *Economica*, 1983, p. 41.

- **Loi** n° 2011-01 du 27 janvier 2011 portant Code des télécommunications, JORS, n°6576 du 14 mars 2011, pp. 273 et s.
- **Loi** n° 2008-12 du 25 janvier 2008, sur la protection les données à caractère personnel, JORS, n° 6406, du 3 mai 2008, pp. 434 et s.
- Loi n° 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal
- **Décret** n° 2007-909 du 31 juillet 2007 portant organisation de la présidence de la république et fixant les missions du service technique central des chiffres et de la sécurité des systèmes d'information.
  - **Décret** n° 2008-720 du 30 juin 2008, relatif à la certification électronique pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, JORS, n° 6442 du 13 décembre 2008 ;
  - Décret n° 2010-1209 du 13 Septembre 2010 relatif à la loi n° 2008-41 du 20 Août 2008 sur la Cryptologie au Sénégal ;
  - **Décret** n° 2008-721 du 30 juin 2008, portant application de la loi 2008-12 du 25 janvier 2008 sur la protection les données à caractère personnel, JORS, n° 6443 du 20 décembre 2008 ;
  - **Décret** n° 2008-718 du 30 juin 2008, relatif aux commerces électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, JORS, n° 6440 du 29 novembre 2008.
  - **Décret** n° 2008-719 du 30 juin 2008, relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, JORS, n° 64339 du 22 novembre 2008.

❖ **Sur la Cybercriminalité**

Au Sénégal, l'année 2008 a marqué le système juridique de cyber sécurité. La promulgation simultanée de plusieurs textes touchants le cyber espace suppose que l'action était réfléchie et coordonnée.

La loi n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité a prévu un certain nombre d'infractions liées aux technologies de l'information et de la communication. Ces infractions figurent aujourd'hui dans le Code pénal en ses articles **431-7 à 431-65 16.**

A l'analyse de ces textes, les infractions visées sont relatives aux :

- ♠ Atteintes aux systèmes informatiques ;
- ♠ Atteintes aux données informatisées ;

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

Parallèlement, le **Code de procédure pénale** adapte la procédure en matière d'infractions commises au moyen des technologies de l'information et de la communication. A l'examen des **articles 677-34 à 677-42, il est prévu :**

- ♠ La conservation rapide de données informatisées archivées ;
- ♠ Perquisition et de la saisie informatique
- ♠ Interception des données informatisées ;
- ♠ Preuve électronique en matière pénale

Améliorations : En 2016, ce dispositif répressif est renforcé. Pour s'en convaincre, il suffit de se référer aux lois ci-après :

- **Loi** n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal, *JO n° 6975* du 25 novembre 2016, pp. 1613 et s. (Cette loi a modifié celle n° 2007-01 du 12 février 2007 modifiant le Code pénal, *JO n° 6332* du 10 Mars 2007, pp. 2375 et s.) ;
- **Loi** n° 2016-30 du 08 novembre 2016 modifiant la loi n°65-61 du 21 juillet 1965 portant Code de procédure pénale, *JO n° 6976* du 25 novembre 2016, p. 1627 et s. (Cette loi a modifié celle n° 2007-04 du 12 février 2007 modifiant le Code de procédure pénale, *JO n° 6332* du 10 Mars 2007) ;
- **Loi** n° 2016-33 du 14 décembre 2016 relative aux Services de renseignement, JO n° 6984 du samedi 07 janvier 2017 ;

Ce renforcement se manifeste par le développement de nouvelles techniques mises à la disposition des investigateurs, inaugurées par les fameuses écoutes téléphoniques, la géolocalisation[10].

2. b. Réponses judiciaires

Présentement, les réponses judiciaires s'apprécient plus avec les lois n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale et n° 2016-33 du 14 décembre 2016 relative aux Services de renseignement.

