UNIVERSITE ASSANE SECK DE ZIGUINCHOR

L'excellence, ma référence

UFR des Sciences Économiques et Sociales

Département de Sociologie

Mémoire de Master

Intitulé du master : Politiques Publiques, Cultures et Développement

Spécialité : Politiques Publiques et Développement

La cybercriminalité dans les réseaux sociaux au Sénégal : les contours d'un fait social

Présenté par :

Cheikh Sidath Mbagnick DIOUF

Sous la direction de :

Benoît TINE, Maître de conférences

Soutenu publiquement le Samedi 27 Juillet 2024 à la salle Visio de l'UASZ

COMPOSITION DU JURY

Amadou Hamath DIA	Maître de conférences	UASZ	Président du jury
Mamadou Aguibou DIALLO	Maître-assistant	UASZ	Examinateur
Pape GUEYE	Docteur en droit et Commissaire de police	Directeur Général de l'École nationale de cybersécurité à vocation régionale	Examinateur
Benoît TINE	Maître de conférences	UASZ	Directeur de Mémoire

Année universitaire 2022-2023

DEDICACES

Je dédie ce travail à :

Ces merveilleuses personnes qui sont parties très tôt, ma défunte mère Woré FAYE et mon défunt frère Amath DIOUF ;

Mon très cher père Aliou DIOUF, mon idole ;

Mon merveilleux grand frère Mamadou DIOUF, l'un des artisans de cette réalisation ;

Mes tantes Fatou FAYE et Awa DIOUF et mon oncle Mactar FAYE

Mes frères et sœurs ;

Toute ma famille ;

Tous ceux qui, de près ou de loin, ont contribué à ma réussite.

REMERCIEMENTS

Je tiens à adresser mes remerciements les plus sincères à toutes ces personnes qui, de près ou de loin, ont contribué à cette réalisation :

A mon directeur de mémoire le Professeur Benoît TINE, socio-criminologue et enseignant-chercheur à l'Université Assane Seck de Ziguinchor (UASZ), à qui je témoigne reconnaissance et gratitude pour ses enseignements et directives tout au long de mon cursus et pour la rédaction de ce mémoire. Mes remerciements également pour le professionnalisme, la patience et l'intransigeance dont il a fait montre pour notre réussite ;

Au Dr Mamadou Aguibou DIALLO, pour ses orientations et directives ;

Aux enseignants du département de sociologie de l'Université Assane Seck de Ziguinchor (UASZ) en l'occurrence Pr Paul DIEDHIOU, Pr Jean-Alain GOUDIABY, Pr Fatoumata HANE, Pr Amadou Hamath DIA, Dr Abdoulaye KA, Dr Ibrahima Demba DIONE, Dr Abdoulaye NGOM, Dr Aboubacar Abdoulaye BARRO, pour leurs brillants enseignements ;

Aux enseignants du département de sociologie de l'Université Cheikh Anta Diop de Dakar (UCAD), pour leurs brillants enseignements ;

A mon père Aliou DIOUF et à ma défunte mère Woré FAYE, pour avoir été de merveilleux parents, pour toutes les valeurs transmises et leur amour ;

A mon grand frère Mamadou DIOUF, sans doute la personne à qui je dois mon intérêt pour la sociologie. Merci d'avoir été là dans les bons comme dans les mauvais moments ;

A mes frères et sœurs, particulièrement à Cheikh Boucar DIOUF, Cheikh Ousmane DIOUF, Cheikh Sadibou DIOUF, Mohamed DIOUF, pour leur exemplarité et pour leur soutien inconditionnel ;

A mes oncles et tantes, particulièrement Mactar FAYE, Fatou FAYE et Awa DIOUF pour leur amour et leur soutien ;

A mon ami et camarade étudiant El hadji Mamadou DIAKHABY pour la cartographie

A mon meilleur ami Mouhamadou Moustapha KEBE pour le soutien et l'assistance ;

A mes camarades étudiants de la promotion 2017 avec qui j'ai effectué mon parcours du Master.

Liste des abréviations

ADIE : Agence de l'informatique de l'Etat

ANSD : Agence nationale de la statistique et de la démographie

BHS : Banque de l'habitat du Sénégal

BSIC : Banque sahélo-saharienne pour l'investissement et le commerce

BSLC : Brigade spéciale de lutte contre la cybercriminalité

CDP : Commission de protection des données personnelles

CEDEAO : Communauté économiques des États de l'Afrique de l'ouest

CER : Communauté économique régionale

CESTI : Centre d'études des sciences et techniques de l'information

CHEDS : Centre des hautes études de défense et de sécurité

CNIL : Commission nationale de l'informatique et des libertés

DAF : Direction de l'automatisation des fichiers

DCSSI : Direction générale du chiffre et de la sécurité des systèmes d'informations

DIC : Division des investigations criminelles

DPAF : Direction de la police de l'air et des frontières

DPTEV : Direction de la police des étrangers et des titres de voyages

DOCRITIS : Direction de l'office central de la répression du trafic illicite des stupéfiants

DPJ : Direction de la police judiciaire

DSC : Division spéciale de cybersécurité

ESGIB : École supérieure de génie industriel et de biologie

GAFAM : Google, Amazon, Facebook, Apple, Microsoft

IAM : Institut africaine de management

IIC : Infrastructures d'informations critiques

LOSI : Loi d'orientation sur la société de l'information

LT : Lieutenant

ONU : Organisation des nations unies

ONUDC : Organisation des nations unies pour la drogue et le crime

OSIRIS : Observatoire sur les systèmes d'information, les réseaux et les inforoutes du Sénégal

PAQUET-EF : : Programme d'Amélioration de la qualité, de l'Équité et de la Transparence du secteur de l'Éducation et de la Formation

PNLC : Plateforme numérique de lutte contre la cybercriminalité

SENUM : Sénégal numérique

SMSI : Sommet mondial de la société de l'information

SN : Sénégal numérique

SNC : Stratégie nationale de cybersécurité

SSI : Société sénégalaise de l'information

S/LT : Sous-Lieutenant

TIC : Technologies de l'information et de la communication

UA : Union Africaine

UASZ : Université Assane Seck de Ziguinchor

UCAD : Université Cheikh Anta Diop de Dakar

UEMOA : Union Économique et Monétaire Ouest Africain

UIT : Union internationale des télécommunications

VDN : Voie de dégagement nord

VPN : Virtual private network (Réseau privé virtuel)

TABLE DES ILLUSTRATIONS

Liste des tableaux

Liste des cartes et images

Liste des graphiques

Liste des schémas

Résumé

Ce présent mémoire sur la cybercriminalité dans les réseaux sociaux au Sénégal est un diagnostic sociologique de cette forme de déviance. Une recherche sociologique de la cybercriminalité dans les réseaux sociaux ne suppose pas simplement de faire l'esquisse de ses formes. Elle se veut une analyse des dynamiques et des tendances de celle-ci et par extension à leur compréhension. La réalisation d'une telle entreprise a nécessité un important travail théorique et méthodologique, qui a permis d'inscrire cette recherche dans un continuum. En raison de la complexité de notre problématique et de nos objectifs, cette recherche sociologique a été réalisée sur la base d'une triangulation méthodologique. De surcroît, nous avons procédé une collecte de données empiriques, instituant ainsi leur analyse et leur interprétation.

C'est ainsi que se sont dégagées les tendances cybercriminelles autour d'usages et de traitements illégaux de données à caractère personnel, d'atteintes à l'images et à la vie privée, d'escroqueries, d'incitation à la violence et de la xénophobie. De plus, différents facteurs explicatifs de la cybercriminalité dans les réseaux sociaux se sont aussi dégagés, permettant ainsi de dresser un tableau un peu plus complet de cette forme de déviance au Sénégal. Malgré son importante législation et ses initiatives de cybersécurité et de lutte contre la cybercriminalité, le Sénégal est confronté à d'importants défis, qui sont essentiellement constitués des limites de ses politiques publiques.

Mots clés : cybercriminalité, réseaux sociaux, déviance, tendances, Sénégal

Abstract

This dissertation on cybercrime in social networks in Senegal is a sociological diagnosis of this form of deviance. Sociological research into cybercrime in social networks does not simply involve sketching out its forms. It's about analyzing the dynamics and trends of cybercrime and, by extension, understanding them. Such an undertaking has required a great deal of theoretical and methodological work, which has enabled us to place this research on a continuum. Given the complexity of our problematic and our objectives, this sociological research was carried out on the basis of a methodological triangulation. In addition, we collected empirical data, thus instituting their analysis and interpretation.

Cybercrime trends emerged in the form of illegal use and processing of personal data, attacks on images and privacy, fraud, incitement to violence and xenophobia. In addition, various explanatory factors for cybercrime in social networks were also identified, providing a more complete picture of this form of deviance in Senegal. Despite its extensive legislation and initiatives in cybersecurity and the fight against cybercrime, Senegal faces major challenges, which essentially consist of the limitations of its public policies.

Keywords : cybercrime, social networks, deviance, trends, Sénégal

SOMMAIRE

INTRODUCTION GENERALE

« *Comme l'indique l'étymologie grecque Kubernêtikê (gouvernail), le cyber gouverne désormais nos vies* » (CHEDS, 2022). Ainsi, avec l'avènement d'internet et des technologies de l'information et de la communication (TIC) ainsi que leur immixtion dans la vie de l'individu, le sociologue se voit offrir un nouveau champ de recherche. Internet avec ses possibles s'est incrusté dans la vie sociale de l'individu au point d'en être incontournable. De plus, les technologies de réseautage telles que les réseaux sociaux nous permettent non seulement de maintenir nos relations sociales, mais aussi d'en créer de nouvelles. Ce nouveau champ de recherche n'est autre que le cyberespace, milieu virtuel dans lequel se déroule une grande partie des activités de l'espace physique, offre aussi à l'individu la possibilité d'adapter les réseaux sociaux à ses besoins. D'ailleurs, c'est ce qui est à l'origine de la confrontation entre les besoins des individus, parce que ceux-ci ne sont pas uniformes. Par conséquent, y sont observables des comportements qui pourraient être qualifiés de déviants.

Maurice Cusson définit les comportements déviants comme « *l'ensemble des conduites et des états que les membres d'un groupe jugent non conformes à leurs attentes, à leurs normes ou à leurs valeurs et qui, de ce fait, risquent de susciter de leur part réprobation et sanction* ». (Cusson, 1992). Cette définition de Maurice Cusson montre de façon un peu plus clair que pour que l'on parle de comportements déviants, il faut nécessairement une ou des conduites n'étant pas en phase avec les règles sociales établies et que le groupe social au sein duquel se manifestent ces comportements déviants réagit de sorte à les condamner. Ce qui implique que dans les réseaux sociaux, sont qualifiés de comportements déviants, l'ensemble des actions ou des conduites non conformes aux lois et règles régissant les plateformes numériques et les États au sein desquels elles sont utilisées. De ce fait, il convient pour les États et gouvernements de penser et de s'interroger sur la réglementation du cyberespace.

Cependant, des interrogations sont à soulever sur la nature, ce dont il convient de se protéger. Ce que Benbouzid et Ventre ont bien évidemment soulevé en posant les jalons dans leur article intitulé *Hackers malveillants, cybervictimations, traces du web et reconfigurations du policing* en disant « *si la sécurité devient l'un des principaux enjeux de la gouvernance d'Internet et du contrôle des usages du web, de quoi s'agit-il de se protéger ? Des crimes contre les ordinateurs (la protection de l'intégrité des systèmes d'information) ? Des crimes commis avec des ordinateurs (l'ordinateur comme moyen) ? Ou encore des crimes stockés dans l'ordinateur*

(l'ordinateur comme contenant et diffuseur de fichiers illégaux ou d'informations à risque) ? » (Benbouzid & Ventre, 2016)

Ces interrogations définissent le champ d'application de la cybercriminalité en signifiant de façon généralisée les aspects de ce phénomène. Ces interrogations de Benbouzid et Ventre jettent les bases de l'étude de cette forme de déviance en nous indiquant ce en quoi consistent les activités cybercriminelles. D'ailleurs, ce travail de recherche s'inscrit dans cette perspective en s'intéressant aux différentes formes sous lesquelles elle se manifeste au Sénégal, à ses facteurs explicatifs et aux représentations sociales sur le phénomène. De plus, pour saisir la cybercriminalité dans les réseaux sociaux au Sénégal, il est primordial de s'intéresser à la situation du phénomène en question dans sa globalité.

Le premier cas de cybercriminalité répertorié au Sénégal fut l'attaque perpétrée par un pirate informatique rattaché à la « Hack Army », dont a été victime le site officiel du Gouvernement du Sénégal en mai 2001[1]. A cela s'ajoute les actes de sabotage informatique par « cheval de Troie » dirigés contre le site d'informations en ligne nettali.com en janvier 2008[2]. D'ailleurs, selon le magistrat de formation Pape Assane Touré, ces événements ont précipité, au Sénégal, l'élaboration d'un cadre juridique pour encadrer le développement du numérique. Il l'avance en ces termes : « *face aux enjeux suscités par l'avènement de la cybercriminalité, les pouvoirs publics sénégalais ont, dès janvier 2005, entrepris, un vaste chantier juridique de mise en place des textes législatifs et réglementaires favorables au développement des TIC au Sénégal, en vue de protéger les biens, les personnes et les institutions publiques contre le phénomène cybercriminel* » (Touré, 2010). La prégnance de la menace cybercriminelle fait que le Sénégal est classé, selon le site de cybersécurité Kaspersky, à la 71^{e} place[3] des pays les plus attaqués au monde.

De ce fait, a été adopté en 2008 un ensemble de lois qui aborde le fonctionnement du numérique au Sénégal. Parmi celles-ci, nous avons la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité, qui définit le champ d'application de cette forme de criminalité ; autrement dit, ce qui y a trait. Le cadre juridique permet de catégoriser les infractions et d'en fixer les sanctions. C'est pourquoi dans ce présent mémoire, nous avons entrepris de porter un intérêt

[1] Le site Web du Gouvernement attaqué par un « hacker », in Batik, Osiris, n° 22, mai 2001, p. 4

[2] Ch. Mb. GUISSE, Sabotage et destruction du site Nettali.com : le parquet aux trousses d'un « cheval de Troie » : http://www.osiris.sn/article3464.html

[3] https://cybermap.kaspersky.com/fr

particulier aux formes que revêt cette criminalité, à ses causes et à comment la société se la représente.

Étudier la cybercriminalité dans les réseaux sociaux revient à faire ce que Pierre Merklé appelle la sociologie des réseaux sociaux. Il indique que cette dernière implique :

> un ensemble de méthodes, de concepts, de théories et d'enquêtes mis en œuvre en sociologie comme dans les autres disciplines des sciences sociales (anthropologie, psychologie sociale, économie etc.) qui consistent à prendre pour objet non pas les attributs des individus (leur âge, leur profession etc.), mais les relations entre les individus et les régularités qu'elles présentent pour les décrire, rendre compte de leur formation et de leur transformation, analyser leurs effets sur les comportements individuels (Merklé, 2011).

De cette pensée, Pierre Merklé jette les bases méthodologiques de l'étude des réseaux sociaux en évoquant avec précision ce en quoi elle doit consister. Il met en avant une étude de relations entre les individus et les régularités qu'elles présentent. Ce qui est d'ailleurs l'objet fondamental de ce présent mémoire sur la cybercriminalité dans les réseaux sociaux. Celle-ci étant l'activité illégale à l'issu d'une interaction entre individus par le biais des technologies de réseautage. Par ailleurs, l'étude du crime en général et de la cybercriminalité en particulier dans les réseaux sociaux s'inscrit dans la même perspective que la sociologie de Merklé en faisant usage d'un ensemble de méthodes, théories et concepts permettant de saisir notre problématique de recherche dans sa généralité.

Ainsi, pour appréhender la cybercriminalité dans les réseaux sociaux, nous nous sommes employé à étudier non seulement ses formes, causes, mais aussi les stratégies et politiques de lutte contre cette criminalité. Pour se faire, nous avons scindé ce travail en deux grandes parties. La première partie regroupe les approches théoriques et méthodologiques et la deuxième partie consiste en l'analyse et l'interprétation des résultats obtenus après l'enquête empirique. Le cadre théorique et l'approche méthodologique, qui constituent la première partie de ce travail, est divisé en trois (3) chapitres : le cadre théorique, la présentation du cadre d'étude et l'approche méthodologique

Comme seconde partie, nous avons l'analyse et l'interprétation des données recueillies à la suite des enquêtes de terrain. Celle-ci est constitué de sept (7) chapitres abordant la problématique de la cybercriminalité dans les réseaux sociaux au Sénégal dans sa généralité.

Première partie : Cadre théorique et approche méthodologique de la recherche

Le cadre théorique et l'approche méthodologique constitue le préambule de toute étude sociologique. Le cadre théorique, dans son ensemble, permet au chercheur d'avoir une maitrise de sa problématique de recherche à travers une connaissance des différentes théories et des travaux déjà réalisés. L'approche méthodologique, quant à elle, confère à la recherche sa scientificité. Dans le cadre de cette recherche, nous avons divisé cette partie en trois (3) chapitres.

