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

Etude critique de la Stratégie Nationale de Cybersécurité du Sénégal

DIOUF Astou,

Experte juridique

Formatrice – Consultante juridique

dioufastou.ecf@yahoo.com

Avril 2019

METHOLOGIE DU TRAVAIL

Dans le cadre de l'étude sur la stratégie nationale de cybersécurité, nous sommes partis d'un vaste travail de recherche de collecte d'ouvrage, de texte législatifs nationaux, communautaires et internationaux auprès des bibliothèques et des centres de documentation.

Nous sommes partis également vers des praticiens et experts en cybercriminalité et cybersécurité dans le but d'entretenir avec eux pour avoir une vision plus claire du phénomène cybercriminel.

Ce travail scientifique nous a donné l'idée de rédiger une étude critique de la Stratégie Nationale de Cybersécurité du Sénégal (SNC 2022) en collaboration avec JONCTION (organisation de promotion et de défense des droits numériques) en vue de permettre une intégration des droits de l'homme dans le processus de cybersécurité et de cybercriminalité.

Cette étude traite cinq points fondamentaux du phénomène cybercriminel et de la cybersécurité du Sénégal.

- **Explorer la stratégie nationale du Sénégal en matière de cybersécurité et de cybercriminalité**

Dans des pays africains comme le Sénégal, la cybercriminalité a pendant longtemps été considérée comme une criminalité spécifique aux pays développés. Cette approche classique était légitimée par le faible taux de pénétration des TIC en Afrique et par la fracture numérique séparant les Etats développés de ceux en développement. Mais l'ascension fulgurante des TIC et la généralisation progressive de l'accès au réseau Internet au Sénégal, à partir des années quatre-vingt-dix, se sont accompagnées de l'émergence d'une criminalité informatique facilitée par le développement de la société sénégalaise de l'information[1].

Depuis la connexion officielle du Sénégal au réseau Internet en 1996[2], sa connectivité n'a cessé de s'améliorer, en raison de l'élargissement progressif de la bande passante de liaison qui est l'une des plus importantes de l'Afrique de l'Ouest.

L'extension récente de l'intranet gouvernemental aux autres régions du Sénégal ainsi que le démarrage des activités du troisième opérateur de télécommunication, ont fini par placer la vision du e-Sénégal au cœur de la stratégie plus globale déclinée par le Plan Sénégal Emergent (PSE) qui a identifié l'accélération de la diffusion des TIC comme un des « fondements de l'émergence »[3]. Ces progrès ont d'ailleurs valu à notre pays de se voir confier le volet TIC dans le cadre du Nouveau Partenariat pour le Développement de l'Afrique (NEPAD).

[1] Au Sénégal, en l'absence de la tenue d'un système fiable des statistiques criminelles, il n'existe pas, à notre connaissance, de chiffres sur les cyberinfractions commises ou poursuivies, en ce sens. Le secteur de la justice et l'Etat de droit : Une étude *d'AFRIMAP et de l'Open Society Initiative for West Africa (OSIWA*), novembre 2008, p. 12, cité par P. A. TOURE, *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal*, l'Harmattan, p. 18.

[2] La Société nationale des télécommunications (SONATEL), filiale de la multinationale française France Télécom, avait mis en place une ligne spéciale à 64 kbps reliant le Sénégal aux USA, avant de signer avec la société américaine MCI un accord permettant la connexion internationale à l'Internet. L'on a assisté ainsi au coup d'envoi de l'ère Télécom Plus, dont le premier client fut la présidence de la République. Sur l'ensemble de la question, A. BA, *op. cit*, p. 110, cité par P. A. TOURE, *op. cit*, p. 16.

[3] Voir Plan Sénégal Emergent, p. 80.

L'informatique, « science de traitement automatique et rationnel de l'information en tant que support des connaissances et des communications »[4], les technologies de communication ont donné naissance à l'Internet[5], « la toile d'araignée mondiale »[6].

Sur ce, il ressort de l'article 3 de la loi sénégalaise n° 2011-01 du 24 février 2011 portant Code des Télécommunications que la notion de *technologies*[7] *de l'information et de la communication* renvoient à des *« technologies employées pour recueillir, stocker, utiliser et envoyer des informations et incluent celles qui impliquent l'utilisation des ordinateurs ou de tout système de communications y compris de télécommunications* ». De plus, les technologies de l'information peuvent s'entendre, pour reprendre une définition donnée par le conseil des communautés européennes[8], de l'ensemble des *« systèmes, équipements composants et logiciels*

[4] Le petit Larousse illustré, Larousse HER 2000, p. 546.

[5] Le mot *« Internet »* est composé du préfixe « Inter » qui indique un lien entre deux éléments et le mot *« Net »* qui est traduit de l'anglais par *« réseaux »*. Internet est alors un lien entre deux ou plusieurs réseaux informatiques, *« un réseau de réseaux »*. En fait, il s'agit du plus grand réseau informatique de la planète. Il regroupe une multitude de réseaux régionaux, gouvernementaux et commerciaux. Tous ces réseaux discutent entre eux par le biais du même protocole de communication, TCP/IP (*transmission* Control Protocol Over Internet Protocol). La connexion est effectuée par l'utilisation de lignes, des câbles, et des satellites comme joint des lignes téléphoniques. Contrairement aux appels téléphoniques traditionnels, qui transmettent l'information par le circuit commutation. L'Internet transmet l'information par la *« paquet commutation »* ; dans ce mode, les communications sont changées aux petits signaux. Après ils sont envoyés aux paquets de bénéficiaire avec arrivant à leur destination par les routes différentes, la communication est alors reconstruite à la fin du récepteur. Sur ces points V. K. HAFNER : *Where Wizards Stay Up Late : The Origins of the INTERNET* (N.Y., TOUCHSTONE) , [1996] p. 12; J. NAUGHTON: *A Brief History of the Future: From Radio Days to Internet Years in a Lifetime* (N. Y. , WoodStock) , [1999] p. 140; A. BRIGGS: *A Social History of the Media: From Gutenberg to the Internet* (Cambridge, Polity Press) , [2002] pp. 311 et s. Selon une étude réalisée par l'Aftel (Association française de télématique), la France comptait en 1998 plus d'un million d'utilisateurs d'Internet. Le nombre d'ordinateurs raccordés au réseau mondial est passé de 198 000 ordinateurs en juillet 96 à 321 000 en juillet 97, soit une progression annuelle de 62 %. Au niveau global, l'Internet avait plus de 100.000 million des utilisateurs et accessible par plus de 100 Etats. V. *A. F-N VOLUNTEER* ; An Introduction to the Internet. Disponible sur : <http://www.austinfree.net/> (2/3/2001), sur l'ensemble de cette question, V. M. CHAWKI, in « Essai sur la notion de cybercriminalité », IEHEI, juillet 2006, ibid.