Par exemple, aux termes des articles 9**0-10 et 90-11 du Code de procédure pénale issus de la loi n° 2016-30**, le juge d'instruction ou l'officier de police judiciaire sur délégation judiciaire ou pendant l'enquête sur autorisation et sous le contrôle du procureur de la République, peut accéder à distance et à l'insu du mis en cause aux correspondance stockées par voie des communications électroniques ainsi que la saisie, l'enregistrement et la copie de ces données. Les données ainsi recueillies, si elles sont utiles à l'investigation, sont jointes au procès-verbal des opérations[11]. Il apparaît que le législateur automatise le régime de la saisie de correspondance électronique en le rendant indépendant de celui des perquisitions.

De même, **l'article 10 de la loi n° 2016-33 du 14 décembre 2016** relative aux Services de renseignement précise que : « *Les services spéciaux de renseignement peuvent, lorsqu'ils disposent d'indices relatifs à l'une des menaces prévues à l'article 2 et en l'absence de tout autre moyen, recourir à des procédés techniques, intrusifs, de surveillance ou de localisation pour recueillir les renseignements utiles à la neutralisation de la menace* ». A travers ce texte, l'on permet au service de renseignement de procéder à une infiltration, géolocalisation pour empêcher ou neutraliser une menace.

NB : Relativement à la jurisprudence, Voir le ***Bulletin d'Information de la Cour suprême du Sénégal***, n° 7-8, décembre 2015, pp. 116 et s.

2. c. Réponses administratives

Au point de vue administratif, le traitement est à apprécier par rapport aux institutions ou structures administratives crées par l'Etat du Sénégal dans le cadre de la lutte contre de la cybercriminalité et la culture de la cybersécurité**.** On peut noter :

---

[10] T. A. NDIOGOU, « Réflexions sur la nouvelle législation sénégalaise antiterroriste », in *Droits fondamentaux*, n° 16, janvier 2018 – décembre 2018 www.droits-fondamentaux.u-paris2.fr

[11] Selon l'article 90- 2 alinéa 1er du Code de procédure pénale sénégalais : « *le juge d'instruction peut opérer à une perquisition ou accéder à un système informatique lorsque les données stockées sont utiles à la manifestation de la vérité* ». Ce pouvoir lui permet de recueillir les indices et preuves des faits visés dans la poursuite, procède à des auditions, en vue d'une éventuelle décision de renvoi devant la juridiction de jugement. Ce même pouvoir est reconnu aux des officiers de police judiciaires agissant sur délégation judiciaire.

- La création d'un Service technique central des chiffres et de la sécurité des systèmes d'information ;
- La création de la Division Spéciale de lutte contre la Cybercriminalité (DSC), ayant son siège à la Division des Investigations Criminelles (DIC) ;
- La création d'une Ecole Nationale de cybersécurité à vocation Régionale (ENCVR) en collaboration avec la France sise dans les locaux de l'Ecole nation d'administration de Dakar[12].
- La Commission de Protection des données (CDP).

Par ailleurs, la stratégie globale destinée à renforcer l'effectivité et l'efficacité de la lutte doit s'accompagner d'un renforcement significatif, en ressources humaines et en crédits d'investissement pour l'administration centrale comme les parquets et juridictions[13].

2. d. Réponses sociétales

L'Etat du Sénégal a un réel besoin d'élaborer une stratégie appropriée qui combine les réponses étatiques et sociétales. Ce faisant, la culture de la cybercriminalité et de la cybersécurité est nécessaire pour tous les citoyens. Pour y parvenir, il est judicieux, entre autres, de sensibiliser et de former non seulement les internautes et des prestataires techniques mais aussi les enseignants et les élèves.

3. Inventaire des manquements au respect des normes des droits de l'homme dans la lutte contre la cybercriminalité et en matière de politiques de cybersécurité

Plusieurs atteintes peuvent cependant être décriées car elles portent un gros coup sur l'équité procédurale et impactent négativement sur la conduite loyale de la procédure[14].

[12] Le CNC qui est une personne de droit public dotée d'un patrimoine, de moyens de gestion et de l'autonomie financière. Cette entité aura pour mission la préservation et la lutte contre la cybercriminalité en vue de promouvoir au Sénégal un environnement numérique de confiance. L'article 4 du décret portant organisation et fonctionnement d'un Centre National de Cybersécurité fait dudit Centre « *le point de contact central national dans les échanges internationaux en matière d'enquête relative à la cybercriminalité*.