Le chapitre 1, dont l'intitulé est le cadre théorique de la recherche, consiste en ce travail que nous avons fait en amont pour mieux cerner la problématique de la cybercriminalité dans les réseaux sociaux. Celui-ci a débuté par une mise au point de la littérature sur le crime en général et sur la criminalité numérique en particulier. Ce qui nous a permis d'inscrire cette recherche dans un continuum de par l'élaboration de ce en quoi consiste cette problématique de recherche. Cette dernière s'est articulée sous forme de questions et d'objectifs de recherche qui constituent l'essence de ce travail. Ces derniers ont suscité l'élaboration d'hypothèses de travail qui seront nécessairement confirmées ou infirmées par nos données d'enquête.

Après l'élaboration du cadre théorique, il nous a incombé procéder à la délimitation du champ de l'étude qui constitue le chapitre 2 de cette première partie. Elle consiste à désigner la zone dans laquelle s'effectue la recherche et de ses caractéristiques.

Comme chapitre 3, nous avons le cadre méthodologique comme second chapitre. Celui-ci est constitué de l'ensemble des méthodes, techniques et outils de collecte de données. Cette problématique, dans sa généralité, nous pousse à opter pour une approche mixte pour mieux l'appréhender.

Chapitre 1 : Cadre théorique

Le cadre théorique d'une recherche sociologique est constitué d'un ensemble d'opérations intellectuelles qui nous permet en tant que chercheur d'avoir une base sur laquelle nous appesantir pour mener à bien notre étude.

1.1. Revue de la littérature

La revue de la littérature est une étape très importante dans une recherche en sciences humaines et sociales, particulièrement en sociologie, parce qu'elle permet non seulement au chercheur de savoir ce qui est déjà fait, mais aussi elle lui permet de trouver un ou des angles par lesquels aborder sa recherche.

Pour ce qui est de notre sujet, à savoir *la cybercriminalité dans les réseaux sociaux au Sénégal : les contours d'un fait social,* nous notons une importante littérature vue que nous n'allons pas uniquement nous limiter aux productions sur la criminalité numérique. Nous allons par ailleurs nous intéresser à celle se rapportant au phénomène criminel de manière générale.

Bien que nous étudions ici la cybercriminalité, les appréhensions sur le phénomène criminel ne sont en aucun cas uniformes. Bien au contraire, elles sont différentes de par les auteurs et les postures. Ces appréhensions vont des théories holistiques à celles interactionnistes. Concernant les théories dites holistiques, leur approche est l'explication d'un fait social par un autre fait social. Elles prônent à la fois un déterminisme social, structurel, culturel et environnemental.

D'ailleurs Edwin Sutherland et Donald Cressey le souligne dans leur ouvrage *Principes de criminologie* en ces termes « *l'idée centrale de l'école de sociologie est que le comportement criminel obéit aux mêmes processus que les autres comportements sociaux. Les sociologues ont tenté d'attribuer les variations du taux de criminalité aux variations de l'organisation sociale et de préciser le processus qui fait qu'un individu devient un criminel* ». (Sutherland & Cressey, 1966)

Ainsi, la criminalité, dans son ensemble, ne saurait être l'affaire d'une seule société. Elle se manifeste partout, même si les formes et proportions ne sont pas les mêmes. C'est un « phénomène normal » pour parler comme Durkheim. Pour lui, « *le crime est normal, parce qu'une société qui en serait exempte est tout à fait impossible* » (Durkheim, 1895). Cette assertion de Durkheim rend compte du caractère inhérent du crime et ce peu importe le niveau de dévoloppement ou d'organisation sociale.

De sa pensée ressort cet élément essentiel qui n'est rien d'autre que « la conscience collective », par laquelle, un acte est défini criminel ou non. Il le dit en ces termes dans son ouvrage *De la division du travail social*, « *un acte est criminel quand il offense les états forts et définis de la conscience collective* ». (Durkheim, 1893)

Ce qui veut dire, à travers les normes socioculturelles qu'elle a établi, chaque société définit ce qui est « normal » et ce qui est « pathologique » pour continuer à parler comme Durkheim. Il utilise cette terminologie parce qu'il considère la société comme un organisme vivant où chaque organe remplit une fonction. Et quand un organe ne remplit plus ou pas correctement sa fonction, on assiste à ce qu'il appelle un dysfonctionnement conduisant à une situation dite pathologique ou anormale. Par voie de conséquence, l'analyse durkheimienne suppose que le comportement criminel vient à la suite de ce que l'on pourrait appeler un dysfonctionnement de la structure sociale.

Dans le même prolongement, Clifford R. Shaw et Henry D. McKay insistent sur le fait que « *le milieu social dans lequel vit un individu imposent des façons de sentir, de penser et d'agir et permet, dans le même temps, de se familiariser et, enfin, d'acquérir des habitudes socialement considérées comme « bonnes » ou « mauvaises* » » (Shaw & Mckay, 1942). Les conduites sociales ou comme les appelle Pierre Bourdieu « habitus » sont façonnées par notre milieu social. L'intériorisation de comportements édictés par les structures sociales fait que l'individu agit de façon « normal » ou « anomique » pour emprunter les expressions de Durkheim.

On ne pourrait faire abstraction des travaux des auteurs constituants ce qu'on appelle l'Ecole franco-belge quand on parle de sociologie du crime parce qu'elle s'inscrit dans la même logique déterministe que les travaux cités précédemment. Dans leur analyse, une place de choix est accordée au pouvoir d'action du milieu sur le passage à l'acte. Parmi les auteurs de cette école, nous avons Gabriel Tarde, dont l'analyse est axée sur le rapport entre le milieu environnemental et la délinquance. Une approche qui accorde encore le primat aux conditions sociales et structurelles ou aux conditions extérieures à l'individu de manière générale. Autrement dit, l'acte criminel est en quelque sorte la conséquence de ces conditions extérieures. D'ailleurs, son collègue de la même école, Lacassagne, abonde dans le même sillage en préconisant que l'entourage porte les germes des formes de déviance. Il avance cette idée lors de sa communication du premier congrès international d'anthropologie du crime, organisé à Rome en 1885, en disant que « *les sociétés n'ont que les criminels qu'elles méritent (…). Le milieu social est le bouillon de culture de la criminalité ; le microbe, c'est un élément qui n'a*

d'importance que le jour où il trouve le bouillon qui le fait fermenter » (Lacassagne, 1913). Ce qui sorte comme remarque de cette posture de Lacassagne, est qu'il accorde le pouvoir d'action du milieu social sur l'action individuel. Autrement dit, le criminel ou le délinquant ou encore le déviant n'est pas un être antisocial. Ses actions sont la conséquence de conditions qui lui sont extérieures comme le souligne Ferri dans son ouvrage *Sociologie du crime* en ces termes : « *tous les crimes sont la résultante des conditions individuelles et sociales. L'influence de ces facteurs est plus ou moins importante selon les conditions sociales particulières* » (Ferri, 1893).

Tous ces auteurs, avec leurs postures holistiques, font de l'individu un être passif, subissant les effets du social et contraint d'agir en conséquence. Ils réduisent l'individu en un simple agent dont l'action est déterminée par les conditions au sein de son environnement social.

Mais, dans le vaste champ de la sociologie ou de l'anthropologie criminelle, une autre forme d'appréhension du phénomène criminel fut établie par des chercheurs de l'École de Chicago comme Howard Becker et Erving Goffman. Cette forme s'inscrit évidemment dans une perspective interactionniste puisque l'interactionnisme est la théorie que l'on retrouve principalement dans leurs idées. Ces auteurs, à savoir Goffman et Becker, vont utiliser les notions de transgression, stigmatisation, d'étiquetage dans leur analyse du crime. Dans le champ de la sociologie criminelle, le crime, la délinquance et la déviance ont la même signification.

Dans leur thèse, la focale réside dans le lien interactif entre le transgresseur ou le déviant ou encore le criminel et ceux qui le qualifie comme tel. Dans son ouvrage *Outsiders*, Becker dit :

> On peut considérer la déviance et les déviant, qui incarnent ce concept, comme le résultat d'un processus d'interaction entre des individus et des groupes : les uns en poursuivant la satisfaction de leurs intérêts propres, élaborent et font appliquer (par le biais de divers appareils idéologiques ; et divers agents : entrepreneurs de morales et « grands stigmatisateurs ») des normes que transgressent les autres qui poursuivent de leur côté la satisfaction de leurs propres intérêts (qui sont divergent), commettent des actes qui sont qualifiés de déviants par les premiers (Becker, 1963)

Dans leur besoin d'asseoir leur domination et de légitimer leur pouvoir, le premier groupe dont parle Becker se sert entre-autres de l'appareil juridique et social (les normes juridiques et sociales). Ce qui limite le pouvoir d'action du second groupe s'il ne veut pas être considéré comme déviant ou criminel. Dans les échanges ou interactions, chaque individu ou groupe

d'individus essaie de maximiser ses chances en cherchant son profit, qu'il soit matériel ou non. Et dans cette recherche de profit ou de satisfaction, l'individu se sert de son arsenal pour obtenir ce qu'il cherche, quitte à enfreindre les normes sociales en vigueur. Et c'est à ce moment que commence le processus de stigmatisation et étiquetage. L'individu fait le choix de passer à l'acte en calculant coûts et bénéfices. Donc l'acte vient à la suite d'un choix rationnel de l'individu jugé selon les normes sociales comme criminel ou déviant.

Néanmoins, même si l'individu fait le choix de passer à l'acte dit criminel, on ne saurait soustraire l'influence des facteurs extérieurs dans ce choix. Parce que même si l'on considère que l'individu est maitre de son action, son groupe social est l'initiateur des manières de penser et d'agir, autrement dit sa socialisation. Par voie de conséquence, c'est à travers le milieu social que l'individu intériorise les actes socialement « bons » ou « mauvais ».

Après avoir porté un intérêt particulier à la littérature sur le crime dans sa globalité, nous allons maintenant nous astreindre à celle se rapportant spécifiquement à la cybercriminalité. Et quand on se limite à la production sur cette forme de criminalité, on se rend compte que la littérature n'est pas aussi importante au Sénégal dans le domaine des sciences sociales comme elle l'est pour le phénomène criminel de manière générale. Chose compréhensible parce que quand on parle de cybercriminalité, on fait allusion à une nouvelle forme de criminalité.

La cybercriminalité dans les réseaux sociaux constitue un domaine de recherche en pleine expansion, reflétant l'importance croissante des plateformes en ligne dans nos vies. Cette revue de littérature vise à fournir un aperçu des recherches existantes sur ce sujet, en mettant en lumière les tendances et les défis dans ce domaine émergent.

Facteurs explicatifs de la cybercriminalité

Une série de recherches examine les facteurs qui contribuent à l'émergence de la cybercriminalité dans les réseaux sociaux. Parmi ces facteurs, l'anonymat, la facilité d'accès aux informations personnelles et l'hyper-connectivité sont souvent cités comme des conditions favorables à la criminalité en ligne. De plus, les caractéristiques spécifiques des plateformes de médias sociaux, telles que leur architecture technique, leurs fonctionnalités de partage et leurs politiques sur les contenus, peuvent influencer la fréquence et la nature des délits commis.

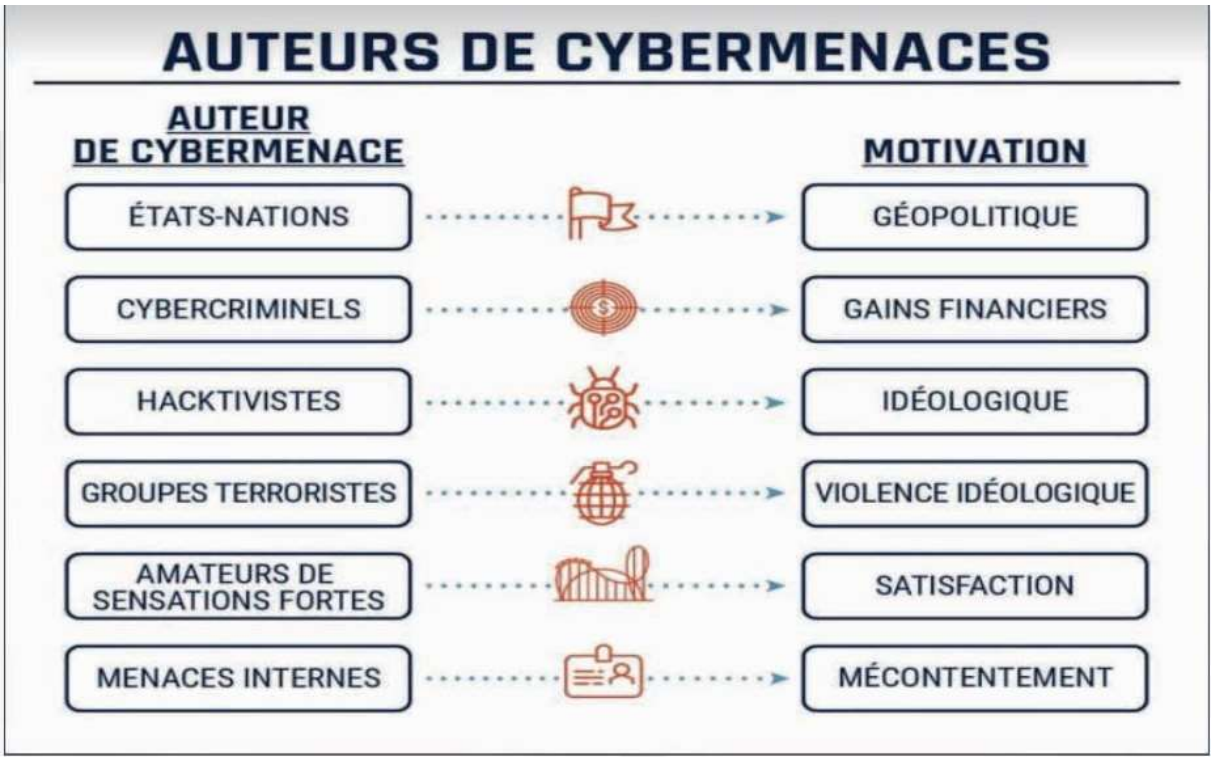
S'agissant des chercheurs ayant produit sur le sujet en question, la logorrhée s'accorde sur un point essentiel, qui est l'hyper-connectivité. Ce milieu des possibles qu'est internet, expose ses utilisateurs à ses méfaits, comme le souligne le magistrat Pape Assane Touré : « *plus on est*

connecté, plus on est cyber-vulnérable » (Touré, 2014). Ce dernier met aussi en évidence la faible législation en matière de cybercriminalité en Afrique, particulièrement au Sénégal. Il souligne que les cybercriminels se réfugient dans les pays comme le Sénégal pour continuer à exercer leurs activités. Ce qui, dans une certaine mesure, reflète inefficacité des mesures dissuasives et répressives.

D'ailleurs la conseillère en cybersécurité de l'organisation des nations unies pour la lutte contre la drogue et crime (ONUDC) Carmen Corbin souligne aussi cette hyper-connectivité comme facilitateur de la cybercriminalité. Elle le fait en ces termes : *« l'une des conséquences de la pandémie du covid-19 est l'augmentation du nombre de personnes connectées sur internet (…). Cette augmentation de personnes connectées a donné lieu à une forte recrudescence du nombre de cybercriminels* » (Corbin, 2020). Durant cette période le télétravail remplace la pratique habituelle du travail et occasionne de ce fait un nombre illimité de personnes connectées, offrant plus de possibilités aux « cybercriminels ». Le cyberespace étant ce le lieu d'interactions où chacun essaie de satisfaire en quelque sorte son désir, les cybercriminels obtiennent ainsi un choix illimité de cibles.

Dans la même perspective, le centre des hautes études de défense et de sécurité (CHEDS) dresse différents profils cybercriminels et leurs motivations.

Schéma 1 : Schématisation des profils cybercriminels en fonction des motivations



Source : Article n°2 du Magazine du centre des hautes études de défense et de sécurité (CHEDS, 2022)

Sur ce tableau, il y est mis en avant les différents profils cybercriminels et leurs motivations et ce à toutes les échelles de la cybercriminalité. Cependant, pour la catégorie cybercriminels, la motivation peut aller au-delà de la recherche de gains financiers. De plus, les cybercriminels peuvent aussi être des amateurs de sensations fortes à la recherche de satisfaction comme le fait de mesurer ses compétences ou de relever un défi.

Mohamed Chawki quant à lui dans son *Essai sur la notion de cybercriminalité* (Chawki, 2006) dresse une série de facteurs criminogènes caractéristiques de cette forme de déviance :

- Il évoque d'abord le niveau d'intelligence et d'ingéniosité des cybercriminels en précisant qu'il est clair que s'introduire sur un ordinateur à distance n'est pas dans les possibilités de n'importe qui et que le simple *deface*[4] de site nécessite un minimum de connaissances ;
- L'infaillibilité de l'ordinateur ou plutôt le fait que son utilisateur le croit infaillible ;

[4] Deface mot anglais qui désigne une modification d'un site web à la suite d'un piratage

- Le faible risque de voir la fraude découverte. Pour lui les criminels peuvent facilement supprimer la preuve de leurs méfaits en effaçant simplement les données.