[6] D. SOW, « Retour sur l'adaptation du droit au numérique », Revue CAMES/SJP, n°001/2016, p. 77-100.

[7] Les instruments technologiques renvoient : D'une part, aux technologies dites « classiques » de la première moitié du XXe siècle que sont la radio, la télévision, le télex, le télégraphe et le téléphone, qui assurent essentiellement une fonction de transmission et de diffusion de l'information par la voie des ondes hertziennes. D'autre part, les TIC désignent surtout les technologies « nouvelles » ayant pour support le numérique, considéré comme le procédé technique permettant la transcription de l'information sous forme binaire. Les technologies numériques regroupent notamment les ordinateurs, les cartes bancaires, les programmes informatiques, les Smartphones, les tablettes numériques et les réseaux électroniques nés du besoin d'interconnexion des ordinateurs. Cette distinction importante est faite par le professeur P. A. TOURE, *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal », op. cit., p. 20.*

[8] Décisions du 22 décembre 1986 relative à la normalisation dans le domaine des technologies de l'information et des télécommunications JO des Communautés Européennes, cité par ND. DIOUF, *« Infractions en relation avec les Nouvelles technologies de l'information et procédure pénale : l'inadaptation des réponses nationales face à un phénomène de dimension internationale »* disponible sur *www.ohada.com* consulté le 26 novembre 2018 à 15 h 28 ; Selon le PNUD, *« Les NTIC sont des outils de traitement de l'information, un ensemble hétéroclite de biens, d'applications et de services qui sont utilisés pour produire, stocker, traiter et diffuser l'information (…) »*. Cette définition est citée par P. DANDJINOU, « Les nouvelles technologies de l'information et de la communication (TIC) et les Objectifs du millénaire pour le développement en Afrique », in *« L'Afrique et les Objectifs du*

qui sont nécessaires pour assurer la recherche, le traitement et le stockage de l'information dans tous les domaines de l'activité humaine et dont la mise en œuvre fait généralement appel à l'électronique et aux technologies similaires ». Il s'agit donc, des équipements, dispositifs et programmes ayant pour objet le stockage, le traitement, la transmission et la communication de l'information.[9]

Etant indispensable à la vie, l'utilisation des TIC dans de nombreux domaines de la vie quotidienne, a conduit à introduire le concept moderne de « *société de l'information* », modèle de société qui offre d'immenses possibilités. Ainsi, mettre l'information en libre accès, c'est la retirer des mains du pouvoir central, et donc renforcer la démocratie.

Cependant, comme l'enseignait le doyen Jean Carbonnier, ***« l'évolution des mœurs et des techniques donne naissance à de nouvelles formes de délinquance*** »[10]. La plupart des grandes découvertes technologiques ont engendré presque toujours, à côté des progrès économiques qu'elles procurent à l'humanité, des retombées négatives parmi lesquelles figures en bonne place l'avènement de nouvelle forme de criminalité dénommée sous le vocable de cybercriminalité[11].

millénaire pour le développement en Afrique », PNUD 2003, p. 552, in, P. A. TOURE, *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal »*, *ibidem.*

[9] L'information est un nom commun féminin issu du latin informatum, et signifie selon le Dictionnaire Le Robert, un renseignement ou un événement qu'on porte à la connaissance d'une personne, d'un public. Dans une seconde acception, l'information est définie comme ce qui peut être transmis par un signal ou une combinaison de signaux (message) selon un code commun et par un canal et ce qui est transmis est matérialisé comme étant l'objet de connaissance ou de mémoire. Autrement dit, un simple signal peut constituer une communication, un code en est un symbole. A titre d'illustration, les feux tricolores en matière de code de la route. De plus, l'idée de transmettre la connaissance par « le système de bouche-à-oreille », ou « téléphone arabe » est une autre manière de communiquer et c'est le moyen grâce auquel les personnes qui ont reçu cette information se cultivent et l'enregistrent. Sur cette question, V. T-B. A. JEANINE, *La répression de la cybercriminalité dans les Etats de l'Union européenne et de l'Afrique de l'ouest*, Thèse de Doctorat-2014/2015, p. 18.

[10] J. CARBONNIER, *Sociologie juridique*, Paris, *PUF*., 1978, p. 401.

[11] J. CAZENEUVE, « La cybercriminalité : l'émergence d'un nouveau risque », Act. Jur. Pén, 2012, p. 268 et s.

La cybercriminalité[12] a, d'une part, été définie par des instruments juridiques internationaux, communautaires[13], d'autre part, des Institutions[14] comme l'O.N.U. La « cybercriminalité » doit recouvrir « 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 « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique ».

En droit sénégalais, les rédacteurs de la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité ont semblé la définir comme *« toute infraction qui implique l'utilisation des technologies de l'information et de la communication »*[15]. Cette définition du cybercrime n'est pas éloignée de celle retenue par le droit pénal camerounais. Selon la loi n° 2010-12 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun[16], la cybercriminalité est *« l'ensemble des infractions s'effectuant à travers le cyberespace par des moyens autres que ceux habituellement mise en œuvre et de manière complémentaire à la criminalité classique ».*

La cybercriminalité n'est ni un phénomène criminel sénégalais ou africain et le Professeur Abdoullah CISSE écrira que « ***l'Afrique a souvent tendance à développer des réponses locales à des questions d'importance globale ».***

Conscient de cela, le Sénégal considère que sa Stratégie Nationale de Cybersécurité (SNC 2022) s'avère importante dans le but de guider les actions de l'Etat concernant la cybersécurité tout

[12] Il y a deux grandes catégories de cybercrimes : La première catégorie est celle où l'ordinateur est l'objet du crime. Cette cybercriminalité consiste en crimes précis, liés à des ordinateurs et à des réseaux. Ce sont de nouveaux actes criminels qui sont expressément liés à la technologie informatique et à Internet. Nous pouvons citer le piratage ou l'utilisation illicite de systèmes informatiques, la défiguration de sites Web ou la création et la propagation malveillante de virus informatiques. La seconde est celle où l'ordinateur est l'instrument de perpétration. Elle comprend les crimes que les organismes de maintien de l'ordre ont combattu dans le monde matériel, mais doivent combattre aussi, aujourd'hui, de plus en plus, dans le monde virtuel d'Internet, qu'il s'agisse de pornographie enfantine, de harcèlement criminel, de fraude, de violation de la propriété intellectuelle ou de vente de substances ou de produits illicites, in « Guide pratique des risques liés à la cybercriminalité envers les enfants », L. KJIRI, Publications de l'Organisation islamique pour l'Education, les Sciences et la Culture –ISESCO 1433H/2012A.D, p. 13.