[13] M. QUEMENER, « Protéger les internautes, rapport sur le cybercriminalité », Revue du GRASCO, n° 10, septembre 2014, p. 17, disponible sur www.grasco.eu, consulté le 1er décembre 2018 à 12h 18.

[14] L'article 6 alinéa 1er de la loi n°2008-10 du 25 janvier 2008 portant loi d'orientation relative à la société de l'information, a posé les bases d'une cyberéthique en énonçant que le principe de la sécurité « *garantit les droits fondamentaux des personnes et les droits sur les biens et sauvegarde l'ordre public ainsi que les valeurs fondamentales de la société de l'information* ».

3. a. Par rapport à la recherche de preuve

Dans la recherche de la preuve dans l'univers numérique, l'applicabilité des garanties de protection des libertés individuelles et de l'inviolabilité du domicile (la présence de l'inculpé ou du tiers chez qui la perquisition a lieu et l'interdiction de la perquisition de nuit) aux opérations de perquisition électroniques, ainsi que le recours au principe de proportionnalité en matière de saisie électronique, constituent des garanties efficaces pour la protection des libertés individuelles.

Malheureusement, l'élaboration de la politique de modernisation du droit pénal face à la cybercriminalité et à la cybersécurité, ne se soumet pas toujours à ces contraintes de politique criminelle.

D'une part, l'absence de limitation de la durée de l'interception des données par l'autorité, et sur le droit de recours contre la décision judiciaire d'interception, constituent de réels dangers susceptibles de favoriser des atteintes à la vie privée des citoyens.

D'autre part, l'habilitation expresse donnée aux officiers de police judiciaire par l'article 677-39 du Code de procédure pénale pour recourir aux nouveaux mécanismes de recherche de preuve, à savoir l'interception de données de contenu et la conservation rapide de données « *pour les nécessité de l'enquête* », nous parait dangereuse pour les libertés individuelles, dont le seul garant est le juge.

En définitive, les articles 90-4 et 90-17 permet à un juge d'instruction d'ordonner à des « *personnes ayant une connaissance particulière* » d'un système informatique ou d'un service de communication, de chiffrement ou de transmission des données, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder à des données dans une forme compréhensive. Ces articles sont formulés d'une manière imprécise et semblent étendre les pouvoirs d'enquête du juge d'instruction au-delà des données spécifiques concernant un individu ciblé présumé en lien avec l'activité criminelle en cause. Ces pouvoirs semblent en effet s'étendre au fonctionnement même du système informatique, ce qui compromet l'ensemble des données qui y sont relatives.

3. b. Par rapport à la présomption d'innocence

La dialectique liberté/sécurité constitue un enjeu de débat que le principe de présomption d'innocence engendre aujourd'hui puisqu'elle est d'abord un équilibre à trouver entre le droit de la société à se protéger et celui du citoyen à se défendre, lorsqu'il est mis en cause. À cet égard, la présomption d'innocence n'est pas sans diviser la société entre les tenants de la liberté d'une part et les tenants de la sécurité d'autre part.

En clair, cette situation aboutit à une phagocytose de la présomption d'innocence par la présomption de culpabilité.

Parallèlement, une lecture pratique démontre aussi une application quotidienne des effets de la présomption de culpabilité tout en excipant de la présomption d'innocence.

3. c. Par rapport au droit de la défense de l'inculpé

En l'état actuel de notre législation, l'inculpé ne peut pas attaquer immédiatement par voie d'appel la décision du juge d'instruction le plaçant en détention provisoire[15]. Tout ce qu'il peut faire, c'est d'introduire ultérieurement une demande de liberté provisoire pour provoquer la prise d'une ordonnance de refus de mise en liberté provisoire susceptible d'appel[16]. En revanche, lorsque le ministère public requiert la délivrance d'un mandat de dépôt à travers son réquisitoire introductif, le juge d'instruction est tenu. Mais, s'il refuse, il prend une ordonnance de refus susceptible de faire l'objet d'appel. Donc on exclut l'appel de l'inculpé et non du ministère public, ce qui porte atteinte aux droits de la défense d'inculpé.