Cette caractérisation de Chawki des facteurs cyber-criminogènes ne prend pas en compte l'ensemble des facteurs explicatifs de ce phénomène. En effet, elle est pour ainsi dire très limitée, parce que n'évoquant que les aspects techniques. Or, un ensemble de facteurs concourent au passage de l'acte cybercriminel.

Cependant, dans ce même essai, il nous fait remarquer une différence notoire entre le cybercriminel et le criminel classique. Cette différence intervient du fait que le milieu où se déroule les deux actes criminels ne revêtent pas les mêmes caractéristiques. Il avance en ces termes l'idée selon laquelle : « *les délinquants en informatique sont insensibles aux valeurs qui n'ont pas d'incidences matérielles. L'éclatement de la relation binaire 'auteur-victime' engendre l'absence de scrupule. Le délinquant en informatique ne bénéficie pas de l'image stéréotypée du délinquant classique, qualifié de respecter par son statut social et son niveau culturel* » (Chawki, 2006). Autrement dit, à la différence du criminel classique, le cybercriminel peut échapper aux contrôles sociaux physiques de son milieu. Par conséquent, il n'est pas soumis aux mêmes règles ou au cas où il l'est, celles-ci ne s'appliquent pas de la même façon pour lui.

Ce postulat de Chawki est pour ainsi dire semblable à celui des docteurs en criminologie Frank Schmalleger et Michael Pittaro sur la transition spatiale qu'ils ont abordé dans l'ouvrage *Crimes of the internet* (Schmalleger & Pittaro, 2008). Ils mettent en avant l'idée selon laquelle les personnes qui ont tendance à réprimer un comportement criminel dans le milieu physique en raison de leur statut et de leur position, ont une propension à en commettre dans le cyberespace. Ce qui, selon la théorie de la transition spatiale de Jaishankar (Jaishankar, 2008), est dû à la souplesse de l'identité, l'anonymat dissociatif et l'absence de facteur de dissuasion dans le cyberespace. Ce qui introduit le profilage des cybercriminels fait par Philippe Rose et Jean-Marc Lamère dans leur ouvrage *Menaces sur les autoroutes de l'information* (Rose & Lamère, 1996). Ces derniers mettent en avant trois (3) profils cybercriminels :

- L'utilisateur qui cherche le profit d'un capital financier ;
- Les destructeurs qui compensent une frustration personnelle ou professionnelle et qui ne commettent des cybercrimes que dans le but de nuire aux entreprises ou aux organisations ;

- L'entrepreneur qui vise l'activité ludique ou qui fait de ce cybercrime un défi.

Ce profilage de Rose et Lamère des cybercriminels semble incomplète parce que celle-ci ne se limite qu'à un aspect de la cybercriminalité. Il ne prend en considération que les cas de cyber-déviance qui se déroule dans le milieu des entreprises. C'est pourquoi, avec l'évolution des technologies de l'information et de la communication, le profilage fait par Daniel Martin dans ouvrage *La criminalité informatique* (Martin, 1997) semble un peu plus complet. Ce dernier fait état de quatre (4) profils différents de cybercriminels :

- L'utilisateur qui recherche le gain financier ;
- L'utilisateur qui rechercher la reconnaissance sociale ;
- L'utilisateur qui recherche la perte du sens des réalités ;
- L'utilisateur ayant un comportement idéologique.

Même si cette catégorisation des facteurs explicatifs de la cybercriminalité semble plus englobante, il est clair que les deux premiers profils cybercriminels peuvent être regroupés en un seul, puisqu'à travers le gain financier l'individu jouit d'une reconnaissance sociale, surtout dans un contexte où le pouvoir d'achat détermine la position sociale.

Quant à Philippe Ségur et Sarah Périé-Frey, ils dressent un tableau des facteurs explicatifs de la cybercriminalité qui semble un peu plus complet et contextuel au vue de l'adaptation des technologies de l'information et de la communication aux besoins humains. Dans leur article intitulé *Cybercriminalité, ordre public, économique et déstabilisation de l'Etat*, ils évoquent les motivations des cybercriminels en ces termes « *parmi les multiples causes qui engendrent la cybercriminalité, on peut citer : la vengeance suite à une déception amoureuse, le ressentiment d'être lésé pour une promotion au service, la recherche du gain facile, l'ambition politique, la recherche du pouvoir, la pratique de l'espionnage pour un développement industriel* » (Ségur & Périé-Frey, 2023). Cette esquisse de Ségur et Périé-Frey prend non seulement en compte les motivations d'une cybercriminalité dans le milieu de l'entreprise, mais aussi dans un contexte d'utilisation sociale, politique et économique des technologies de l'information et de la communication.

Dans un contexte africain, les chercheurs ayant abordé la problématique de la cybercriminalité en Afrique, s'accordent à évoquer les situations de pauvreté et précarité comme facteurs explicatifs de cette criminalité. c'est d'ailleurs le cas avec le docteur Jacques Aguia Daha,

directeur de l'office central de répression de la cybercriminalité du Bénin, qui, lors d'un reportage sur la cybercriminalité : origines et motivations des Gaïmans affirme que « *toute société qui n'arrive pas à trouver des réponses à ses jeunes est à l'épreuve de ce genre de situation où les jeunes eux-mêmes se cherchent des repères, des moyens pour la survie* »[5]. Ce postulat met en corrélation les conditions sociales et économiques telles que la pauvreté, le chômage, le manque d'emploi avec le passage à l'acte cybercriminel.

La typologie des cybercrimes

La typologie des cybercrimes a été abordée un ensemble de chercheurs, chacun définissant à sa façon les différentes formes sous lesquelles la cybercriminalité se manifeste. Ils évoquent entre autres la fraude en ligne, le vol d'identité, la diffusion de contenus illicites et la manipulation de l'opinion publique. Ce qui met en évidence la diversité des comportements criminels qui se produisent dans le cyberespace.

David Wall (Wall, 2007), dans son ouvrage *Cybercrime : the transformation of crime information Age* procède à une classification de la cybercriminalité en trois (3) catégories :

- La première catégorie de cybercrimes concerne les opérations de fraude effectuées de façon discrète. Ce premier niveau de catégorisation ne concerne que l'utilisation d'un seul système informatique pour commettre des actes cybercriminels ;
- La seconde catégorie aborde les cybercrimes dont l'exécution nécessite l'utilisation de réseau informatique, c'est-à-dire un ensemble de systèmes informatiques ;
- La troisième et dernière catégorie de cybercrimes concerne les virus informatiques qui permettent aux cybercriminels d'infecter et/ou d'infiltrer les systèmes informatiques de sorte à en prendre le contrôle.

Cette classification de Wall n'aborde pas la cybercriminalité dans sa généralité parce qu'elle ne concerne essentiellement que les cybercrimes visant les systèmes informatiques. Or, avec l'évolution des technologies de l'information et de la communication, il est possible d'ajouter une quatrième catégorie de cybercriminalité qui aborde essentiellement la diffusion de contenus illicites. D'ailleurs, c'est à cette quatrième catégorie que nous pouvons assimiler une grande majorité des cybercrimes que nous retrouvons dans les réseaux sociaux.

[5] Cybercriminalité : origines et motivations des Gaïmans
https://www.youtube.com/watch?v=kXsL4rNZi6k&t=105s visionné le 21 Janvier 2024

C’est pourquoi, la classification à travers la convention de Budapest semble plus englobante. Trois catégories de cybercriminalité sont évoquées à travers cette convention :

- Les formes traditionnelles de la criminalité qui concernent l’ensemble des crimes commis dans le milieu physique et que nous retrouvons dans le cyberespace parce que facilités par les technologies de l’information et de la communication ;
- La publication des contenus illicites par voie électroniques qui implique essentiellement l’utilisation des données à caractère personnel ;
- Les infractions propres aux réseaux électroniques qui regroupent les actes visant les systèmes informatiques à travers des attaques comme le piratage, le déni de services etc.

L’union internationale des télécommunications (UIT) a procédé à une classification des cybercrimes en cinq (5) catégories à l’intérieur desquelles nous retrouvons différentes sous catégories.

1. **Les infractions contre la confidentialité, l’intégrité et la disponibilité des données et des systèmes informatiques**

C’est une catégorie d’infractions cybercriminelles qui regroupe quatre (4) types de cybercrimes.

Tableau 1 : Les infractions contre la confidentialité, l’intégrité et la disponibilité des données et des systèmes informatiques

Types	**Définition**
Piratage	est caractérisé par un accès illégal à un ordinateur ou à un système informatique
Interception illégale de données	consiste à intercepter des données numériques lors de leur transfert par le biais d’un piratage
Atteinte à l’intégrité des données	consiste à supprimer ou à altérer des données numériques.
Atteinte à l’intégrité d’un système informatique	Elle consiste à perturber le fonctionnement d’un système informatique. C’est à l’image des attaques de déni de services (DOS)

2. Les infractions se rapportant au contenu

Ces infractions cybercriminelles sont caractérisées par la diffusion de données à caractère personnel ou des atteintes à l'image.

Tableau 2 : Les infractions se rapportant au contenu

Types	**Définition**
Les contenus érotiques ou pornographiques	Ce sont des contenus à caractère sexuel diffusés sans le consentement de la personne ou leur diffusion est interdit par la législation nationale
Pornographie infantile ou pédopornographie	Elle consiste à diffuser des contenus à caractère sexuel mettant en scène des mineurs.
Racisme, discours de haine, apologie de la violence	consiste à s'attaquer par le biais des technologies de l'information et de la communication à une race, un groupe ethnique ou groupe religieux à travers des propos xénophobes et/ou sous forme d'incitation à la violence.
Paris et jeux illégaux	Les paris et jeux illégaux en ligne désignent des activités de jeu d'argent sur Internet qui ne sont pas autorisées par la législation du pays. Cela inclut les plateformes de jeux de casino non agréées, les sites de paris sans licence, et les jeux de hasard interdits. Ces sites opèrent souvent en dehors de tout cadre réglementaire, ce qui expose les joueurs à des risques d'arnaque, de fraude et d'addiction, sans garantie de paiement des gains.
Diffamations et fausses informations	consiste à diffuser ou propager, au moyen des technologies de l'information et de la communication, des informations de nature fausse sur individu ou sur une situation quelconque.
Pollupostage et risques connexes	Désigné aussi sous le vocable de spam, qui consiste à envoyer massivement des messages ou courriels non sollicités.

3. Les infractions sur la propriété intellectuelle et les marques commerciales

Elles consistent en leur grande majorité à des contrefaçons de marques ou de technologies.

Tableau 3 : Les infractions sur la propriété intellectuelle et les marques commerciales

Types	**Définition**
Atteinte à la propriété intellectuelle	Elle consiste à reproduire une œuvre sans le consentement du propriétaire
Atteinte aux marques	Elle consiste à reproduire un ou des marques dans le but de tromper les consommateurs

4. Les infractions informatiques

Cette catégorie d'infractions cybercriminelles regroupe trois (3) cybercrimes.

Tableau 4 : Les infractions informatiques

Types	**Définition**
Fraude informatique	Elle consiste à subtiliser de l'argent à un ou des individus par biais des systèmes bancaires automatisés.
Falsification informatique	Elle désigne une manipulation de documents numériques. Elle se manifeste soit par une altération de documents, soit par la création de documents qui semblent provenir d'une institution digne de confiance.
Vol d'identité	Elle consiste à usurper l'identité numérique d'un internaute c'est-à-dire se faire passer pour quelqu'un d'autre

5. Les infractions combinées

Tableau 5 : Les infractions combinées

Types	Définition
Cyberterrorisme	Il consiste à planifier des actes terroristes à travers internet, à procéder à des recrutements d'individus en vue de perpétrer des crimes ou à faire de la propagande
Guerre numérique ou cyberguerre	Elle se manifeste sous forme de conflit entre États ou groupes d'intérêt à travers des attaques sur des infrastructures dont le fonctionnement dépend de la technologie numérique.
Cyberblanchiment	Il consiste à blanchir de l'argent par le biais de transactions électroniques multiples.
L'hameçonnage	Il consiste à collecter les données personnelles des utilisateurs en les poussant à travers des méthodes frauduleuses à révéler leurs informations personnelles.

A l'image des nations occidentales subissant la facette criminelle des technologies de l'information et de la communication, celles africaines n'échappent pas à la cybercriminalité. Cette dernière se développe dans le continent presque au rythme que le numérique y fait son expansion. Comme menaces cybercriminelles en Afrique, Interpol révèle que nous retrouvons essentiellement cinq (5) grandes catégories (Intepol, 2021) :

Premièrement, nous avons les escroqueries en ligne, qui sont des pratiques courantes sur internet et qui se manifestent sous différentes formes. Parmi celles-ci il y a :

- L'hameçonnage est très souvent réalisé par courriel, message ou appel téléphonique.

D'ailleurs, dans son rapport intitulé *African Cybersecurity Research Report* (Knowbe4, 2019), l'entreprise de cybersécurité Knowbe4 indique que lors d'une étude sur huit cent (800) individus en Afrique du sud, au Kenya, au Nigéria, au Ghana, en Égypte, à l'Ile Maurice, et au Botswana 28,14% des enquêtés ont admis avoir cliqué sur un lien d'hameçonnage. Cette dernière est une pratique très récurrente d'autant plus que les cybercriminels font montre d'une très grande ingéniosité en usurpant les identités d'entreprises dans le cadre de supposés

recrutements ou en ayant recours dans les réseaux sociaux à des annonces de subventions ou d'offres gratuites d'accès à un programme. Par ailleurs, pour mettre en évidence la prégnance de l'hameçonnage en Afrique, l'un des leaders mondiaux en cybersécurité Kaspersky a détecté au cours de l'année 2020 près de deux (2) millions de tentatives d'hameçonnage en Afrique du sud, au Kenya, en Egypte, au Nigeria et en Ethiopie (Burger, 2020).

- Le vol de carte de crédit ou fraude à la carte bancaire est une forme d'escroquerie dont les cybercriminels « *exploitent les vulnérabilités des systèmes non protégés des banques ou des particuliers, en mettant en œuvre des tactiques d'ingénierie sociale pour obtenir les informations des cartes de crédit ou accéder aux informations bancaires en ligne* » (Intepol, 2021) ;
- L'usurpation d'identité : elle consiste à se faire passer pour quelqu'un d'autre ;
- L'escroquerie à l'avance de frais : elle consiste à proposer un faux service ou produit en ligne dont l'acquisition nécessite pour l'intéressé un paiement à l'avance.
- La fraude au paiement à distance
- Les escroqueries aux cybermonnaies

Dans leur ensemble, les escroqueries constituent une partie importante des menaces cybercriminelles en Afrique. D'ailleurs, son Rapport Knowbe4 fait état de 27,71% sur huit cent (800) individus qui ont déjà été victime d'une escroquerie (Knowbe4, 2019). Quant à Richard Chelin, dans son article *Afrique : nouvel eldorado d'arnaques aux crypto-arnaques et du blanchiment d'argent* (Chelin, 2021), fait état d'escroqueries aux cybermonnaies dont une qu'il considère comme la plus grande arnaque aux cybermonnaies à l'échelle mondiale en 2020. Cette cyberattaque s'est déroulée en Afrique du Sud et a été perpétrée par Mirror Trading International. Cette escroquerie aux cybermonnaies a été fomentée sous forme de système Ponzi, faisant ainsi des centaines de milliers de victimes avec une valeur de cinq cent quatre-vingt-huit (588) millions de dollars américains en bitcoins. L'autre escroquerie perpétrée en Afrique du Sud en 2021 est chiffrée à 3,6 milliards de dollars. Elle a été perpétrée par une entreprise du nom de Africrypt.