[13] La cybercriminalité recouvre « 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 « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique », définition donnée par l'ONU, cité par M. CHAWKI in « Essai sur la notion de cybercriminalité » *IEHEL*, juillet 2006 ; *http://www.ieh.org* ,consulté le 28 novembre 2018 à 13h 10.

[14] V. Onzième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, Bangkok, 18-25 avril 2005, disponible sur *www.un.org*, consulté le 20 novembre 2018 à 12h 5.

[15] 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.

[16] Journal officiel de la République du Cameroun du 21 décembre 2010, p. 3 et s, Voir, *note de bas de page* 20.

en proposant une vision aux sénégalais, y compris aux organismes des secteurs privé et public, tout comme aux institutions universitaires, à la société civile et à d'autres parties prenantes.

La stratégie considère la cybersécurité comme la protection des systèmes d'information, des données qui y sont incluses ainsi que des services qu'ils fournissent ou sur lesquels ils s'appuient, contre tout accès, modification, entrave, destruction ou usage illicites.

Dans le but de faciliter la mise en œuvre du dispositif d'entraide judiciaire prévu et de garantir la rapidité d'intervention des services répressifs, l'article 35 de la Convention sur la cybercriminalité a obligé les Etats à désigner « *un point de contact joignable 24 heures sur 24, sept jours sur sept* »[17]. Il est destiné à garantir la fourniture d'une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale.

Selon la Convention de Budapest[18], l'essentiel est que le point de contact désigné soit capable d'agir en coordination avec les autorités responsables de l'entraide internationale ou de l'extradition dans l'Etat selon une procédure accélérée.

Enfin, le § 3 de l'article 35 de la Convention impose à chaque point de contact du réseau d'être opérationnel et de *« disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau* ».

- **Analyser le traitement du phénomène de la cybersécurité et les réponses étatiques (législatives ; judiciaires ; administratives) et sociétales (sensibilisation ; éducatives ; plaidoyer).**

En politique criminelle[19], « traiter » un phénomène cybercriminel consiste à y apporter une réponse de politique criminelle, c'est-à-dire une « *réponse organisée, voulue ou acceptée, en*

[17] Dans le cadre de la mise en place de ce réseau, qui *« figure parmi les moyens les plus importants prévu par la Convention »*, chaque partie à toute latitude pour décider de la place du point de contact 24/7 dans l'organigramme de ses services répressifs. Il peut ainsi s'agir d'un service administratif ou d'un service de police spécialisé dans la lutte contre la criminalité i informatique. Le Sénégal envisage de créer un Centre National de Cybersécurité (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 projet de décret portant organisation et fonctionnement d'un Centre National de Cybersécurité a fait dudit Centre « *le point de contact central national dans les échanges internationaux en matière d'enquête relative à la cybercriminalité »*, cité par P. A. TOURE, *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal*, *op. cit.*, p. 544.

[18] Convention européenne de Budapest sur la cybercriminalité du 23 novembre 2001.

[19] Selon M. DELMAS-MARTY, la politique criminelle comprend « *l'ensemble des procédés par lesquels le corps social organise les réponses au phénomène criminel* ».

tout cas codée par la société »[20]. D'une manière beaucoup plus large, on peut retenir la politique criminelle comme l'ensemble des procédés par lesquels le corps social organise les réponses au phénomène criminel. Il s'agit non seulement des procédés répressifs, mais aussi de tout autre procédé[21].

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

Pour cela, l'Etat du Sénégal, dans le cadre de sa mission régalienne a adapté son système juridique à l'évolution moderne des technologies de l'information de la communication en apportant des réponses législatives, judiciaires, administratives et sociétales.

1- Les réponses législatives :

Conscient de l'inadaptation de la législation sénégalaise par rapport aux particularités de la délinquance numérique, le législateur sénégalais avait, en date du 25 janvier 2008, entrepris un vaste chantier de réforme du cadre juridique des technologies de l'information et de la communication avec l'adoption d'un arsenal juridique presqu'intégral de lutte contre la cybercriminalité. Il en est ainsi de la loi portant loi d'orientation sur la société de l'information[22], de la loi sur la cybercriminalité[23], de la loi sur la protection des données à caractère personnel[24] et enfin de la loi sur les transactions électroniques[25].

[20] M. DELMAS-MARTY, *Modèles et mouvements de politique criminelle*, Paris, *Economica*, 1983, p. 41.
[21] Sur l'ensemble de la question, voir, P. GUEYE, *Criminalité organisée, Terrorisme et cybercriminalité : Réponses de politiques criminelles,* L'harmattan -Sénégal 2018, p. 35.

[22] 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, p. 419 et s.).

[23] Loi n° 2008-11 du 25 janvier 2008, portant sur la cybercriminalité (JORS, n°6406 du 03 mai 2008, p. 419) (annexe n°1).

[24] Loi n° 2008-12 du 25 janvier 2008, sur la protection les données à caractère personnel (JORS, n°6406, du 3 mai 2008, p.434).

[25] Loi n° 2008-08 du 25 janvier 2008, sur les transactions électroniques (JORS, n° 6404 du 26 avril 2008, p. 395).

De plus, le législateur sénégalais en marche vers le Droit de l'informatique a posé les jalons les plus significatifs de cette discipline en mettant en œuvre des décrets d'application pour conforter les quatre lois du 25 janvier 2008[26].

Par ailleurs, on constate que depuis l'avènement de la législation sur la cybercriminalité, le phénomène cybercriminel prend de plus en plus d'ampleur. Ce qui a permis au le législateur sénégalais de renforcer son dispositif législatif par un élargissement des pouvoirs du juge d'instruction ou de l'Officier de police judiciaire agissant sur délégation judiciaire dans le cadre de l'investigation des faits cybercriminels par le biais d'une adoption de trois lois au cours de l'année 2016[27]. Il ressort également de ces lois, une approche originale de Co régulation du cyberespace en esquissant une démarche de politique criminelle participative avec les prestataires techniques.

Egalement, l'essor des contenus illicites sur les réseaux sociaux constitue une véritable menace pour le développement d'une société de l'information à dimension éthique. L'impérieuse nécessité de lutter contre ces contenus préjudiciables a conduit le législateur sénégalais à adopter le nouveau Code sur les communications électroniques.[28]

En outre, à cause de la dimension transnationale d'Internet et de la mondialisation des services, un nombre croissant de cyber délits revêtent une dimension internationale. Les Etats africains ont adopté des approches voire des réponses communautaires.