De surcroît, le juge d'instruction peut aussi imposer aux inculpés l'interdiction de communiquer pour une période de dix jours, cette durée étant renouvelable ; il retarde également l'obtention des permis de visite ou refuse même de délivrer un permis de visite à un membre de la famille de la personne inculpée, ce qui porte atteinte à ses droits.

4. Exploration des atteintes aux droits numériques notamment la liberté d'expression sur internet et les données à caractère personnel

4. a. Sur la liberté d'expression

La loi 2016-29 précitée, à son article 431- 43 incrimine « *l'insulte commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance, l'origine nationale ou ethnique ou la religion ou envers un groupe de personnes qui se distingue par une de ces caractéristiques* ».

En l'absence de définition du mot « *insulte* », cette disposition pourrait être utilisée afin de mettre certaines personnes à l'abri des critiques du public et aurait pour effet d'étouffer la liberté d'expression. Cette disposition pourrait notamment être utilisée pour réprimer les personnes critiques à l'égard de groupes religieux. En 2016, Amnesty International a enregistré au moins deux cas de personnes condamnées pour injures liées à la religion.

[15] Article 90- 16 de la loi n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale portant Code de procédure pénale.
[16] C. DIAKHOUMPA, « Traité théorique et pratique de procédure pénale », 1ère Edition, p. 271.

Aussi, l'article 431-60 de la même loi incrimine la fabrication, l'affichage, l'exposition ou la distribution, par un moyen de communication électronique, de *« tous imprimés, tous écrits, dessins, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images contraires aux bonnes mœurs »*. La notion de « bonnes mœurs » ne fait pas l'objet de définition dans le Code pénal et peut être utilisée pour restreindre la liberté d'expression et réprimer les personnes en fonction de leur orientation sexuelle ou de leur choix vestimentaire.

4. b. Sur les données à caractère personnel

Constitue des données personnelles, toute donnée permettant d'identifier directement ou indirectement une personne[17].

Les opérations de ***collecte des données*** (vidéosurveillance, collecte par internet, téléphone ou formulaire, fichiers du personnel, collecte de données personnelles en cas de recrutement, fichiers de gestion des accès) ou de ***Traitement des données*** (exploitation, archivage, transfert, traitement intelligent des données et les nouveaux usages qui en résultent tel que le Big data, open data, data mining…), attestent une évolution des pratiques dont les avantages sont importants notamment pour les entreprises. Toutefois, ces opérations sont porteuses de risques d'impacts négatifs sur la vie privée (risque de vol des données, usurpation d'identité, cybercriminalité, d'exclusion, de discrimination, de stigmatisation…).

Quelques exemples d'atteintes aux données. La protection de ces données induit premièrement que la personne (morale ou physique) qui traite les données dispose d'une autorisation de la Commission de protection pour traiter les données. Deuxièmement et sans que la liste ne soit exhaustive, ladite personne est tenu d'obtenir le consentement du titulaire des données sauf dispense par un texte légal.

Dans la pratique, l'on constate qu'une quantité importante d'informations sur des personnes physiques sont collectées par des organismes en l'absence d'accomplissement des formalités administratives préalables requises (autorisation de la commission) et même d'information des personnes.

[17] Sont considérées comme des données à caractère personnel, notamment : le nom d'une personne, une photo, un numéro de téléphone, le numéro unique d'identification nationale, un numéro de plaque d'immatriculation, un code, un numéro de compte bancaire, une adresse e-mail, une empreinte digitale, etc. Egalement, il existe une catégorie de données personnelles dites données sensibles dont le législateur a prévu une protection accrue dès lors qu'elles sont collectées ou traitées, il s'agit concrètement des données relatives à la santé, le passé judiciaire, etc.