Deuxièmement, nous avons l'extorsion en ligne qui est sans doute l'un des cybercrimes les plus prééminent en Afrique. Appelée aussi sextorsion, les auteurs de ce type de cybercrime font usage de fausses allégations ou données à caractère sexuel réelles en vue de pousser leurs victimes à payer une rançon. Pour parvenir à leurs fins, les cybercriminels utilisent pour la plupart du temps des techniques d'ingénierie sociale pour obtenir de leurs victimes les donner leur permettent de les faire chanter. D'ailleurs, Interpol a identité un des modes opératoires des

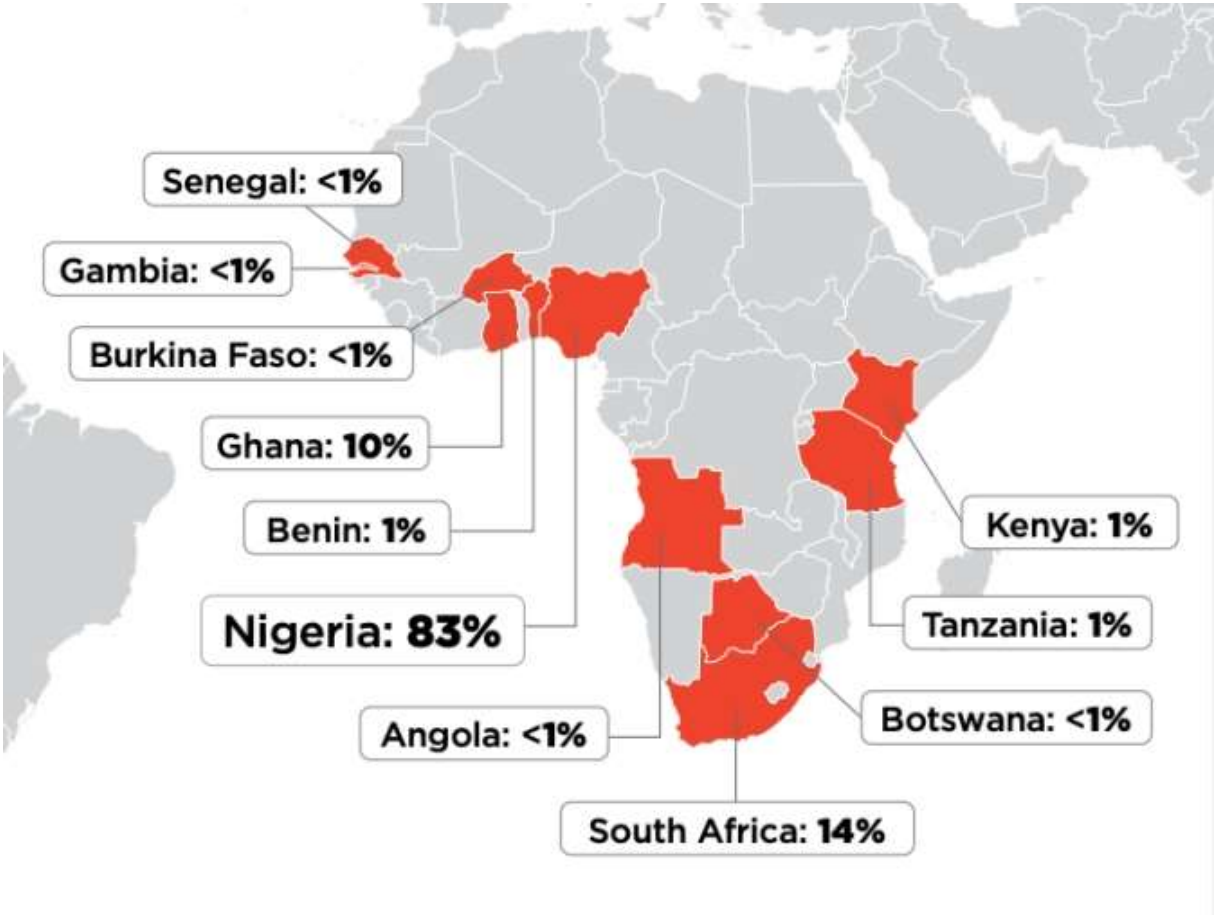
cybercriminels pour ce type de pratique. Ils « *louent des serveurs privés virtuels (VPS) avec un service SMTP (Simple Mail Transfer Protocol) pour lancer des campagnes en masse de courriels d'extorsion. Les acteurs des menaces y prétendent souvent avoir compromis la sécurité des ordinateurs, des fichiers ou des historiques de navigation de leurs victimes* » (Interpol, 2021).

Troisièmement, nous avons les escroqueries aux faux ordres de virement dont les principales victimes sont les entreprises et les organisations. Pour ce type de cybercrime, les cybercriminels opèrent de façon très ingénieuse.

> Ils en compromettent les comptes de messagerie professionnelle par des méthodes comme l'enregistrement de frappe ou des attaques par hameçonnage ou ils en contrefont simplement les courriers électroniques pour donner l'impression qu'ils ont été envoyés du compte de messagerie légitime de la victime. Des courriels frauduleux sont ensuite envoyés depuis ces comptes de messagerie au niveau de confiance établi aux autres salariés ou à des contacts de la victime en leur demandant de transférer des données ou des fonds sur un compte bancaire spécifique. (Interpol, 2021)

Selon la division cyber renseignement d'Agari, « *la majorité (60 %) des acteurs mondiaux de la menace FOVI sont basés en Afrique, dans 11 pays de la région. Ce rapport signale également que « 83 % des agresseurs africains, et 50 % des acteurs mondiaux de la menace FOVI, provenaient du Nigéria* » (ACID, 2022). Ces statistiques mettent en lumière la forme présence des cybercriminels en Afrique, qui ont fait de cette dernière leur terrain fertile.

Carte 1 : Répartition géographique des cybercriminels sur les menaces liées aux faux ordre de virement bancaire en Afrique



Source : Agari : répartition des acteurs de la menace aux faux ordres de virement en Afrique (ACID, 2022)

D'ailleurs cette cartographie des acteurs de la menace aux faux ordres de virement en Afrique illustre cette forte présence et montre que ces derniers opèrent un peu partout en Afrique.

Dans son rapport *Evaluation 2021 des cybermenaces en Afrique*, Interpol classe les escroqueries aux faux ordres de virement en trois catégories.

- La fraude à la facture fictive : « *elle implique habituellement une entreprise qui a une relation établie avec un fournisseur. Le fraudeur demande par le biais d'un courriel, d'un appel téléphonique ou d'une télécopie contrefait(e) à ce que le virement dû au titre d'une facture soit réalisé sur un nouveau compte, frauduleux* ». (Intepol, 2021)
- La fraude au président : « *Dans le cas de la fraude au président, les fraudeurs se présentent comme des dirigeants de haut niveau (DAF, DG, DSI, etc.), des avocats ou*

d'autres catégories de représentants légaux. Ils prétendent s'occuper d'affaires confidentielles ou contraintes par le temps et demandent un transfert par virement sur un compte qu'ils contrôlent. Dans certains cas, la demande frauduleuse de virement est envoyée directement à l'institution financière avec des instructions pour transférer de manière urgente les fonds à une banque. Cette escroquerie porte différents noms, « fraude au président », « escroquerie au président ». » (Intepol, 2021)

- La compromission de comptes : « *Dans les cas de compromission de comptes, le compte de messagerie électronique d'un(e) salarié(e) est piraté, puis utilisé pour envoyer des demandes de paiement de factures sur des comptes bancaires contrôlés par le fraudeur. Les messages sont envoyés à plusieurs fournisseurs identifiés dans la liste de contacts de la victime. L'entreprise cliente peut rester dans l'ignorance de cette fraude tant que les fournisseurs ne s'enquièrent pas du statut du paiement de leurs factures* » (Intepol, 2021)

Quatrièmement, il y a les bonnets qui sont des réseaux d'ordinateurs et de dispositifs piratés et infectés ; d'où l'appellation de réseaux de machines zombies,

Cinquièmement, nous avons les Rançongiciels. « *Un rançongiciel est un logiciel malveillant qui crypte les données de la victime ou verrouille ses systèmes, désorganisant les opérations des organisations victimes en rendant leurs données et leurs systèmes inaccessibles* » (Intepol, 2021) . Il est généralement la phase finale d'un piratage d'un réseau informatique. Selon Interpol, les attaques par Rançongiciel engendrent trois niveaux d'extorsions : « *l'attaque par rançongiciel initiale est démultipliée par le vol de données sensibles de l'entreprise, des demandes de rançon aux victimes en les menaçant de les humilier publiquement par la diffusion des informations volées, et la réexploitation des vulnérabilités exposées par le passé, ce qui soumet les organisations à un cycle sans fin d'attaques par rançongiciel.* » (Intepol, 2021)

Toutefois, au Sénégal, nous pouvons distinguer, selon le commissaire Moustapha Diouf, nous pouvons distinguer trois catégories de cybercriminalité (CHEDS, 2022). Il s'agit d'une :

- Cybercriminalité individuelle ou contre la personne : elle implique une personne qui distribue des informations malveillantes ou illégales en ligne. Il peut s'agir de cyber-harcèlement, de distribution de pornographie ou tout simplement de diffusion de données à caractère personnel.

Ces cybercrimes contre l'individu englobent aussi les usurpations d'identité comme il en est le cas avec l'affaire de la voyante Selbé Ndom. Cette affaire fait état d'usurpation de l'identité de

la voyante par un individu, qui est escroqué des émigrés sénégalais par le biais de consultances spirituelles sur le réseaux social Facebook.

> La section de recherches de la gendarmerie de Colobane a mis fin à l'escroquerie de Mamadou Lamine Ndiaye qui utilisait le nom de la voyante, Selbé Ndom, pour arnaquer les Sénégalais de la diaspora. (…). Après deux ans de cabale, Ndiaye a arnaqué, d'après la voyante plusieurs émigrés d'une valeur approximative de plus de 20 millions de francs CFA. La plupart de ses victimes sont des Sénégalais établis en Angleterre, Italie, Espagne, France, etc. (Diakhaté, 2013)

Il en est de même de l'affaire de la « cité Mixta »[6] qui fait état de divulgation de vidéos à caractère sexuel. Cette affaire s'est déroulée en Mai 2020, au lendemain de la fête de Korité.

- Cybercriminalité contre la propriété : Il peut s'agir d'un cas réel où un criminel possède illégalement les coordonnées bancaires ou de carte de crédit d'une personne. Le pirate vole les coordonnés bancaires d'une personne pour avoir accès à des fonds, faire des achats en ligne ou lancer des arnaques par hameçonnage (phishing) afin d'inciter les gens à divulguer leurs informations. Il pourrait également utiliser un logiciel malveillant pour accéder à une page Web contenant des informations confidentielles.

- Cybercriminalité gouvernementale : Cette catégorie est moins répandue, mais elle est la plus grave. Elle comprend le piratage de sites Web gouvernementaux, de sites militaires ou la diffusion de propagande. Ces criminels sont habituellement des terroristes ou des gouvernements ennemis d'autres pays. Ce type de cybercriminalité n'est pas encore répandue au Sénégal.

En définitive, la cybercriminalité dans les réseaux sociaux est une criminalité multiforme à laquelle les États et gouvernements sont disposés à faire face par le biais de politiques de cybersécurité et de lutte contre la cybercriminalité.

Les stratégies de lutte contre la cybercriminalité

La cybercriminalité, de par ses effets et son ampleur, est une problématique sur laquelle les États, les entreprises, les organismes internationaux et les particuliers travaillent pour mettre en place des mécanismes de lutte. La complexité de ce phénomène, due à son caractère transnational, en fait une problématique mondiale dont la lutte ne se limite pas uniquement au plan national pour les États. C'est dans cette perspective que des politiques internationales ou

[6] https://www.leral.net/VIDEO-Scandale-a-Dakar-Les-auteurs-du-LOMOTIF-qui-a-secoue-la-toile-arretes_a275555.html

continentales ou encore sous régionales sont mises en place dans un cadre de coopération bien défini.

Sur le plan international, l'Union international des télécommunications, dans son rapport *Comprendre la cybercriminalité: Guide pour les pays en développement* (UIT, Comprendre la cybercriminalité: Guide pour les pays en développement, 2009) décrit avec clarté ce en quoi doivent consister les stratégies de lutte contre la cybercriminalité. C'est en ce sens différents points ont été énumérés en ces termes :

> Le renforcement de la sécurité d'internet (et la protection des internautes) fait aujourd'hui partie intégrante du développement des nouveaux services, mais aussi des politiques gouvernementales. Les stratégies de cybersécurité, par exemple le développement des systèmes techniques de protection ou la prévention, par la formation des victimes de la cybercriminalité peuvent contribuer à la réduction des risques d'infraction dans le cyberespace » (UIT, 2009).

A cet effet, les États et gouvernements ont entrepris sous la banière de convention ou d'une seule entité des mesures de lutte contre la cybercriminalité. La convention de Budapest en est le parfait exemple. Elle permet aux États membres et signataires d'avoir un cadre législaif et instutionnel par lequel faire face à cette criminalité. cette convention définit en clair les natures des infractions se rapportant à la cybercriminalité, les mesures et les sanctions qui y siéent et le cadre procédural de coopération entre États pour la traque et la mise en accusation des cybercriminels. Ayant ratifié à la convention en Décembre 2016, le Sénégal dispose à ce jour d'un cadre lui permet d'effectuer des poursuites au niveau international. Cette convention établit en principe l'entraide entre les États membres et les éventuelles extraditions de cybercriminels.

S'agissant du niveau africain, nous avons la Convention de Malabo, adoptée par l'Union africaine en 2014, qui vise à harmoniser les législations sur la cybersécurité en Afrique. Elle établit des normes pour protéger les données personnelles, lutter contre la cybercriminalité, et renforcer la coopération entre les États membres pour une sécurité numérique accrue. La convention couvre également les droits et la protection de la vie privée dans le cyberespace, soutenant la confiance dans les transactions électroniques à travers le continent.

Au-delà des niveaux international et continental, des perspectives de lutte contre la cybercriminalité de portée sous régionale ont été mises en place. Dans une volonté de collabotion, les États membres de la CEDEAO et de l'UEMOA, au dela de leurs politiques nationales, ont mis en place un cadre de coopération sur la cybersécurité et la lutte contre la

cybercriminalité définissant essentiellement la cybercriminalité et ses formes. Ceci permet aux institutions des États membres de poursuivre les cybercriminels au-delà de leurs frontières.

Bien que la cybercriminalité soit transnational, la lutte contre elle, commence d'abord au niveau national. C'est-à-dire qu'il revient aux États et aux gouvernements de penser à des politiques nationales pour faire face à cette criminalité. C'est ainsi qu'au Sénégal, il a été mis en place un ensemble de lois et politiques sur la gouvernance du numérique. En 2008, fut adopté un ensemble de lois dont celle caractérisant et définissant la cybercriminalité. Il s'agit de la loi n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité. L'adoption de lois s'est accompagnée de la création d'institutions de lutte contre la cybercriminalité telle la commission de protection des données personnelles (CDP), qui a été instituée par la loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel[7]. Cette institution a été mise en place dans le but de garantir le respect de la vie privée dans le traitement des données personnelles.

Après ce premier pas vers les politiques de cybersécurité, s'en suit l'établissement de programmes axés sur les technologies de l'information et de la communication, qui sont inclus dans le plan Sénégal émergent (PSE). Dans ce plan, est adoptée une stratégie nationale de transformation du Sénégal en une société du numérique. Elle porte le nom de Sénégal numérique 2025 (SN2025) et s'appuie sur trois points essentiels tels que : le cadre juridique et institutionnel, le capital humain et la confiance numérique.

Cette panoplie de programmes et de stratégies mises en place par l'Etat du Sénégal s'inscrit dans une logique de protection et de sécurisation du cyberespace dans son ensemble. D'où la vision « *En 2022, au Sénégal, un cyberespace de confiance, sécurisé et résiliant pour tous* » (Stratégie nationale de cybersécurité du Sénégal , 2017)

Même si le Sénégal a mis en place une législation sur la cybercriminalité et des politiques de cybersécurité et tente de les perfectionner, il n'en demeure pas moins qu'un bon nombre de cas de cybercrimes ont été notés, touchant les institutions financières, les usagers d'internet et même parfois les infrastructures gouvernementales.

1.2.La problématique

La problématique est l'essence même d'une recherche en sciences sociales, particulièrement en sociologie. Elle permet au chercheur de situer la recherche. Dans cette étape importantissime,

[7] Chapitre 2 de la loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel

le chercheur fait une description exhaustive de son sujet, tout en soulevant ce qui constitue pour lui un problème sociologique. C'est-à-dire de préciser ce qu'il veut faire et pourquoi il veut le faire. Et dans le cas de figure où nous sommes, le crime en général, pour ne pas dire seulement la cybercriminalité, comme nous l'avons souligné tantôt avec Emile Durkheim est un « fait social normal ».

De ce fait, parler de la cybercriminalité dans les réseaux sociaux comme problématique sociologique revient à souligner le lien entre l'homme et la technologique numérique. Et c'est à travers ce lien, que l'on peut comprendre les différents usages de cette technologie et par la même occasion l'utilisation socialement et juridiquement répréhensible des technologies de l'information et de la communication en général et des réseaux sociaux en particulier.

Le XXIe siècle a vu la consécration des technologies du numérique. Cette consécration est liée au lancement d'internet par Tim Berners-Lee, qui est considéré comme son inventeur. Cette invention qu'est internet, a favorisé la création d'un espace virtuel, appelé « cyberespace » qui est « *un ensemble de réseaux commerciaux, publics, privés, d'enseignements, de services qui opèrent à l'échelle planétaire*.» (Lebert, 1999)

Les technologies de l'information et de la communication et plus particulièrement les réseaux sociaux, de par leur développement et leur fulgurante expansion, vont gagner du terrain dans la vie de l'homme, au point d'être omniprésent. D'ailleurs, ces statistiques présentées par le département de recherche du site Statista[8] en sont une parfaite illustration. Il révèle qu'en Avril 2022, on comptait plus de cinq milliards d'internautes dans le monde, soit 63,1 % de la population mondiale. Sur ce total, 4,7 milliards soit 58,4 % sont des utilisateurs de réseaux sociaux. Ces statistiques montrent à quel point le numérique en général et les réseaux sociaux en particulier sont répandus et que leur utilisation est mondiale. Ce qui justifie sans doute le fait de dire que l'ère du numérique a révoqué le concept de frontière géographique en connectant le monde, au point qu'il devienne un « village planétaire »[9]. Elle a facilité l'accès à la connaissance en favorisant les échanges entre les personnes, sans que la distance ne soit un problème. Le numérique est une mine d'or et est porteur d'infinies possibilités. Il a changé la donne, en permettant à ce qu'il soit possible de réaliser tout ce que l'on pouvait accomplir à travers le contact physique humain dans cet espace virtuel, voire même plus. Il a permis à ce

[8] https://fr.statista.com/themes/9568/utilisation-d-internet-dans-le-monde/ consulté le 3 Mars 2023
[9] Village planétaire ou global village (en anglais) est une expression de Marshall Mcluhan, tirée de son ouvrage *The Medium is the Massage* paru en 1967, pour qualifier les effets de la mondialisation, des médias et des technologies de l'information et de la communication

que cela s'effectue à une vitesse hallucinante, tout en améliorant les conditions dans lesquelles l'homme peut réaliser ses besoins.