---

[26] 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) ; 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° 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).

[27] Il s'agit notamment de la loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal (JORS n°6975) ; Loi n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale (JORS n°6976) ; Loi n° 2016-33 du 14 décembre 2016, relative aux services de renseignement (JORS, n° 6984 du 07 janvier 2017).

[28] Loi votée par l'Assemblée nationale du Sénégal le mercredi 28 novembre 2018.

D' abord, la CEDEAO s'est dotée d'une directive portant sur la cybercriminalité[29], des Actes additionnels sur à l'harmonisation des politiques et cadre réglementaire du secteur des Technologies de l'Information et de la Communication (TIC)[30], sur transactions électroniques dans l'espace de la CEDEAO[31], sur transaction numérique dans l'espace de la CEDEAO[32] et enfin sur protection des données à caractère personnel dans l'espace de la CEDEAO[33].

Ensuite, les Chefs d'Etats et de gouvernement de l'Union Africaine ont adopté la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, lors de la réunion des 26 et 27 juin à Malabo en Guinée équatoriale[34]. La convention de Malabo consacre son chapitre III à la promotion de la cybersécurité et à la lutte contre la cybercriminalité. Elle oblige les Etats membres signataires à adopter une politique nationale de cybersécurité et à mettre en place des institutions spécifiques en la matière.

Par ailleurs, conscient de la complexité du phénomène cybercriminel, le Sénégal avait entrepris une longue procédure qui a conduit à l'adoption de la Convention de Budapest qui est la seule réglementation internationale complète, contribuant à appréhender la dimension internationale de la cybercriminalité. Ainsi, le 23 novembre 2001, le Conseil de l'Europe a adopté à Budapest une Convention sur la cybercriminalité. La Convention est entrée en vigueur le 1er 2004. Cette convention constitue la première à vocation universelle destinée à lutter contre le cybercrime. Elle s'est fixée comme objectif d'améliorer la coopération internationale, notamment en matière d'extradition[35] et d'entraide répressive

2- Les réponses judiciaires

[29] Directive de la C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

[30] Acte additionnel A/SA du 19 janvier 2007 de la CEDEAO relatif à l'harmonisation des politiques et cadre réglementaire du secteur des Technologies de l'Information et de la Communication (TIC).

[31] Acte additionnel A/SA. 2/01/10 du 16 février 2010 portant transactions électroniques dans l'espace de la CEDEAO.

[32] Acte additionnel du 02 octobre 2009 portant transaction numérique dans l'espace de la CEDEAO.

[33] Acte additionnel du 02 octobre 2009 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO.

[34] Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel signée à Malabo en Guinée équatoriale le 27 juin 2014.

[35] Selon l'article 24 de la Convention de Budapest subordonne l'extradition pour les infractions pénales définies par ladite Convention à condition « *qu'elles soient punissables dans la législation des deux parties concernées par une peine privative de liberté pour une période maximale d'au moins un an ou par une peine plus sévère* ». Il résulte de cette disposition que les faits cybercriminels objet de la demande d'extradition doivent donc être punissables dans les deux pays, mais aussi une exigence tirée de la gravité des cyberinfractions.

L'irruption de ce nouveau phénomène qu'est Internet, utilisé à toutes les sauces et dans toutes les circonstances, caractérisé par la transnationalité, l'immatérialité[36], la volatilité et l'anonymat de ses acteurs a contribué à brouiller les repères du système processuel dont les réponses traditionnelles et permanentes, conçues et élaborées pour un environnement matérialisé et national, se sont vite révélées inappropriées et inadaptées pour saisir cette nouvelle réalité de l'ère numérique. Cette inadaptation des choses incorporelles, immatérielles a permis à L. KALINA de soutenir à ce propos qu'en Afrique : « *au désert numérique s'ajoute donc, effectivement, un véritable désert juridique l'un expliquant l'autre*[37].

Cette nouvelle forme de criminalité pose de nouveaux enjeux à l'enquête judiciaire[38]. Comment les services répressifs vont-ils pouvoir localiser les données dans les *« nuages »* ? Comment identifier le prestataire assurant le stockage des données nécessaires à la manifestation de la vérité ?

Face à ces enjeux stratégiques, à la complexité du phénomène cybercriminel, le législateur sénégalais a apporté des réponses judiciaires.

Celles-ci s'apprécient plus avec la loi n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale. Il ressort de l'exposé des motifs de cette loi, un renforcement des pouvoirs du juge d'instruction et des prérogatives de l'officier de police judiciaire dans la collecte des preuves en cas d'infraction en matière de cybercriminalité. Cette option s'est manifestée notamment par l'institution de mesures d'investigation au moyen des TIC et par l'organisation des procédés d'interceptions de correspondances.

Selon l'article 90- 2 alinéa 1er du Code de procédure pénale[39] 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

---

[36] L'immatérialité est ce qui caractérise Internet. Ce dernier véhicule les biens immatériels, choses que l'on ne peut pas toucher, qui n'ont pas de consistance physique, tels que les données informatiques, les systèmes de traitement des données, les sites et leur contenu, fichiers, logiciels, bases de données, programmes, ou encore le temps de connexion, l'électricité, l'énergie… par Mme V. JAWORSKI et Mlle S. CORIOLAND, « *Droit pénal de l'Internet-Aspects de fond et de procédure* » ; *www.docplayer.fr/18706099-Droit-penal-de-l-internet-aspects-de-fond-et*.. , consulté le 10 novembre 2018 à 10H 5.

[37] L. KALINA, « Afrique et la cybercriminalité : sortir du désert juridique », 3 mars 2006 : http://www.blogg.org/blog-35519-thems-semaine-afrique-et-cybercriminalité-64801.html, cité par P. A. TOURE, *Le traitement de la cybercriminalité devant la juge, l'exemple du Sénégal, op. cit,* p. 461.

[38] A. SEGER, « Le cloud computing, les défis rencontrés par les autorités de répression », in « *Coopération contre la cybercriminalité », conférence Octopus Interface,* 23-25 mars 2010 : http://www.coe.int , P. A. TOURE, *Le traitement de la cybercriminalité devant la juge, l'exemple du Sénégal*, *ibidem*.

[39] La loi n° 2016 -30 du 08 novembre 2016 modifiant la loi n° 65- 61 du 21 juillet 1965 portant Code de procédure pénale.

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 officiers de police judiciaires agissant sur délégation judiciaire.

Egalement, les articles 90-4 et 90-17 de la loi de 2016 portant modification du Code de procédure pénale permettent 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.