- **Les vidéosurveillances** dans certains immeubles, magasins, institutions sans informations des personnes et sans autorisation de la commission. Ce sont les images et les voix des personnes qui sont collectées à des fins ignorées par les concernés.
- **Les prospections commerciales** des banques et autres (envois de messages SMS ou Mail pour les promotions de services sans information). Sur ce point, les banques ont initié pour certaines le processus de régularisation. Quant à orange money, il s'est mis en conformité.
- **Les dossiers de recrutement du personnel des structures**. On collecte une quantité d'informations sur les postulants mais aucune information sur le traitement qui est fait suite à l'échec de la sélection. En ce qui concerne, le personnel retenu, le traitement qui est fait des fichiers sur le personnel sans sécurisation parfois (fichiers parfois accessibles à des tiers ou conservés même après le décès du travailleur ou à son départ de la société). A quel moment les détruit-on car en principe on ne peut les conserver indéfiniment ; ce point s'applique également aux banques, à toute structure dès lors que la finalité pour laquelle les données ont été collectées est éteinte, les données doivent soit détruites ou rendues anonymes pour éviter une consultation indue par les tiers…
- **Sur internet**. D'abord sur le **Web,** les logs de connexion sont automatiquement collectés lors d'un passage sur internet et l'historique des pages consultés également. Ces informations constituent l'or noir d'internet, revendu à des sociétés pour leur permettre de cibler des consommateurs pour leurs articles ; ensuite, sur les **Réseaux sociaux** comme Facebook et WhatsApp, l'accessibilité des données publiées par plusieurs pose un problème ; enfin en matière de **Commerce électronique**, les cybermarchands collectent des informations de façon disproportionnée (données non indispensable pour les transactions sollicitées par le client) ;

  NB : Les géants du net, Google (propriétaire de Facebook et de WhatsApp ont entamé la mise en conformité. Sur WhatsApp, par exemple, les données sont maintenant cryptées pour en assurer la sécurité).
- **Le traitement ou la sécurisation des données concernant les sanctions pénales**. Ce sont des informations personnelles dont la divulgation peut nuire à l'individu. En pratique, il y a des incertitudes sur la confidentialité ou la sécurisation de ces données (qui peut y accéder, dans quelles conditions sont-elles conservées ?, etc.).

III. RECOMMANDATIONS

Ces recommandations sont faites dans le but de prendre en compte la protection et la promotion des droits humains dans l'élaboration de la stratégie nationale de cyber sécurité. Mais auparavant, il nous faut en préciser quelques leçons apprises.

1. Leçons apprises

- L'insuffisance d'actions de sensibilisation sur les cybermenaces (aussi bien de la part du Gouvernement que des OSC) ;
- La méfiance des pouvoirs publics ne semble pas faciliter **l'engagement OSC dans les processus décisionnels nationaux clés en matière de cybersécurité et de cybercriminalité ;**
- La faible implication des OSC **en matière de cybersécurité et de cybercriminalité** ;
- La réponse aux cybermenaces appelle la participation de toutes les parties prenantes de la société sénégalaise ;
- Insuffisance de formation des OSC et des citoyens ;
- L'impossibilité pour le Sénégal de vivre en autarcie.

2. Recommandations

Au programme « intégration des droits de l'homme dans le processus d'élaboration de politiques en matière de cybersécurité et de cybercriminalité » au Sénégal

- Travailler à la mise place d'un cadre de concertation spécifiquement répondant aux objectifs du projet ;
- Niveler les connaissances des acteurs de la société civile en termes de renforcement de capacités dans les domaines de **cybersécurité et de cybercriminalité** ;
- Prendre en compte dans l'élaboration des stratégies et actions de l'existant (les atouts comme faiblesses) ;
- Renforcer les capacités de certains citoyens (notamment les chroniqueurs judiciaires, les élèves et enseignant) sur la cyberculture ;
- Niveler les connaissances des autorités publiques sur l'obligation de dialoguer mais aussi sur les législations en matière **cybersécurité et de cybercriminalité**.
- Mettre en place d'un cadre de concertation réunissant les acteurs de la société civile et des membres de la chaîne judiciaire (Magistrats, Officiers de police judiciaires).

A l'ONG JONCTION

- Accompagner les citoyens conformément à la mission de JONCTION et au-delà des objectifs du présent projet ;
- Mettre en place une plateforme pour pérenniser un mécanisme de veille ;
- Evaluer les atouts et faiblesses des politiques dans le but d'apporter une plus-value.