Cet espace virtuel qu'est le « cyberespace » peut être considéré comme un système social dans la mesure où il est une configuration pleine d'interactions et d'échanges qui peuvent être de nature multiple. Et c'est en ce sens que la confrontation entre les individus est évidente puisque dans ce système social, la satisfaction des besoins personnels est très recherchée. Par conséquent, les comportements au sein de ce système social ne peuvent être uniformes. Parce que supposé qu'il puisse exister une configuration sociale dans laquelle les besoins personnels et les exigences de la vie sociale puissent s'accorder à tout point, serait utopique. Et c'est ce que Norbert Elias dit en ces termes :

> Une coexistence sans affrontements et sans heurts n'est possible que si tous les individus y trouvent suffisamment de satisfaction, et une vie individuelle satisfaisante n'est passible que si le cadre social dans lequel elle se déroule est exempt de tensions, de troubles et d'affrontements. (…) Dans les édifices sociaux dont notre expérience nous rend familiers, il y a toujours semble-t-il, pour la majorité des participants, une contradiction profonde, voire un insupportable abime entre les besoins et les penchants personnels et les exigences de l'existence sociale. (Elias, 1987)

C'est d'ailleurs les confrontations au sein du système de relation qu'est le cyberespace que nous allons étudier. Et par confrontations, nous faisons allusion aux différentes formes d'usage du numérique ne rentrant pas dans le cadre de la normalité et/ou de la légalité. Ces dernières constituent l'ensemble des comportements criminels désignés sous le vocable de cybercriminalité.

Et c'est en ce sens, que l'on dit que le développement du numérique, de par les techniques d'anonymisation et la faiblesse des contrôles sociaux, a entrainé avec lui la prolifération d'une criminalité différente de celle dite « traditionnelle[10] », à savoir la cybercriminalité ou la criminalité numérique. Du fait de l'interconnexion et de l'inexistence de frontières et de limites dans le cyberespace, la cybercriminalité est devenue un problème pas seulement national, mais international. Ce qui fait qu'elle est depuis un bon moment au cœur des débats politiques nationales et internationales. Elle l'est à tel point que les États mettent en place des politiques publiques de gestion de l'espace numérique mais aussi de lutte contre toutes menaces à son encontre. Le Sénégal en est un parfait exemple avec la vision « Sénégal numérique 2025 ». Une vision qui fait état de politiques de cybersécurité. Il va même jusqu'à signer et ratifier des

[10] Par criminalité traditionnelle, on fait allusion à toute infraction ou tout crime commis à travers le contact humain ou sans l'utilisation d'un quelconque outil numérique

conventions sous régionales, régionales et même internationales, parce que comme souligné tantôt la cybercriminalité ne connait pas de frontières et n'est pas l'affaire d'un seul Etat.

D'ailleurs l'objectif principal du traité n°185 de la convention de Budapest sur la cybercriminalité est une parfaite illustration de cette volonté de de coopération entre États dans cette lutte contre la cybercriminalité. Il s'inscrit dans une perspective d'instauration « *d'une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale* ». Cette convention, dont le champ d'application ne concernait que les États membres du conseil de l'Europe, a été élargie aux États non membres comme le Sénégal qui l'a ratifié le 16 Décembre 2016. Mais elle n'entre en vigueur sur le territoire sénégalais qu'à partir du 01 Avril 2017. Elle s'inscrit dans une logique de :

> prévention des actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable » (Convention sur la cybercriminalité, 2001).

De cet objectif de la convention ressort l'aspect général ou mondial de la cybercriminalité. Elle est l'affaire de tous les États. De ce fait même si on se limite à la cybercriminalité dans les réseaux sociaux, sa gestion peut nécessiter une collaboration entre les États puisqu'il n'y a de frontières dans le cyberespace et qu'un citoyen d'une autre nationalité peut commettre un cybercrime à l'encontre d'un citoyen sénégalais.

Ceci étant dit, parler de cybercriminalité, revient d'emblée à évoquer le lien entre l'individu et la machine ou la technologie numérique dans sa généralité. La technologie ou la machine est devenue une extension de l'homme dans la mesure où celle-ci est partie intégrante de la vie de l'être humain. Avec la création d'objets connectés et de technologies comme les GAFAM (Google, Apple, Facebook, Amazon et Microsoft), elle a rapproché les individus en faisant table rase de la distance entre les aires géographiques. Au-delà de ce rapprochement, le numérique a facilité et rendu bien des choses possibles, avec une vitesse d'exécution hallucinante. Les représentations et utilisations des réseaux sociaux, du point de vue de leur divergence, ont fait que des confrontations entre les besoins ou usages des différents utilisateurs soient une

évidence. Un bon nombre d'individus va user de ces réseaux sociaux à des fins personnelles, allant même jusqu'à nuire l'autre. Vladimir Kuskov, responsable de la recherche anti-malware chez Kaspersky, nous le fait remarqué en ces termes :

> Compte tenu de la rapidité avec laquelle le paysage des menaces se déploie et du nombre de nouveaux appareils technologiques qui entrent dans la vie quotidienne des utilisateurs, il est tout à fait possible que l'année prochaine, nous ne détections pas 400 000 fichiers malveillants par jour, mais un demi-million ! Ce qui est encore plus inquiétant, c'est qu'avec le développement des Maas (malware-as-a-service), n'importe quel amateur peut désormais corrompre des appareils sans aucune connaissance technique en programmation. Devenir un cybercriminel n'a jamais été aussi facile. Il est essentiel, autant pour les grandes organisations que pour l'utilisateur lambda, de se doter de solutions de sécurité fiables, afin d'éviter d'être victime des cybercriminels. (Kaspersky, 2022)

Dans le même prolongement, le site internet Kaspersky[11], spécialisé dans la cybersécurité, révèle des statistiques assez alarmantes sur la cybercriminalité au cours de l'année 2022.

- Au cours de cette année, 15,37 % des ordinateurs des internautes dans le monde ont subi au moins une attaque de classe Malware.
- Les solutions de Kaspersky ont bloqué 505 879 385 attaques lancées à partir de ressources en ligne à travers le monde.
- 101 612 333 URL malveillantes uniques ont déclenché les composants de l'Antivirus Internet.
- Notre Antivirus Web a bloqué 109 183 489 objets malveillants uniques.
- Les attaques de ransomwares ont été déjouées sur les ordinateurs de 271 215 utilisateurs uniques.
- Des tentatives d'infection par des logiciels malveillants conçus pour voler de l'argent via l'accès en ligne à des comptes bancaires ont été enregistrées sur les appareils de 376 742 utilisateurs.

Même si elles sont assez inquiétantes, ces statistiques n'occultent en rien à internet ses bienfaits. Et c'est pourquoi nous disons que les réseaux sociaux, autant qu'ils soient, sont d'une très grande utilité dans la vie de l'homme. De par leur éventail de possibilités, ils sont vecteurs de

[11] https://www.kaspersky.fr/about/press-releases/2022_chiffre-de-lannee-les-cybercriminels-sattaquent-aux-internautes-avec-400-000-nouveaux-fichiers-malveillants-par-jour-cest-5-de-plus-quen-2021

maitrise de connaissance, de divertissement, de business comme le E-commerce (commerce en ligne) et tant d'autres choses. Avec la prolifération des nouvelles technologies et principalement des réseaux sociaux, on parle maintenant de E-réputation, qui est cette image que se font les utilisateurs de ces réseaux sociaux. Cette E-réputation est aujourd'hui menacée par les cybercriminels ou cyber-délinquants. Par ailleurs, les réseaux sociaux présentent d'énormes failles et deviennent eux-mêmes des problèmes pour l'individu. Ils permettent la collecte de données personnelles. Cette dernière est l'un des principaux moteurs de cette cybercriminalité. Ils sont facilitateurs d'actes considérés socialement répréhensibles.

C'est malheureusement le propre de toute invention humaine. Elle peut être porteuse de progrès, mais aussi génératrice de comportements déviants. D'autant plus que ces réseaux sociaux offre aux cybercriminels cette capacité de camouflage, à savoir l'anonymat. A cela s'ajoute le côté élogieux d'internet qui occulte au numérique en général et aux réseaux sociaux en particulier leur plus redoutable face. L'une de ces faces n'est rien d'autre que la cybercriminalité.

C'est d'ailleurs, ce qui a fondé nos interrogations de départ, qui sont les suivantes : qu'est ce qui est à l'origine de la cybercriminalité dans les réseaux sociaux ? Et comment se manifeste-elle ?

1.2.1. Les questions de recherche

Les questions de recherche permettent de centrer la recherche et par la même occasion de décliner les objectifs et les hypothèses. Elles sont divisées en deux parties, à savoir une question principale et des questions spécifiques ou secondaires permettant de mieux cerner le champ de la recherche.

1.2.1.1. La question principale

Quelles sont les facteurs explicatifs de la cybercriminalité sur les réseaux sociaux au Sénégal, malgré les politiques de cybersécurité et les lois en vigueur ?

1.2.1.2. Les questions secondaires

1. Sous quelles formes se manifeste la cybercriminalité dans les réseaux sociaux et quels sont les moyens ou techniques pour y parvenir ?

2. Quelles sont les représentations sociales sur la cybercriminalité dans les réseaux sociaux au Sénégal ?

3. Quelles sont les répercussions de la cybercriminalité dans les réseaux sociaux ?

4. Quelles attitudes adoptent les victimes de cybercriminalité dans les réseaux sociaux ?

1.2.2. Les objectifs de recherche

Ils correspondent aux buts que nous nous sommes fixés pour arriver à analyser et à comprendre la cybercriminalité dans les réseaux sociaux. Les objectifs de recherche sont divisés en deux catégories. Nous avons en premier lieu l'objectif général qui constitue le fondement de la recherche et en second lieu les objectifs spécifiques ou secondaires qui vont renforcer l'objectif général et nous permettre de mieux saisir notre objet d'étude.

1.2.2.1. L'objectif général

Saisir les facteurs explicatifs de la cybercriminalité sur les réseaux sociaux

1.2.2.2. Les objectifs secondaires

1. Faire la typologie de la cybercriminalité dans les réseaux sociaux

2. Saisir les représentations sociales autour de cette cybercriminalité

3. Présenter les répercussions sociales de la cybercriminalité dans les réseaux sociaux.

4. Décrire les réactions face à la cybercriminalité dans les réseaux sociaux.

1.2.3. Les hypothèses de recherches

Elles sont des réponses provisoires aux questions de recherche. Elles seront vérifiées sur le terrain à travers les données recueillies auprès des enquêtés. Et par conséquent, ces données nous permettrons de les confirmer ou de les infirmer.

1.2.3.1. L'hypothèse Principale

La cybercriminalité sur les réseaux sociaux au Sénégal est due aux conditions socioéconomiques de l'individu et à l'anonymat qui lui est offert par internet.

1.2.3.2. Les hypothèses secondaires

1. La cybercriminalité dans les réseaux sociaux au Sénégal se manifeste sous la forme d'escroqueries et d'atteintes à la vie privée et à la réputation.

2. La cybercriminalité dans les réseaux sociaux est une activité criminelle à laquelle les individus sont vulnérables et sans défense.

3. La cybercriminalité dans les réseaux sociaux déstabilise l'ordre sociale.

4. Les victimes de cybercriminalité acceptent les exigences des cybercriminels.

1.3. Modèle d'analyse

Dans cette partie, qui est l'élaboration ou la construction du modèle théorique pour l'analyse de notre sujet d'étude, il est coutume de choisir dans la panoplie de théories existantes en

sciences sociales, particulièrement en sociologie et en anthropologie. On choisit celles que l'on pense être les plus à même de nous aider à comprendre et à expliquer notre sujet.

Pour ce qui est de la criminalité en général et de la cybercriminalité en particulier, les théories que nous avons jugées plus aptes à l'analyse du fait cybercriminel sont : le grand ensemble théorique qui est l'holisme dans lequel nous allons nous focaliser sur une approche structuro-fonctionnaliste et l'interactionnisme qui met plutôt la focale sur l'individu. Le choix porté à ces théories est lié au fait qu'elles nous semblent les plus à même d'expliquer et de comprendre la cybercriminalité. Et du fait de la complexité de la cybercriminalité et pour mieux appréhender le phénomène, il convient d'ajouter les théories naissantes avec le fait cybercriminel aux théories d'analyse de la criminologie.

1.3.1. Le structuro-fonctionnalisme de Talcott Parsons

Pour ce qui est de la compréhension et/ou de l'explication du phénomène cybercriminel, l'utilisation de l'approche structuro-fonctionnaliste se justifie par la vocation de cette approche à chercher le motif ou la cause du fait social dans ce qu'il convient d'appeler les conditions extérieures à l'individu. La combinaison du structuralisme et du fonctionnalisme nous semble plus à même de rendre compte de l'importance du déterminisme social dans l'acte individuel, que l'une des théories prise isolément. Cette approche met en évidence la situation contraignante des conditions extérieures mentionnées précédemment sur l'individu. Toujours dans le but de souligner l'importance de cette combinaison théorique, l'idée ici est de mettre en corrélation les fonctions que remplissent les structures sociales dans la vie de l'individu et l'extériorité des contraintes. Qui plus est le structuralisme se veut fonctionnaliste parce que les structures sociales sur lesquelles cette approche se base pour expliquer un fait social remplissent des fonctions dans l'organisation sociale. Et le fait qu'il ne remplissent pas correctement leur fonction crée une désorganisation sociale ou un dysfonctionnement qui peut être synonyme de déviance, de criminalité ou de délinquance. Ce qui justifie d'autant plus le choix de l'analyse combinatoire.

Et c'est dans ce cadre que nous allons utiliser les appréhensions théoriques d'un des piliers de la sociologie contemporaine à savoir Émile Durkheim. Ce dernier va, à travers des notions comme la socialisation, montrer comment un organe ou une structure qui ne remplit pas sa fonction peut créer un dysfonctionnement social. Par exemple, la famille, qui est par essence le premier milieu de socialisation se trouve dans une situation où elle ne permet pas à l'individu d'intérioriser dans les conduites sociales dites « normales », le place dans une situation d'adoption de comportements transgresseurs. Autrement dit, les dysfonctionnements structurels

ou sociaux donnent lieu à des transgressions. Pour lui, la société fonctionne sur la base de règles et normes bien définies, qui régissent les comportements au sein d'un groupe ou d'une société.

En poursuivant toujours avec Durkheim, mais cette fois-ci avec sa théorie sur le suicide. Pour étudier ce fait social, le sociologue Emile Durkheim utilise les processus d'intégration et de régulation sociale. Ces derniers permettent à Durkheim d'apporter des explications sur les causes du suicide. A travers les degrés d'intégration dans le groupe social, déficit ou excès d'intégration, il montre, de par son ouvrage *Le Suicide* (Durkheim, 1897), qu'une forte intégration à la société permet à ses membres de rester attacher aux règles et normes en vigueur. Dans le même sillage, il utilise les processus de régulation sociale, qui permettent de rendre compte sur le fait que l'intégration sociale soit un facteur de régulation. Autrement dit, une forte intégration rend l'individu plus enclin à respecter ou se conformer aux normes juridiques et sociales. Des deux processus, Durkheim décline (4) quatre types de suicide.

Tableau 6 : Analyse théorique du suicide selon Durkheim

Type de suicide	Excès	Défaut
Suicide égoïste		Intégration
Altruiste	Intégration	
Anomique		Régulation
Fataliste	Régulation	

En mettant en corrélation cette schématisation du suicide et le passage à l'acte déviant ou criminel, Durkheim montre à quel point un défaut d'intégration peut rendre l'individu plus enclin à commettre un acte criminel. Ce défaut d'intégration intervient quand l'individu n'a pas vraiment ce sentiment d'appartenance à la société. Cette absence ou faiblesse du lien social fait que l'individu n'aura guère tendance à se conformer aux normes et règles sociales. Il en fait de même en parlant du déficit et de l'excès de régulation. Dans le premier cas de figure, à savoir le déficit de régulation, les normes et règles ne sont pas ou plus aussi contraignantes. L'individu gagne en marge de manœuvre et agit sans restriction. Les relations sociales se fondent habituellement sur des normes et valeurs sociales bien édictées. Ces dernières sont intégrées dans le processus de socialisation de l'individu et conditionnent par essence son comportement. Cet ensemble de valeurs et normes sociales constitue le système de référence du comportement social et fait donc office de régulateur de celui-ci. Et dans la mesure où le système de référence devient inopérant dans le cyberespace, la succession de comportements déviants devient

évident. Quant à l'excès de régulation, il correspond à ce moment où les règles et normes sociales en vigueur sont très coercitives et ne laissent aucune marge de manœuvre à l'individu. Cette situation conduit très souvent à des attitudes rebelles de la part de l'individu qui n'arrive pas à s'épanouir dans ce type d'organisation sociale. Ce comportement rebelle adopté par l'individu se concrétise par le fait d'enfreindre les règles sociales établies.