De plus, l'article 10 de la loi de 2016 relative aux services de renseignement[40] prévoit 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* ». On permet ici à des services de renseignement de procéder à une géolocalisation pour empêcher ou neutraliser une menace.

En outre, le Sénégal considère que c'est bien d'avoir des instruments au plan national et communautaire, mais juge aussi nécessaire la coopération à l'échelle internationale en ratifiant la Convention internationale de Budapest sur la cybercriminalité[41].

Avec Budapest, les autorités policières et judiciaires pourront obtenir l'assistance des acteurs globaux d'Internet comme Facebook, YouTube, Google, Gmail dans leurs investigations. Obtenir également le retrait d'une vidéo compromettante mise en ligne via YouTube ; adresser une réquisition d'identification du titulaire d'un compte Yahoo impliqué dans la commission d'un délit voire même le blocage d'un compte Facebook diffusant des contenus illicites.

En réalité de l'avis de P. A. TOURE, tous les chemins de la lutte contre l'impunité qui sévit dans le cyberespace mènent à Budapest, après des escales à Abuja et à Malabo faisant ainsi référence à la Directive de la CEDEAO et à la Convention de l'Union africaine.

3- Les réponses administratives

[40] Loi n°2016-33 du 14 décembre 2016 relative aux Services de renseignement, J.O. N° 6984 du samedi 07 janvier 2017.

[41] Convention sur la cybercriminalité du 23 novembre 2001, appelée Convention de Budapest du Conseil de l'Europe.

Le traitement du phénomène cybercriminel du point de vue administratif est à apprécier par rapport aux institutions administratives crées par l'Etat du Sénégal dans le cadre de la lutte contre la cybercriminalité et la culture de la cybersécurité**.**

On peut noter la création de la Brigade Spéciale de lutte contre la Cybercriminalité (DSC) en 2013, ayant son siège à la Division des Investigations Criminelles (DIC). Le dispositif de lutte au sein de la police sénégalaise a connu des changements. Une division Spéciale de cybersécurité a été créée par la coopération franco-sénégalaise, laquelle a intégré en son sein l'ancienne Brigade Spéciale de lutte contre la cybersécurité[42].

La création d'une Agence de l'Informatique de l'Etat (ADIE)[43].

La création d'une Commission de Protection des Données Personnelles (CDP)[44].

Aussi, il ressortait du discours du président de la République Macky SALL dans le cadre de la « *Journée des forces armées* », au camp Dial DIOP du samedi 10 novembre 2018, que l'Etat du Sénégal ne cédera pas face aux dérives sur le net. Il annonce également la création d'une Ecole Nationale de cybersécurité à Vocation Régionale (*ENCVR*) en collaboration avec la France sise dans les locaux de l'Ecole nationale d'administration de Dakar. Il avait au préalable soutenu les mêmes propos lors de la cérémonie d'ouverture de la 5^{e} édition du Forum de Paix et Sécurité de Dakar.[45] L'importance de cette institution est de permettre le renforcement des capacités techniques afin de « *former et de sensibiliser les agents de l'Etat* » du Sénégal et de la Sous-région à la « *protection du secret, la sécurité des systèmes d'information et de cybersécurité* ».[46]

4- Les réponses sociétales

La cybercriminalité soulève sur le plan sociétal des questions d'autant plus difficiles à résoudre qu'elle affecte toute une société globalisée.

---

[42] , P. GUEYE, *Criminalité organisée, Terrorisme et cybercriminalité : Réponses de politiques criminelles,* L'harmattan -Sénégal 2018, p. 364.

[43] Décret 2004- 1038 du 23 juillet 2004 portant création et fixant les règles d'organisation et de fonctionnement de l'Agence de l'Informatique de l'Etat (ADIE).

[44] La Commission de protection des Données Personnelles (CDP) est une Autorité Administrative Indépendante (AAI) instituée par la loi 2008-12 du 25 janvier 2008 sur la protection les données à caractère personnel.

[45] Le 6 novembre 2018 à Dakar.

[46] Disponible sur www.rfi.fr.

Sur ce, il nécessite une sensibilisation mondiale voire sénégalaise des internautes, des prestataires techniques. La sensibilisation consiste surtout à informer les internautes de la nécessité d'instaurer des Codes de conduite, mais également à sensibiliser les différents acteurs sur le rôle qu'ils peuvent jouer pour éviter que les crimes informatiques soient commis, pour faire éviter aux internautes, surtout aux mineurs, des dommages ou traumatismes. Les autorités publiques, surtout dans le cadre de la lutte contre la criminalité informatique organisée, doivent mettre en œuvre des règles de conduites permettant de se prémunir de certaines attaques, de vol de données ou d'information , de harcèlements ou de chantage. Une bonne campagne de sensibilisation à l'endroit des usagers constitue un important moyen de prévention[47].

Il importe de noter que la sensibilisation doit être élargie à toutes les couches de la population, notamment les jeunes, les parents et les enseignants, en vue de leur faire comprendre les dangers liés à l'Internet. La sensibilisation porte non seulement sur les risques spécifiques qu'Internet présente, mais également sur les moyens de protection qui existent pour s'en prémunir. Cette sensibilisation s'articule autour de quatre lignes[48] qui sont : l'éducation aux médias, le rôle des parents, l'école et la nécessité d'une collaboration entre le public et le privé.

C'est pourquoi le développement rapide des TIC nous oblige donc à former aussi bien les enseignants que les élèves à ces nouvelles compétences. Or, il apparaît que l'adaptation aux usages des TIC en classe est trop lente. « *Si le système scolaire offre si peu de performance, c'est peut- être qu'il constitue l'un des derniers bastions où les technologies de l'information et de la communication (TIC) n'ont pas été encore véritablement intégrées* »[49]. De plus en plus d'écoles se voient dotées de nouveaux outils technologiques. Cependant, un nombre important d'enseignants se sentent démunis ou à l'écart face à ce nouveau matériel.

Sur ce, pour une bonne infocompétence, *le Dr. P. GUEYE soutenait que : « les Etats de l'Afrique de l'Ouest doivent renforcer les cours d'informatique dans les écoles. Ces cours ne doivent pas se limiter à la connaissance, à la compréhension et aux compétences en informatique, mais doivent comprendre aussi l'acquisition des compétences techniques de protection de base. Ils doivent être programmés à tous les niveaux d'enseignement pour permettre aux enfants de comprendre les enjeux et les risques afin de se projeter sur les moyens*

[47] Sur l'ensemble de la question, voir, P. GUEYE, *Criminalité organisée, Terrorisme et cybercriminalité : Réponses de politiques criminelles*, L'harmattan -Sénégal 2018, p. 330.
[48] Instruments juridiques pour lutter contre le racisme sur Internet. Voir « Soft Law », Conseil de l'Europe, http://www.coe.int/t/dghl/monitoring/ecri/ legal research/combat-racisme-on-internet-chapitre 5-fr.asp ?toPrint=yes§, cité par P. GUEYE, in *Criminalité organisée, Terrorisme et cybercriminalité : Réponses de politiques criminelles*, p. 332.
[49] Bibeau (1999, p. 2).

de protection. Ces derniers sont nécessaires car les technologies et l'Internet sont devenus incontournables dans la vie sociale et la promotion sociale »[50].

Donc, la culture[51] de la cybercriminalité est nécessaire pour tous les citoyens. C'est la raison pour laquelle, le point 4.3 relatif aux objectifs de la stratégie, notamment la promotion de la culture de la cybersécurité au Sénégal prévoit que « *la réussite d'un Sénégal numérique s'appuiera sur la confiance des organisations et des particuliers en matière des services en ligne. Le Gouvernement devra alors travailler avec les secteurs public et privé afin d'augmenter la connaissance et la compréhension des cybermenaces auxquelles sont confrontés le Sénégal et les sénégalais* ».

Le cyberespace constitue une causalité en boucle ouverte, due à l'interface homme-cyberespace-temps. L'être humain découvre en lui-même un nouveau niveau de perception grâce à son interaction avec l'ordinateur, qui affine ses potentialités par l'interaction avec l'être humain.

- **Faire l'inventaire des manquements au respect des normes des droits de l'homme dans la stratégie nationale de cybersécurité du Sénégal**

[50] P. GUEYE, *Criminalité organisée, Terrorisme et cybercriminalité : Réponses de politiques criminelles,* L'harmattan -Sénégal 2018, p. 334.

[51] Selon M. GIBSON, la cyberculture se vit fantastiquement dans le cyberespace « comme un dépassement des limites et tout particulièrement des frontières du corps et de la chair qui sont encombrants dans les voyages ». Et selon M. LEMOS la « *cyberculture* » est la jonction paradoxale entre la technique et la culture. Cette liaison est un des enjeux important de nos sociétés actuelles. Il ne s'agit pas d'une culture « *rationalisée* » mais plutôt l'appropriation de la technique par la culture. Selon cet auteur la « cyberculture » est un : « Ensemble d'attitudes nées à partir du mariage entre les technologies informatiques et les médias de communication. Cet ensemble d'attitudes est le produit d'un mouvement socioculturel pour apprivoiser et humaniser les nouvelles technologies ». Pour le philosophe P. LEVY, la cyberculture n'est pas la culture des fanatiques d'Internet c'est une transformation profonde de la notion même de culture. Il déclare : « Et c'est difficilement séparable des autres transformations sociales que nous connaissons depuis 20 à 25 ans: l'urbanisation galopante; la montée du niveau d'éducation; la mondialisation économique; le développement des contacts entre cultures. L'humanité est en train de se rencontrer elle-même. Internet est pour moi une espèce de matérialisation de l'universel sans totalité », c'est qu'il n'y a pas de centre du réseau, il n'y a pas de sens unique. Chaque fois que vous avez un nouveau nœud dans le réseau, un nouveau site, un nouveau groupe de discussion, un nouvel abonné, vous avez une nouvelle source d'hétérogénéité et de diversité. Depuis dix ans, vous avez de plus en plus de langues, de thèmes abordés, de pays concernés. C'est un processus absolument passionnant à observer. Cette culture est donc l'union de la culture *« poste moderne* » et du développement des NTIC. « L'institutionnalisation se transforme en tribalisme, le contrat en objectifs ponctuels, la positivité en non-finalité et l'utopie en quotidien le plus urgent ». Sur ces points voir. M. GIBSON, op. cit., p. 57 ; C. HEBRARD, précité, voir aussi sur ce point J. HUET : Quelle Culture dans le Cyberespace et quel Droit Intellectuel pour cette Cyberculture (Paris, Chron.), [1998] p. 185 ; Le Temps : Comment l'Intelligence Collective Peut Surgir Sur le Net (Entretien avec Pierre Lévy), [22 février 2001] ; C. HEBRARD, précité. Pour plus de précision voir. M. CHAWKI, *op. cit.*, p.14.

[51] STRATÉGIE NATIONALE DE CYBERSÉCURITÉ DU SÉNÉGAL (SNC2022), novembre 2017.

Certains points de la stratégie nationale de cybersécurité porte atteinte aux droits de l'homme. Il s'agit notamment :

Du point 4.4.2.2 relative à la mise en place des formations obligatoires liées aux investigations numériques et à la manipulation des preuves pour le personnel des services de sécurité, des autorités judiciaires et autres organismes œuvrant dans la détection et la poursuite d'actes de cybercriminalité.

Même s'il est bien d'investiguer dans le cyberespace, cette action doit être faite par des personnes opérationnelles et qualifiées. Il s'avère important de noter qu'au-delà des risques d'atteintes aux principes généraux du droit, les moyens technologiques modernes d'investigation posent des enjeux liés aux risques d'atteinte aux droits fondamentaux de la personne. Il s'agit notamment du droit au respect de la vie privée et de la confidentialité des correspondances.

En effet, « *l'efficience des moyens technologiques modernes d'investigation, en matière de données numériques et de recherche d'informations présente le risque d'aller au-delà du seul but poursuivi par l'enquête, notamment en matière d'atteinte aux droits* », pour reprendre les propos du professeur Nd. DIOUF.

Alors que, dans un État de droit, il n'est pas concevable que les autorités judiciaires bénéficient de toute latitude quant à l'organisation de l'enquête pénale et agissent au mépris des valeurs constituant les fondements d'un État démocratique. Ainsi, la recherche de la vérité n'est pas sans limite, la première tenant « *aux droits fondamentaux dont est titulaire toute personne* »[52] tel que le respect de la dignité humaine ou des droits de la défense ; la seconde tenant aux formalités et procédures légales auxquelles les autorités enquêtrices sont soumises[53]. Ces limites visent non seulement à prévenir tout abus des autorités enquêtrices mais également à garantir l'intégrité, la fiabilité et donc l'utilité de la preuve recueillie dans le respect des règles édictées par le législateur.

Malgré la réglementation, le risque d'atteinte à la vie privée provient de l'État qui cherche à obtenir des renseignements pour mieux organiser le fonctionnement de la société et mieux vaut prévenir le danger.

[52] J. PRADEL, Procédure pénale, 2011, *op. cit*., p. 303.
[53] S. BERNEMAN, «L'admissibilité de la preuve dans un système continental : le modèle belge», Revue de droit pénal et de criminologie, 4, 2007, p. 301. Cité par M. MARTY, *La légalité de la preuve dans l'espace pénal européen*, Thèse de doctorat, Université de Bordeaux, 1er avril 2014, p.8.