Avec cette analyse durkheimienne, on se rend compte que l'acte criminel intervient à la suite de situations antérieures, extérieures et contraignantes à l'individu.

D'ailleurs Robert Sampson et Byron Groves abonde dans le même sens avec leur hypothèse pour tester la théorie de la désorganisation sociale de Shaw et McKay. Leur postulat est que le faible statut économique, l'hétérogénéité ethnique, la mobilité résidentielle et la rupture familiale conduisent à la désorganisation sociale de la communauté, qui augmente, à son tour, les taux de criminalité et de délinquance. La rupture familiale qu'évoque Sampson et Groves renvoie à l'absence ou à la faiblesse du lien social, qui intervient lorsqu'il y a ce que Durkheim appelle un défaut d'intégration.

Toujours dans une logique d'analyse structurelle avec les processus de socialisation, la théorie de l'apprentissage (Burgess & Akers, 1996) se révèle être très instructive dans l'analyse de la cybercriminalité. Parce qu'elle se base sur l'apprentissage par l'observation pour expliquer les comportements criminels. Et dans le milieu du numérique où nous sommes, l'accès à toute forme de pratiques et de connaissances est illimité. Ce qui fait qu'il est facile pour l'individu non seulement d'imiter les pratiques, mais aussi les méthodes de passage à l'acte. Cette approche de l'apprentissage par l'observation de Burgess et Akers s'est d'ailleurs matérialisée au Sénégal avec le phénomène « *flash cas* », qui, après avoir été expérimenté dans la série télévisée Virginie[12] de la maison de production Marodi en 2021, est devenu manifeste dans le milieu scolaire. D'ailleurs, l'aspect imitation y est prégnant puisque le contexte scolaire dans lequel s'est déroulé le phénomène « *flash cas* » s'est reproduit à l'identique dans plusieurs écoles de la capitale sénégalaise ; et ce tout juste après la diffusion de la série télévisée.

Comme Durkheim, Robert Merton soutient que la déviance est inhérente à toute société qui fonctionne. Il s'inscrit dans la même logique que Durkheim en développant la théorie des tensions (Merton, 1953), selon laquelle l'accès à des objectifs socialement acceptables joue un rôle dans la détermination de la conformité ou de la déviation d'une personne. Théorie qu'il

[12] Virginie est une série télévisée composée essentiellement d'adolescent dans un contexte scolaire. C'est une série de la maison de production sénégalaise Marodi. Cette série matérialise les rivalités entre les élèves.

explique par cinq différentes manières à travers lesquelles les gens réagissent entre avoir un objectif socialement accepté et n'avoir aucune façon socialement acceptée de le poursuivre

1. Conformité : ceux qui se conforment choisissent de ne pas dévier. Ils poursuivent leurs objectifs dans la mesure du possible par des moyens socialement acceptés.

2. Innovation : ceux qui innovent et poursuivent des objectifs qu'ils ne peuvent pas atteindre par des moyens légitimes en ayant recours à des moyens criminels ou déviants.

3. Ritualisme : Les personnes qui pratiquent des rituels réduisent leurs objectifs jusqu'à ce qu'elles puissent les atteindre par des moyens socialement acceptables. Ces membres de la société se concentrent sur la conformité plutôt que sur la réalisation d'un rêve lointain.

4. Retrait : D'autres se retirent et rejettent les objectifs et les moyens de la société. Certains mendiants et personnes de la rue se sont retirés de l'objectif de réussite financière de la société.

5. Rébellion : Une poignée de personnes se rebellent et remplacent les objectifs et les moyens d'une société par les leurs. Les terroristes ou les combattants de la liberté cherchent à renverser les objectifs d'une société par des moyens socialement inacceptables.

A travers cette théorie Merton explique comment les contraintes sociales agissent sur le comportement de l'individu ou le pousse à se conformer ou à transgresser les règles et à commettre des actes déviants. Avec ce qu'il appelle l'innovation, Robert Merton montre en quoi la non concordance entre la poursuite des objectifs personnels et les moyens légitimes ou légales pour les réaliser poussent souvent l'individu à enfreindre les normes sociales et juridiques pour atteindre son objectif personnel.

S'inscrivant dans cette même logique structuro-fonctionnaliste, Talcott Parsons, influencé par la biologie, établit, à travers son ouvrage *Le Système social* (Parsons, 1951), un lien entre le fonctionnement de la biologie et celui de la société. Il considère la société comme un système global dans lequel différents sous-systèmes interagissent de façon interdépendante. Par exemple, la communauté, qu'il considère comme un sous-système, permet l'intégration sociale grâce à la socialisation, qui se manifeste par la connaissance des valeurs et des normes qui fondent cette organisation sociale. Ces sous-systèmes dont parle Parsons, comme la famille, la communauté, l'école etc., de par leur fonction de socialisateur, se complètent et permettent d'assurer l'équilibre social. Et par conséquent, l'explication de tout dysfonctionnement est à chercher dans ses sous-systèmes. Ce qui veut dire que les facteurs explicatifs du passage à l'acte ou du comportement cybercriminel sont à chercher les fonctions que remplissent les structures

sociales. C'est ce que Travis Hirschi explique avec sa théorie du contrôle social (Hirschi, 2002) en utilisant la notion de sentiment de déconnexion de la société comme facteur explicatif de la déviance. Cette déconnexion montre à quel les liens sociaux sont faibles.

Hirschi identifie (4) quatre types de liens dans l'élaboration de sa théorie. Il parle de l'attachement comme premier lien, qui permet de mesurer nos liens avec les autres et qui dans une certaine mesure aide l'individu à se conformer aux règles pour pouvoir rester dans le groupe social. A cela, il ajoute d'abord l'engagement, qui fait référence à l'investissement au groupe ou à la société qui selon Hirschi permet d'entretenir ce lien. Ensuite, il nous parle des niveaux d'implication à des activités socialement légitimées. C'est-à-dire n'adopter que des comportements ou de ne faire que des choses qui rentrent dans le cadre de la « normalité sociale » ou qui sont en phase avec les normes sociales. Et en fin, il parle de la croyance comme du lien final qui permet à l'individu de se conformer aux conduites socialement acceptées. Pour lui, la croyance suppose le fait d'être en accord avec les valeurs communes de la société à laquelle on est membre.

Toujours dans la perspective de l'explication du fait cybercriminel à travers l'approche structuro-fonctionnaliste, la théorie de la désindividualisation, que l'on retrouve principalement en psychologie, prône un déterminisme social et structurel. Ce qui fait que dans la logique de la classification traditionnelle des théories sociologiques, elle s'apparente plus à une théorie holiste. Les facteurs qui sous-tendent l'explication de cette théorie sont : l'anonymat et l'absence de contraintes sociales. Et le cyberespace en général et les réseaux sociaux ne répondent pas aux mêmes lois ou normes sociales que l'espace physique social. Dans cette configuration virtuelle, internet offre la possibilité à l'utilisateur de garder l'anonymat ou en utilisant un faux profil. Cette difficulté voire impossibilité d'identification qui s'offre à l'utilisateur dans cet espace fait disparaitre la contrainte sociale. Ce qui fait que les structures sociales, que ce soit la famille, l'école ou la société dans son ensemble, ne peuvent plus jouer leurs rôles de régulateur des comportements sociaux. Parce qu'il y a une difficulté voire même une impossibilité de punition ou de répression de ces comportements cybercriminels.

Ce qui permet dire que la possibilité de compréhension de faits sociaux tels que la cybercriminalité dans les réseaux sociaux réside à travers les faits antérieurs ou connexes ou encore à travers ce que l'on peut appeler les dysfonctionnements des structures sociales.

Cette approche structuro-fonctionnaliste permet de saisir la cybercriminalité dans les réseaux sociaux par le biais des conditions extérieures et de facteurs contraignants à l'individu. C'est-

à-dire à travers sa condition sociale, les structures au sein desquelles sa socialisation s'est effectuée. Parce que dans cette approche, un fait social tel que la cybercriminalité ne pourrait être expliqué que si on l'analyse en fonction de l'environnement social au sein duquel il germe.

1.3.2. L'interactionnisme

L'interactionnisme est une théorie sociologique, qui dans son appréhension des phénomènes sociaux, met la focale sur les relations entre les individus. En d'autres termes les fondements de cette théorie sont les interactions au sein de la société. Le postulat de base de cette théorie est de saisir l'activité sociale, pour parler comme Weber, à travers les interactions et le sens que les individus donnent à leurs actions. Et à la différence de certaines théories comme celles holistiques pour lesquelles l'individu subit les structures sociales, l'interactionnisme se focalise sur les interactions pour expliquer un fait social. Il interroge sur le sens que l'individu donne à son action. La notion centrale dans cette théorie est le sens ou la signification, parce qu'elle est à la base de toute action individuelle. C'est d'ailleurs ce que David Le Breton souligne dans son ouvrage intitulé *L'Interactionnisme symbolique.* Il le fait en ces termes : « Pour l'interactionnisme, l'individu est un acteur interagissant avec les éléments sociaux et non un agent passif subissant de plein fouet les structures sociales à cause de son habitus ou de la force du système ou de sa culture d'appartenance. » (Breton, 2004)

C'est d'ailleurs ce qui en fait une approche inductive. Elle ne se base pas sur des faits connexes pour expliquer la réalité sociale ou le fait social. David Le Breton le met en exergue dans son ouvrage cité précédemment, en utilisant les termes : « la démarche des interactionnistes est inductive. » (Breton, 2004)

C'est pour cela que pour eux, la réalité sociale se donne à voir dans les interactions entre les acteurs. Ce qui fait les facteurs explicatifs d'un fait social ne sont pas à chercher à travers des faits sociaux antérieurs ou parallèles comme le préconisent les chercheurs avec une posture holistique. Pour ce qui de la cybercriminalité dans les réseaux sociaux, il s'agira d'analyser les relations entre les différents acteurs qui gravitent autour du cyberespace pour comprendre le phénomène social en question. Il s'agit d'analyser les liens entre les acteurs, mais aussi le sens que les individus désignés comme « cybercriminels » donnent à leur action. Parce que faire autrement enlèverait à l'action tout son caractère individuel, donc son sens.

En effet le sociologue américain Georges Herbert Mead, dans son ouvrage posthume *L'esprit, le soi et la société*, conteste l'idée de groupes soumis à des pressions sociales pour réaffirmer le caractère individuel de l'action. Il dit dans cet ouvrage : « Un membre de la communauté

n'est pas nécessairement identique aux autres individus parce qu'il est capable de s'identifier à eux. » (Mead, 1963)

Cela remet en question l'analyse holistique sur le fait que l'individu appartenant à un groupe social est soumis aux mêmes comportements que les autres membres. Ce qui n'est pas vraiment le cas dans le cyberespace où même si bien des règles et normes ont été établies, il n'en demeure pas moins que les utilisateurs d'internet en général et des réseaux sociaux en particulier n'ont pas les mêmes besoins et n'appréhendent pas ce milieu virtuel de la même manière.

Pour certains auteurs comme Goffman et Becker qui se réclament de cette théorie, l'explication des phénomènes de déviance ou de criminalité réside dans les processus de stigmatisation et d'étiquetage. Qui plus est Becker considère la déviance comme une construction sociale, qui résulte d'un processus d'interaction. Il l'explique en ces termes

> Les groupes sociaux créent la déviance en instituant les normes dont la transgression constitue la déviance, en appliquant ces normes à certains individus et en les étiquetant comme déviants. De ce point de vue la déviance n'est pas une qualité de l'acte commis par la personne, mais plutôt une conséquence de l'application, par d'autres, de normes et de sanctions à un « transgresseur ». Le déviant est celui auquel cette étiquette a été appliquée avec succès et le comportement déviant est celui auquel la collectivité attache cette étiquette » (Becker, 1985).

Si l'on suit la logique de Becker, le cybercriminel ou le cyber-déviant est un construit social. En réalité, c'est la société qui s'est adjugée de définir les normes sociales et juridiques en vigueur et par conséquent définit aussi ce qui cybercriminel ou cyber-déviant de ce qui ne l'est pas. Donc à l'intérieur de ce groupe social dit cybercriminel, ces actions qualifiées comme du cybercrime ou de la cyber-déviance ne le sont pas. Alors, ce qu'il convient de retenir de cette idée de Becker, est que pour être considéré comme un cybercriminel, il faut transgresser au préalable une norme et ensuite être étiqueté comme tel. C'est cela qu'il appelle le processus d'étiquetage. Et dans ce dernier, il convient de souligner que ce sont ceux que Becker appelle « les entrepreneurs de la morale » qui sont au centre de ce processus. Ces processus de stigmatisation et d'étiquetage mis en avant par Becker et Goffman ne sont possibles que lors des interactions. Et pour ce qui est de la cybercriminalité, cet étiquetage intervient lorsque, dans leurs interactions dans le cyberespace, les individus se confrontent et que certains, dans ces échanges sociaux, ne respectent les règles de confidentialité. Et c'est à partir de ce moment où l'individu ne respectent pas les normes et règles établies dans cette configuration, qu'intervient l'étiquetage. Ces individus, qui ne sont pas dans la conformité, reçoivent cette étiquette de cybercriminel à cause de leur infraction aux conduites régissant cet espace.

Lors du passage à l'acte cybercriminel, puisqu'il s'agit ici de cybercriminalité, l'individu en question pèse son acte pour en calculer les coûts et bénéfices. Il y a ici ce que l'on appelle un choix rationnel de la part l'individu qui est sur le point de commettre l'acte cybercriminel ou qui l'a déjà commis. C'est d'ailleurs ce que l'on retient de la théorie du choix rationnel (Cornish & Clarke, 1987), dans laquelle Cornish et Clarke soutiennent que la prise de décision est fondamentale pour commettre un crime. Cette prise de décision ne peut émaner qu'après réflexion de l'individu sur ce que peut lui coûter la commission de l'acte cybercriminel ou si elle en vaut la peine. Ici, l'individu va faire un calcul pour mesurer les coûts et avantages en fonction des protocoles de cybersécurité, des mesures de dissuasion et répression et de ce qu'il obtiendra après son passage à l'acte. Ce qui revient toujours à mettre la focale sur le sens que l'individu donne à son action. Parce que rechercher le ou les explications d'un acte cybercriminel dans des facteurs extérieurs et/ou antérieurs reviendrait à nier à l'individu sa rationalité, sa capacité à décider de passer à l'acte ou à ne pas le faire.

De plus, Edwin Sutherland, avec sa théorie de l'éducation déviante, qui est le résultat d'un apprentissage, met en avant les logiques d'acquisition de comportements déviants pour expliquer les formes de déviance. Pour Sutherland et Cressey, « *le comportement criminel est appris dans l'interaction avec d'autres personnes par un processus de communication. Une part essentielle de cet apprentissage se déroule à l'intérieur d'un groupe restreint de relations personnelles. Cet apprentissage inclut, d'une part, l'apprentissage de techniques de commission de l'infraction et d'autre part, l'adoption de certains types de motifs, de mobiles, de rationalisation et d'attitudes* » (Sutherland & Cressey, 1966). De cette approche, Sutherland prend en compte dans l'explication du fait social criminel ou des formes de crime la rationalité de l'individu et par conséquent le choix raisonné et la stratégie qui sont à l'origine du passage à l'acte.

Par conséquent, pour expliquer un fait social tel que la cybercriminalité, il faut mettre la focale sur les raisons que l'individu dit « cybercriminel » invoque pour justifier son acte. Parce qu'il y a toujours une raison pour laquelle l'individu passe à l'acte. Ce qui veut dire qu'on ne peut pas appréhender la cybercriminalité à travers les conduites sociales en faisant abstraction de l'objectif qui sous-tend l'action de l'individu. Donc pour expliquer la cybercriminalité dans les réseaux sociaux, il faut comprendre les interactions entre les individus et le sens de leurs actions. Et c'est de cette façon que l'on arrivera à comprendre les causes de ce phénomène qui se trouve être un des points focaux de notre étude. Ainsi, adopter l'approche interactionniste dans l'analyse de la cybercriminalité dans les réseaux sociaux revient à saisir le phénomène du

point de vue du cybercriminel qui, dans ses échanges ou interactions dans le cyberespace, définit ses actions en fonction de sa propre rationalité. Il s'agira d'analyser le passage à l'acte cybercriminel sur la base des justificatifs de l'individu considéré comme cyber-délinquant pour donner du sens à son action.

Même si nous avons mobilisé deux modèles d'analyse pour appréhender la cybercriminalité dans les réseaux sociaux, l'interactionnisme nous semble plus à même de rendre compte des facteurs explicatifs de cette criminalité. Ceci est motivé par le qu'il prend en compte la volonté individuelle dans le passage à l'acte.

1.4. Définition des concepts

Cette étape de la recherche consiste en une opération par laquelle le chercheur procède à la définition des concepts opératoires de son étude. La définition des concepts consiste à isoler les concepts essentiels de l'étude, de les décortiquer afin de rendre plus observable l'objet d'étude. « *La première démarche du sociologue doit donc être de définir les choses dont il traite afin que l'on sache et qu'il sache bien de quoi il est question. C'est la première et la plus indispensable condition de toute preuve et de toute vérification* » (Durkheim, 2007)

1.4.1. Le crime

Définir le crime revient à le faire selon l'approche juridique et celle sociologique. L'approche juridique définit le crime selon un ensemble de lois écrites qui s'inscrivent plutôt dans un principe de légalité. Le crime est défini selon cette approche à différentes échelles qui permettent aujourd'hui de le catégoriser. Contrairement à celle-ci, l'approche sociologique définit le crime selon ce que Durkheim appelle la conscience collective. Cette dernière prend en compte les règles juridiques, mais va plus loin en prenant en considération ces normes et règles relevant d'un commun accord de vivre ensemble. Son caractère généraliste et collectif confère à cette approche sociale sa légitimité.

Ainsi, Emile Durkheim définit le crime comme « *tout acte qui, à un degré quelconque détermine contre son auteur cette réaction caractéristique qu'on nomme la peine* » (Durkheim, 1893). Cette définition de Durkheim montre que l'acte est considéré comme criminel en fonction de la réaction sociale et que c'est la société qui signifie ce qui est criminel ou non. Par conséquent pour qu'un acte soit considéré comme criminel, il faut qu'il soit en déphasage avec les normes sociales établies et qui sont en vigueur. Il faut aussi qu'il y ait une réaction sociale par rapport à l'acte.

D'ailleurs Durkheim poursuit dans le même ouvrage, *De la Division du travail social* en précisant qu'un « *acte est criminel quand il offense les états forts et définis de la conscience collective. Nous ne le réprouvons pas parce qu'il est un crime. Il est un crime parce que nous le réprouvons* » (Durkheim, 1893). Et par conscience collective, nous faisons allusion aux normes sociales définies et applicables à toute l'organisation sociale. Et toujours dans la caractérisation l'acte criminel, Durkheim met toujours l'accent sur la réaction sociale pour définir l'action de l'individu en crime. Ce qui rend compte du caractère relatif du crime dans le temps et dans l'espace. Chaque société définit, selon ses normes et règles, l'ensemble des conduites relevant du criminel.

1.4.2. La cybercriminalité

Comme souligné en prélude, la cybercriminalité est un phénomène qui touche toutes les sociétés qui subissent le développement des technologies de l'information. Et qu'elle soit perpétrée par un individu isolé ou un groupe d'individu, la cybercriminalité est un phénomène qui touche toutes les catégories d'individus et différents aspects de la société. Ce qui, par conséquent, rend compte de sa généralité. Par ailleurs, il est possible pour l'individu de se retrouver soit à la place de la victime, soit à la place du cybercriminel. Ce qui fait que l'individu doit prendre conscience des risques liés à la cybercriminalité et de s'en protéger même si sa présence en ligne ou son utilisation des technologies de l'information et de la communication n'est pas très régulier.

Trouver une définition simple et unanime de cette terminologie n'est pas une chose facile. Le phénomène en question est très complexe et est très souvent défini en fonction de la juridiction dans laquelle on se trouve. La difficulté sur la terminologie à utiliser est un des problèmes fondamentaux pour une définition générale et consensuelle. Au Sénégal, c'est la loi n°2008-11 du 25 janvier 2008 qui constitue la base juridique en matière de cybercriminalité. Dans celle-ci, la terminologie utilisée est la criminalité informatique. Cependant, une précision de taille a été faite en soulignant que criminalité informatique et cybercriminalité avaient la même signification.

Par ailleurs, la cybercriminalité y est définie comme « *toute infraction qui implique l'utilisation des technologies de l'information et de la communication* »[13]. De cette définition ressorte deux éléments essentiels : l'infraction en tant que telle et la technologie comme moyen ou outil à cette infraction. Les infractions sont très souvent ceux que la criminologie traditionnelle[14]

[13] Loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

[14] Par criminologie traditionnelle, nous faisons allusion aux différents crimes commis à travers un contact humain physique.

abordait et qui, aujourd'hui avec la technologie numérique, sont commises dans l'espace virtuel d'internet que l'on appelle cyberespace. Cette définition de la cybercriminalité renvoie à celle retenue par le droit pénal camerounais, qui la désigne comme étant : « *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* »[15].

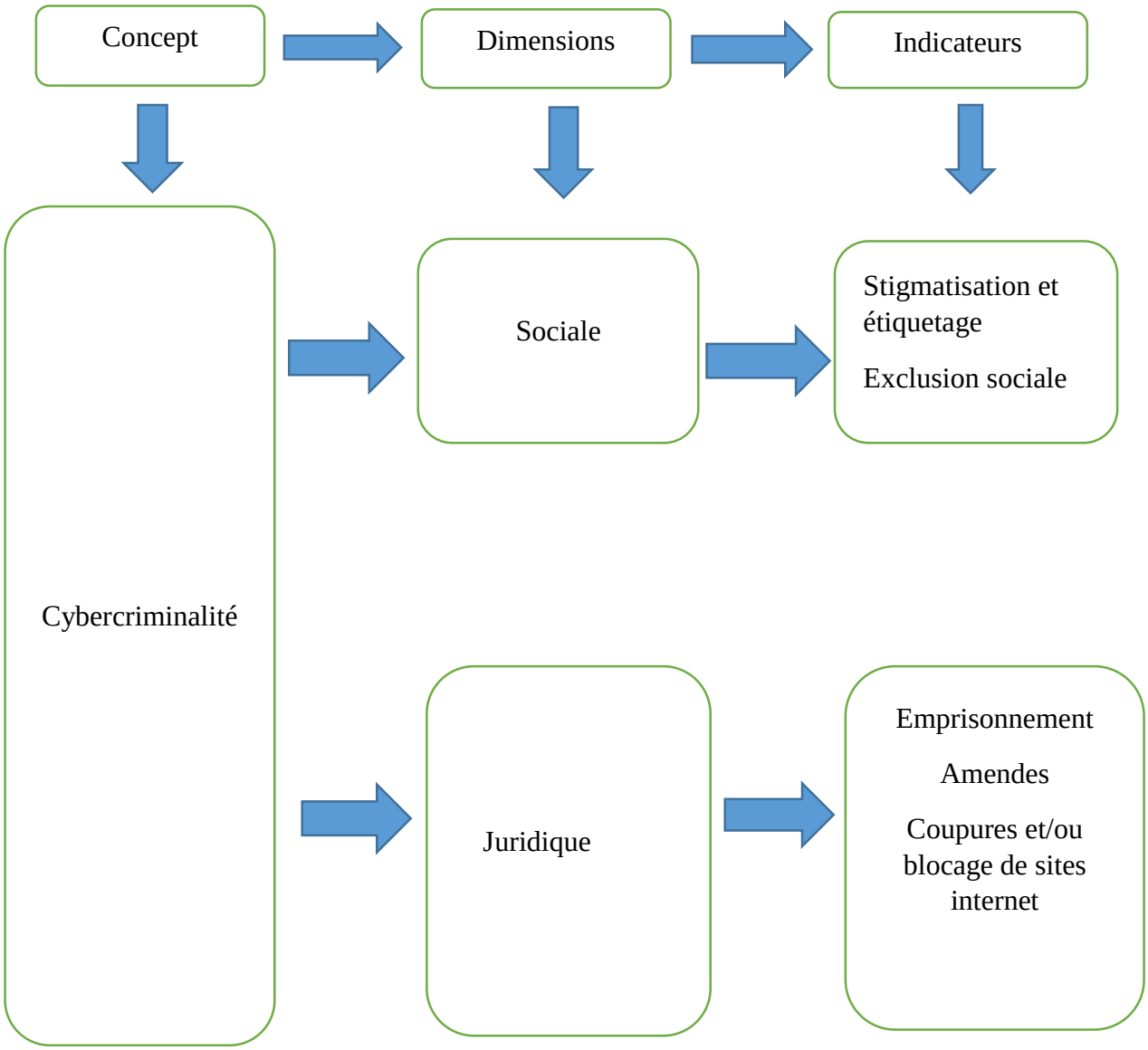
Selon le ministère de l'Intérieur français, la cybercriminalité recouvre « *l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur les réseaux partageant le protocole TCP-IP[16], appelés communément l'Internet* » (Ministère de l'intérieur français, s.d.).

En se basant sur la définition durkheimienne du crime et de celles de la cybercriminalité, précédemment citées, nous pouvons dire que la cybercriminalité regroupe l'ensemble des actes exécutés à l'aide du numérique, ne respectant pas les règles et normes établies régissant le cyberespace. Contrairement au crime qui prend en compte à la fois l'aspect social et juridique, la cybercriminalité est essentiellement une notion définie et caractérisée selon les législations des nations ou dans un cadre plus large qui est le niveau international avec les institutions de cette configuration.

[15] 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

[16] TCP/IP est un acronyme anglais qui signifie transmission control protocol /internet protocol. Il a été créé par la DARPA (Defense Advanced Research Projects Agency) aux États unis. C'est un protocole de liaison de données utilisé sur internet pour permettre aux ordinateurs et aux autres appareils d'envoyer et de recevoir des données. Ce protocole permet aux appareils connectés à internet de communiquer entre eux via les réseaux.

Schéma 2 : conceptualisation de la cybercriminalité



1.4.3. Le cyberespace

Le mot cyberespace est évoqué pour la première fois dans le roman de science-fiction de William Gibson, Neuromancer, publié en 1984. Il le décrit en ces termes « *une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts des mathématiques... Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain. Une complexité impensable, des traits de lumières disposés dans le non-espace de l'esprit, des amas et des constellations de données* ». (Gibson, 1984)

Cette définition de Gibson peut être une base pour toute tentative de définition du terme « cyberespace ». Si l'on saisit bien la description de Gibson, on retient déjà présent la virtualité

de l'espace qu'il tente de décrire. C'est-à-dire que cet espace est insaisissable, donc n'est pas physique. C'est aussi un espace connecté dans lequel les utilisateurs sont en interconnexion. Cette interconnexion se fait par le biais de l'utilisation d'outils et de technologies informatiques.

Dans le journal officiel de la République française, le cyberespace y est défini comme étant « *un espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'internet, et par les données qui y sont traitées*[17] ». Ainsi, on peut considérer le cyberespace comme un univers virtuel qui met en relation des systèmes d'information, qui, à leur tour, facilitent les échanges des données et d'informations entre les utilisateurs du fait de leur interconnexion.

Ainsi, le terme cyberespace est utilisé pour décrire l'environnement virtuel créé par les systèmes informatiques interconnectés. C'est un espace favorisant la communication entre utilisateurs, le partage d'informations, les transactions et les interactions à travers des réseaux informatiques tels que les réseaux sociaux. Le cyberespace englobe Internet ainsi que d'autres réseaux informatiques privés et publics. Il est devenu un élément essentiel de la vie moderne, influençant de nombreux aspects de la société, de l'économie, de la politique et de la culture. Cependant, il présente également des défis en matière de sécurité, de confidentialité et de gouvernance.

1.4.4. La cybersécurité

La cybersécurité concerne la protection des systèmes informatiques, des réseaux, des programmes et des données contre les cyber-menaces. Ces menaces peuvent prendre différentes formes, telles que les attaques de logiciels malveillants, les attaques par déni de service, le piratage informatique, le phishing, entre autres.

L'objectif de la cybersécurité est de prévenir, détecter et répondre aux attaques ou aux incidents de sécurité informatique afin de garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques. Cela implique la mise en place de mesures de sécurité telles que la gestion des identités et des accès, la surveillance des réseaux, la cryptographie, les pares-feux, les antivirus, les mises à jour régulières des logiciels, la sensibilisation des utilisateurs, etc.

La cybersécurité est devenue une préoccupation majeure dans le monde moderne, étant donné la dépendance croissante aux technologies de l'information et de la communication (TIC) dans

[17] Journal officiel de la République française, n° 0219 du 19 septembre 2017.

tous les aspects de la vie quotidienne. Ainsi, elle se distingue de la cybercriminalité en tant qu'ensemble de mesures visant à protéger les systèmes informatiques et les données contre les attaques. Contrairement à celle-ci, qui représente une menace pour ces systèmes et données, la cybersécurité œuvre à leur préservation. Ce domaine évolue rapidement avec l'avènement du numérique et la montée en compétences des individus dans le domaine informatique. Cependant, cette expertise n'est pas toujours utilisée de manière conforme aux normes établies, d'où l'importance de la cybersécurité pour garantir la sécurité et la confidentialité des données numériques.

Dans la stratégie nationale de cybersécurité (SNC2022), la cybersécurité est considérée comme la protection des systèmes d'information (logiciels, équipements et infrastructures), 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 usages illicites. Cela inclut des actes intentionnels ou non, issus de manquements lors de l'application des bonnes pratiques ou des procédures de sécurité

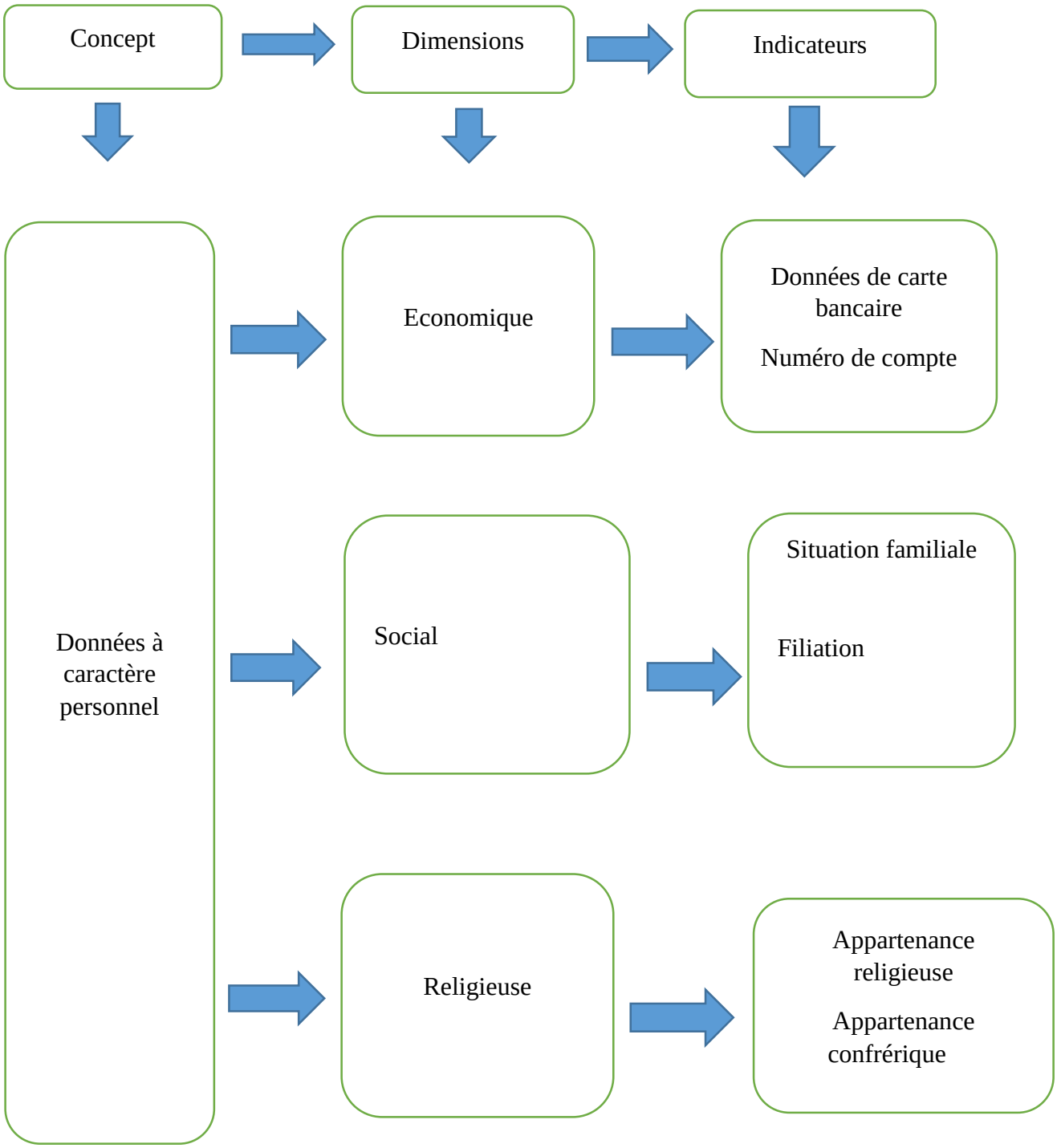
1.4.5. Les données à caractère personnel

La législation sénégalaise, à travers la loi n° 2008-12 du 25 Janvier 2008 relative à la protection des données à caractère personnel, définit une donnée à caractère personnel comme étant « *une information permettant d'identifier une personne ou qui la rend identifiable. Il s'agit du nom de la personne, de son état civil, de numéros identifiants qui lui sont propres, de sa photo, de ses empreintes, référence à un simple numéro identifiant, etc.*»[18]

De ce fait, les données à caractère personnel peuvent être considérées comme toute information qui permet d'identifier de manière directe ou indirecte une personne. Elles peuvent s'agir d'éléments tels que le nom, l'adresse, le numéro de téléphone, l'adresse e-mail, l'adresse IP, l'identifiant d'appareil, des données biométriques, des données de localisation, des données médicales, des données financières, une vidéo, une image, un enregistrement audio ou toute autre information par laquelle l'on pourrait identifier une personne. Et dans les réseaux sociaux les données à caractère personnel constituent l'océan de merveilles des cyber-délinquants. Pour les cybercrimes tels que les sextorsions, les diffusions d'images pornographiques, et certains cas d'atteintes à l'image, ce sont les données personnelles des individus comme des images, sons, vidéos qui sont utilisées pour commettre des activités cybercriminelles.