Aussi, les risques d'intrusion des autorités judiciaires dans la vie privée des personnes peuvent résulter de l'imprécision de la règlementation. A titre d'exemple, la législation sénégalaise sur les interceptions des données ne prévoit pas certaines conditions de sauvegarde de la vie privée expressément exigées par le rapport explicatif de la Convention de Budapest sur la cybercriminalité. Il en est ainsi, de l'impossibilité d'exercer un recours contre la décision d'interception. En vérité, ces insuffisances législatives sont de nature à favoriser des atteintes à la vie privée du citoyen qui ne dispose pas toujours de garanties suffisantes.

On note également des manquements liés à des difficultés procédurales. En droit sénégalais, le juge d'instruction ne prend pas une ordonnance de mise en détention provisoire, laquelle serait susceptible d'appel devant la chambre d'accusation. En d'autres termes, l'inculpé d'une infraction cybercriminelle ne peut pas, en l'état actuel de notre législation, attaquer immédiatement par voie d'appel la décision du juge d'instruction le plaçant en détention provisoire. Tout ce qu'il peut faire, c'est introduire ultérieurement une demande de liberté provisoire pour provoquer la prise d'une ordonnance de refus de mise en liberté provisoire susceptible d'appel[54]. Ce qui porte atteinte aux droits de la défense de l'inculpé.

Lorsqu'une infraction est détectée, les magistrats instructeurs ont pour mission de trouver son auteur et de recueillir les éléments nécessaires à la preuve de sa culpabilité pour que sanction juridictionnelle s'en suive. Les règles de procédure pénale sont alors entièrement dédiées à la recherche et au jugement des délinquants[55] et vont donner aux autorités investies de cette mission les moyens d'enquêter, instruire, puis juger le délinquant. Or, il serait intolérable que cette mission souffre d'inefficacité[56].

Quoi qu'il en soit, le traitement de données à caractère personnel qu'autorise la rétention de données de connexion doit être proportionnel aux objectifs poursuivis par les autorités judiciaires. Il résulte de l'article 35 alinéa 2 de la loi sur les données à caractère personnel que les données personnelles « *doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectés et traitées ultérieurement* »[57].

[54] C. DIAKHOUMPA, « Traité théorique et pratique de procédure pénale », 1ère Edition, p. 271.
[55] F. DEBOVE, F. FALLETTI et T. JANVILLE, Précis de droit pénal et de procédure pénale, 3ème éd., Paris, *PUF*, 2010, p. 319.
[56] La mise en état des affaires pénales, rapport de la Commission « Justice pénale et droits de l'homme », Éd. La Documentation française, 1991, p. 11, in « LA LÉGALITÉ DE LA PREUVE DANS L'ESPACE PÉNAL EUROPÉEN », *op. cit.* p. 53.
[57] La loi n° 2008 – 12 sur la Protection des données à caractère personnel.

Concernant le respect de la confidentialité des correspondances[58], le droit constitutionnel sénégalais a consacré le principe du secret des correspondances. Aux termes de l'article 13 de la constitution du 7 janvier 2001, *« le secret de la correspondance, des communications postales, télégraphiques, téléphoniques et électroniques est inviolable. Il ne peut être ordonné de restriction à cette inviolabilité qu'en application de la loi* ». Aussi, l'article 431-12 du Code pénal protège la confidentialité des données de contenu en incriminant l'interception frauduleuse de données. Malgré cette règlementation, l'utilisation des écoutes téléphoniques a tendance à porter atteinte à la confidentialité des correspondances.

Les atteintes peuvent être appréciées notamment par rapport à la liberté d'expression, car aucun point de la stratégie ne fait référence à cette liberté fondamentale qui est celle d'exprimer librement ses opinions sans restriction.

Oui, il est bien de réglementer, de sécuriser, mais une réglementation efficace doit tenir compte des droits et libertés fondamentaux et quel que soit le domaine concerné. Il s'agit par exemple de la liberté d'expression, qui renferme, comme il en résulte de la Convention du Conseil de l'Europe sur la cybercriminalité, signée par la France le 23 novembre 2001, *"le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée"*.

- **Explorer les atteintes aux droits numériques dans la stratégie nationale de cybersécurité du Sénégal.**

Il ressort de la lecture globale de la stratégie nationale de cybersécurité une non prise en compte des droits numériques car le gouvernement du Sénégal, étant lui-même prestataire de services numériques et par là détenteur de données, doit adopter des mesures strictes pour protéger ces données ainsi que ses systèmes d'information afin d'éviter les atteintes aux droits numériques.

Les atteintes aux droits numériques peuvent résulter des atteintes au fonctionnement des systèmes informatiques. L'interconnexion sans cesse croissante des réseaux numériques qui a

[58] Le respect de la correspondance n'est pas une préoccupation propre aux sociétés modernes. Dès 1742, une déclaration royale punissait de la peine de mort la violation de la correspondance privée. En 1775, un arrêt du Conseil du roi proclamait que : « Tous les principes mettent la correspondance secrète des citoyens au rang des choses sacrées dont les tribunaux comme les particuliers doivent détourner les regards », tandis que le « cabinet noir » du roi permit une information politique qui fut dénoncée dans les cahiers de doléances rédigés lors des états généraux de 1789 (Doc. AN, projet de loi no 2068, p. 2). Le XIXe siècle connaîtra l'utilisation de mesures avoisinantes (Cass. ch. réunies 31 janv. 1888, S. 1889. 1. 241, concernant le fait, pour un juge d'instruction, de se faire passer pour l'inculpé dans une conversation téléphonique avec un présumé complice de celui-ci), in « Les écoutes téléphoniques judiciaires », par P. DOURNEAU-JOSETTE, *op. cit.*, p. 2.

fourni de redoutables armes aux cybercriminels a accru la vulnérabilité des systèmes d'information. Ainsi, ces *« infrastructures critiques* » des entreprises et des Etats sont de plus en plus l'objet d'actes de sabotages, de manipulations et de destructions de leurs données. Ces actions malveillantes compromettent durablement la compétitivité des entreprises et occasionnent souvent des pertes importantes aux économies des pays[59].

Ainsi, on peut citer les atteintes à l'intégrité des systèmes informatiques, dont la propriété est pénalement protégée par l'article 431-10 du Code pénal sénégalais. Ce texte incrimine « *quiconque aura entravé ou faussé ou aura tenté d'entraver ou de fausser le fonctionnement d'un système informatique* ».

Il y a également les infections informatiques (virus informatiques, vers informatiques, bombes logiques et chevaux de troie), qui occupent une place de choix dans la liste des entraves intellectuelles au fonctionnement du système informatique. Elles peuvent être définies comme des « *programmes destinés à perturber le fonctionnement ou à détruire les éléments indispensables au fonctionnement normal du système informatique* »[60].

La pratique du « spamming » peut être considérée comme une atteinte, car elle consiste à *« l'envoi massif et parfois répété de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière* »[61].

La volatilité et le caractère manipulable des données informatiques consistent à une atteinte aux droits numériques. Les technologies offrent aux délinquants de grandes facilités de manipulations de données de nature à nuire à la bonne marche du système informatique. Il en de même de la modification qui constitue un changement des données existantes sans en modifier la nature (magnétique)[62]. Ce procédé frauduleux correspond à la technique frauduleuse appelée « *tripatouillage »* ou *« maquillage »* de données[63]. Elle se traduit nécessairement par une modification de l'information que la donnée informatique contient.

---

[59] Ph. ROSE, *La criminalité informatique*, Paris, PUF, coll. « *Que sais-je ?* », 2e édition, 1995, p. 3, cité par P. A. TOURE, in « *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal*, p. 79.
[60] N. TORTELLO et P. LOINTIER, *Internet pour les juristes*, Paris, Dalloz 1996, p. 116, cité par P. A. TOURE, *op. cit*, p. 83.
[61] Voir, M. QUEMENER et J. FERRY, *Cybercriminalité. Défi mondial*, 2e édition, Paris, Economica, 2009, p. 80.
[62] J. P. BUFFELAN, *« Les nouveaux délits informatiques »*, Expertises, n° 104, 1988, p. 103, cité par P. A. TOURE, *ibidem.*
[63] P. A. TOURE, *ibid.*

Pire encore, le droit pénal sénégalais à travers la loi sénégalaise sur la cybercriminalité prévoit une protection pénale aux données informatiques indépendamment de leur insertion dans le système à travers l'article 431-13 du Code pénal[64] , alors les atteintes sont toujours présentes ce qui devrait permettre à la stratégie de consacrer un point relatif à la protection des droits numériques.

Donc, la pertinence de la stratégie reste à voir dans la mesure où le disfonctionnement du système informatique paralyse l'usage efficient du système.

- **Faire des recommandations pour la prise en compte du respect des droits de l'homme dans l'élaboration de la stratégie nationale de cybersécurité du Sénégal**

La mise en place d'une stratégie nationale de cybersécurité peut représenter une intrusion significative dans les droits fondamentaux. Les principes suivants devraient être particulièrement respectés :

1. Toute restriction au droit à la vie privée doit être prévue par la loi et doit être proportionnelle, légitime, et nécessaire dans une société démocratique. L'Etat doit s'engager à ne pas porter atteinte à la vie privée des personnes concernées dans le cas de la géolocalisation en procédant par un désactivation du dispositif de localisation en dehors des heures de travail.

2. L'utilisation des TIC dans l'information et dans le système de justice pénale doit respecter le droit à la protection des données à caractère personnel. Les objectifs de la prévention de la criminalité et l'enquête devraient être dûment équilibrés avec l'empiètement des droits fondamentaux.

3. Etablir des principes et des règles de procédure pénale conformément à l'Etat de droit et les droits de l'homme dans l'utilisation des TIC en prévoyant une politique efficace de gestion des données personnelles.

4. Garantir que l'utilisation des TIC ne porte pas atteinte aux droits de la défense et à l'équité des procédures pénales.

[64] *« Quiconque aura endommagé ou tenté d'endommager, effacé ou tenté d'effacer, détérioré ou tenté de détériorer, altéré ou tenté d'altérer, modifié ou tenté de modifier, frauduleusement des données informatisées, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement ».*

5. Chercher une mise en œuvre efficace des nouvelles technologies de lutte contre les crimes complexes graves utilisant les ordinateurs ou le système de réseaux.

6. Traiter les affaires cybercriminelles dans un délai raisonnable permet de lutter contre les longues détentions. C'est pour cela, l'article 7 de la Charte africaine des Droits de l'Homme et des Peuples et l'article 9 du Pacte international relatif aux droits civils et politiques ont affirmé le droit de toute personne d'être jugée dans un délai raisonnable ou libérée pendant la procédure.

7. Le respect du droit à l'information des personnes concernées ; à liberté d'expression et à la liberté d'aller et venir.

8. La protection de la vie privée dans le respect du principe et de la diversité culturelle devra être de mise ainsi que la lutte contre les contenus illégaux et nuisibles à certains groupes et personnes vulnérables (la pornographie infantile et la pédophilie sur l'Internet) pour faire du cyberespace un environnement libre et sain. Selon l'UNESCO, « *cette lutte ne peut justifier aucune atteinte à la liberté d'expression et doit se faire par l'éducation de tous les acteurs du cyberespace, l'autorégulation par les producteurs et diffuseurs d'information sous forme de codes de conduite, et la mise à disposition des utilisateurs finals de moyens techniques de sélection ou de filtrage qu'ils puissent adapter à leurs valeurs éthiques propres* ».

9. Conscient du fait que les enjeux couvrent l'ensemble des droits de l'homme, certains acteurs ont initié une « Déclaration Universelle des Droits de l´Internaute du 19 juin 2009 » pour inciter à une relecture des droits de l'homme à l'aune des valeurs du cyberespace. Nous appelons le gouvernement du Sénégal à tenir compte de cette Déclaration Universelle pour mieux garantir les droits des internautes sénégalais.

10. Relire toute la problématique des acteurs de la société de l'information pour tenir compte de leur extrême diversité due notamment à l'émergence d'acteurs nouveaux à l'échelle internationale comme les entreprises du secteur privé, les organisations de la société civile.

11. L'intégration efficace des TIC ne peut se réaliser sans formation à l'appui. Former les enseignants à l'usage des TIC en classe semble important dans notre société où l'innovation technologique prend de plus en plus d'ampleur. Donc, c'est non pas la maîtrise technologique qui sera déterminante dans le changement, mais l'augmentation des compétences qui permettent de communiquer, coopérer, s'organiser, gérer, qui obligent à considérer celui qui apprend comme un acteur à part entière, dont l'engagement et l'action influent sur l'efficience du dispositif.

12. La mise en œuvre d'une stratégie globale destinée à renforcer l'effectivité de la lutte contre la cybercriminalité, compte-tenu des préjudices dont elle est à l'origine et des enjeux qu'elle représente, doit s'accompagner d'un renforcement significatif, en ressources humaines.