[18] Article 4-6 de la Loi n° 2008-12 du 25 Janvier 2008 relative à la protection des données à caractère personnel

Schéma 3 : opérationnalisation du concept de données à caractère personnel



1.4.6. La déviance

Dans son ouvrage *Le phénomène criminel*, Jean Pinatel mentionne que le vocable « déviance » est apparue pour la première fois dans la nomenclature de la Criminologie par l'intermédiaire des membres de la *National deviance conference*, bureau anglais spécialisé dans la Criminologie radicale. (Pinatel, 1987)

Le terme déviance s'applique à tout comportement ou attitude qui s'écarte des normes établies au sein de la société ou du groupe social ; qu'elles soient tangibles ou abstraites. La déviance peut être expliquée comme la violation d'une loi ou d'une règle formelle ou implicite, comme la transgression d'une norme sociale.

Ainsi dans son ouvrage intitulé *Outsiders,* Howard Becker définit la déviance « *comme le produit d'une transaction effectuée entre un groupe social et un individu qui, aux yeux du groupe, a transgressé une norme* » (Becker, 1985)

De cette définition de Becker, l'on peut retenir d'ores et déjà que la déviance suppose une transgression des normes sociales établies. De plus, nous pouvons retenir aussi la caractérisation de l'acte par le groupe social d'appartenance en de la déviance. Ce qui veut dire qu'un acte ne saurait être de la déviance si ce n'est que le groupe social, au sein duquel il s'est déroulé, le considère comme telle. C'est d'ailleurs, ce qui fait que la déviance est singulière selon le temps et l'espace.

Dans une acception large, la déviance renvoie aux comportements qui s'écartent de la norme sociale. C'est-à-dire aux comportements et attitudes des individus ou groupes d'individus n'étant pas en conformité avec les règles sociales en vigueur. Alors que certains comportements déviants peuvent entraîner des sanctions pénales, d'autres peuvent simplement entraîner des réactions sociales négatives ou des formes de stigmatisation sociale. De plus, ce qui est considéré comme déviant peut varier d'une culture à l'autre et évoluer au fil du temps en fonction des changements sociaux et des valeurs dominantes.

1.4.7. La norme

Ne touche pas aux biens d'autrui, ne fait pas du mal aux gens, ne médisez point les gens. Autant de règles ou normes sociales que l'on nous enseigne au cours de notre vie. Toute société ou groupe social est régi(e) par des normes et conduites sociales. Qu'elles soient écrites, comme les normes juridiques, ou non comme c'est le cas avec certaines normes sociales. Les normes regroupent l'ensemble des conduites et pratiques socialement et/ou juridiquement acceptées.

« *Les normes sociales sont les règles perçues, informelles, et pour la plupart non-écrites, qui définissent les actions acceptables et appropriées au sein d'un groupe ou d'une communauté donnée, guidant ainsi le comportement humain* » (UNICEF, 2021). Par ailleurs, la pensée du sociologue Emile Durkheim s'inscrit dans cette même perspective. Il qualifie les normes de manières de faire. Pour lui, « *ces manières de faire ne sont pas seulement des habitudes que chacun se répète, mais des règles contraignantes, fixées et définies dans la société, que nous*

adoptons parfois sans y penser. » (Durkheim E. , 1895). Autrement dit, les normes regroupent les façons d'agir issues de ce que Durkheim appelle la conscience collective.

Ainsi, évoquer les normes juridiques est très important pour une thématique telle que la cybercriminalité parce que ce phénomène est défini en fonction des législations nationales et conventions et directives internationales. Ce qui fait que l'on parle aujourd'hui de cyber-droit[19]. Les normes juridiques sont l'ensemble des textes de lois régissant dans un cadre général le bon fonctionnement de la société et dans un cadre plus particulier la marche d'un secteur. Comme c'est le cas avec le cyber-droit qui regroupe l'ensemble des textes de lois régissant le domaine du numérique.

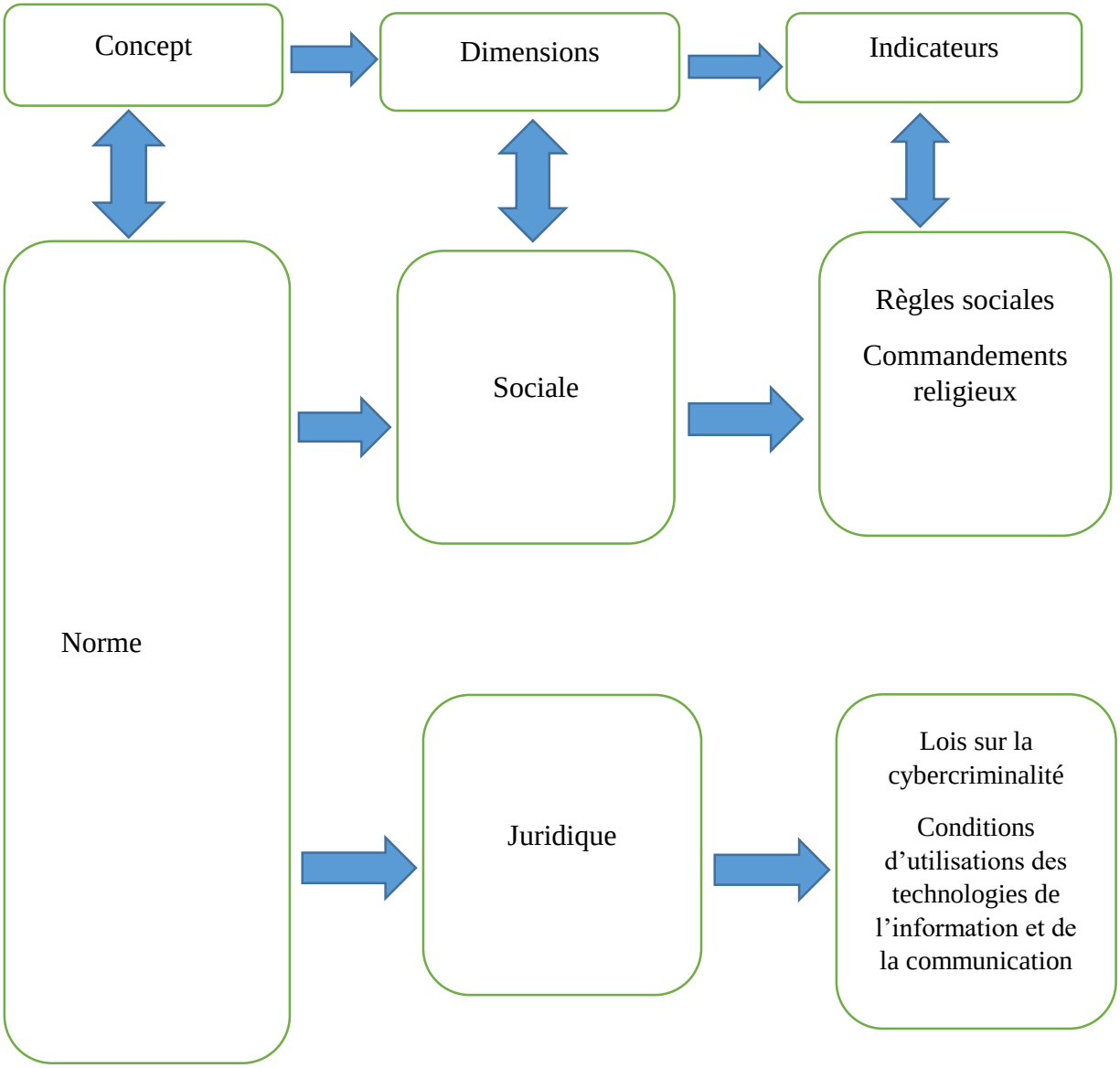
Le Sénégal comme n'importe quelque pays s'est employé à établir un ensemble de lois et même de politiques publiques sur le numérique pour maitriser ce secteur. Le numérique correspond au secteur des services qui, on peut dire, permet la bonne marche de bien des structures. C'est pourquoi, il est essentiel d'avoir des normes juridiques pour non seulement sécuriser le secteur du numérique, mais aussi de protéger les utilisateurs à travers un cyberespace sûr et fiable. Ces normes juridiques ont été matérialisées pour ce qui est de la cybercriminalité en différentes lois régissant l'univers numérique au Sénégal. Au cours de l'année 2008, le Sénégal a adopté nombre important de lois pourtant sur les infractions numériques. Cependant nous allons en citant quelques-unes se rapportant à la cybercriminalité dans les réseaux sociaux. Il s'agit des lois n°2008-08 du 25 Janvier 2008 portant sur les transactions électroniques, n°2008-10 du 25 Janvier 2008 portant sur loi d'orientation sur la société de l'information, n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité et n°2008-12 du 25 Janvier 2008 portant sur la protection des données à caractère personnel.

Au-delà des normes juridiques, nous avons les normes sociales. Néanmoins, il convient de souligner que les normes juridiques sont aussi des normes socialement acceptées, mais à la différence des normes sociales, elles sont écrites et les sanctions qui découlent d'elles ne sont pas pareilles. Celles découlant des normes juridiques sont entre autres les peines punitives (enfermement, contrôle judiciaire, sursis) et les peines pécuniaires (amendes). En outre, pour les normes sociales, les sanctions sont pour la plupart des rejets et/ou étiquetage. C'est-à-dire l'exclusion sociale et la stigmatisation.

[19] Le cyber-droit est l'ensemble des textes juridiques dont la vocation est la règlementation du cyberespace.

En définitive les normes regroupent l'ensemble des conduites socialement et/ou juridiquement acceptées. Elles sont synonymes des lois et des règlements régissant le comportement de l'individu au sein du groupe social dans lequel il évolue.

Schéma 4 : opérationnalisation du concept de norme



1.4.8. Un réseau social

Pierre Merklé définit le réseau social comme « *un ensemble d'unités sociales et de relation que ces unités sociales entretiennent les uns avec les autres* » (Merklé, 2004)

La définition de Merklé du réseau social suppose que celui-ci est composé d'un ensemble d'individus entretenant des relations. Elle suppose aussi que l'on ne peut parler de réseau social

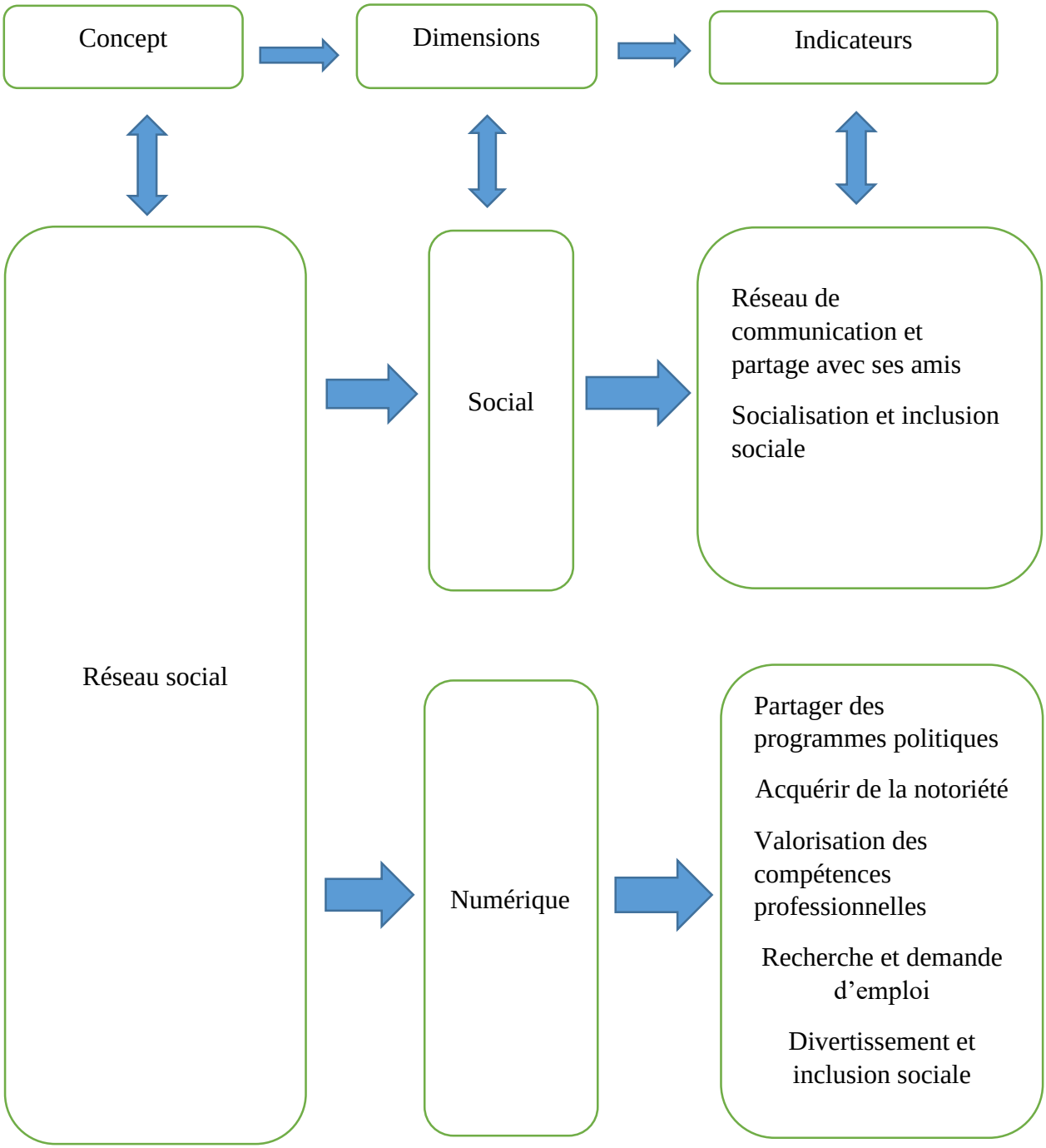
sans qu'il y ait de relation sociale, voire de l'interaction entre les individus qui composent ce réseau.

Ainsi, on peut définir le réseau social comme un système relationnel entre des individus ou des groupes d'individus. Ce système est basé sur un ensemble d'échanges et interactions qui détermine la nature de celui-ci. En d'autres termes, on parle de réseau social quand le lien entre les individus qui sont supposés le composer est tangible. Et la tangibilité de celui-ci est déterminé par les interactions.

Du point de vue technologique, un réseau social peut être défini comme une application basée sur des échanges entre les individus et permettant leur interaction. Il permet de créer ou d'entretenir un ou des liens entre les utilisateurs, même si celui-ci reste virtuel. D'ailleurs Solange Ghernaouti et Arnaud Dufour définisse le réseau dans une perspective informatique en ces termes « *le réseau est constitué d'un ensemble collaboratif de ressources informatiques de transmissions offrant des services permettant de réaliser : le partage des ressources informatiques interconnectées, la mise en relation des applications et des personnes, l'exécution de programmes à distance, le transfert d'information* » (Dufour & Ghernaouti-Hélie, 2019). Aujourd'hui, avec les technologies telles que les GAFAM (Google, Amazon, Facebook, Apple, Microsoft) qui sont les géants en ce sens, ont facilité la connexion et le contact entre utilisateurs.

La nature du réseau social dépend intrinsèquement de la nature des interactions entre les individus qui le composent, c'est-à-dire des liens et échanges qu'ils entretiennent. De ce fait, on retrouve des réseaux sociaux dont les fondements sont à chercher dans les affects ou dans les professions. D'ailleurs, les plateformes numériques faisant office de réseaux d'échanges entre individus s'inscrivent dans cette perspective. Les réseaux sociaux intègrent deux dimensions dans leur logique de réseautage. Celles-ci ne sont autres que les liens affectifs et les besoins professionnels. Cependant, il est primordial de préciser que la finalité de ces plateformes de réseautage est pour le moins redéfinie par les usages et besoins des individus.

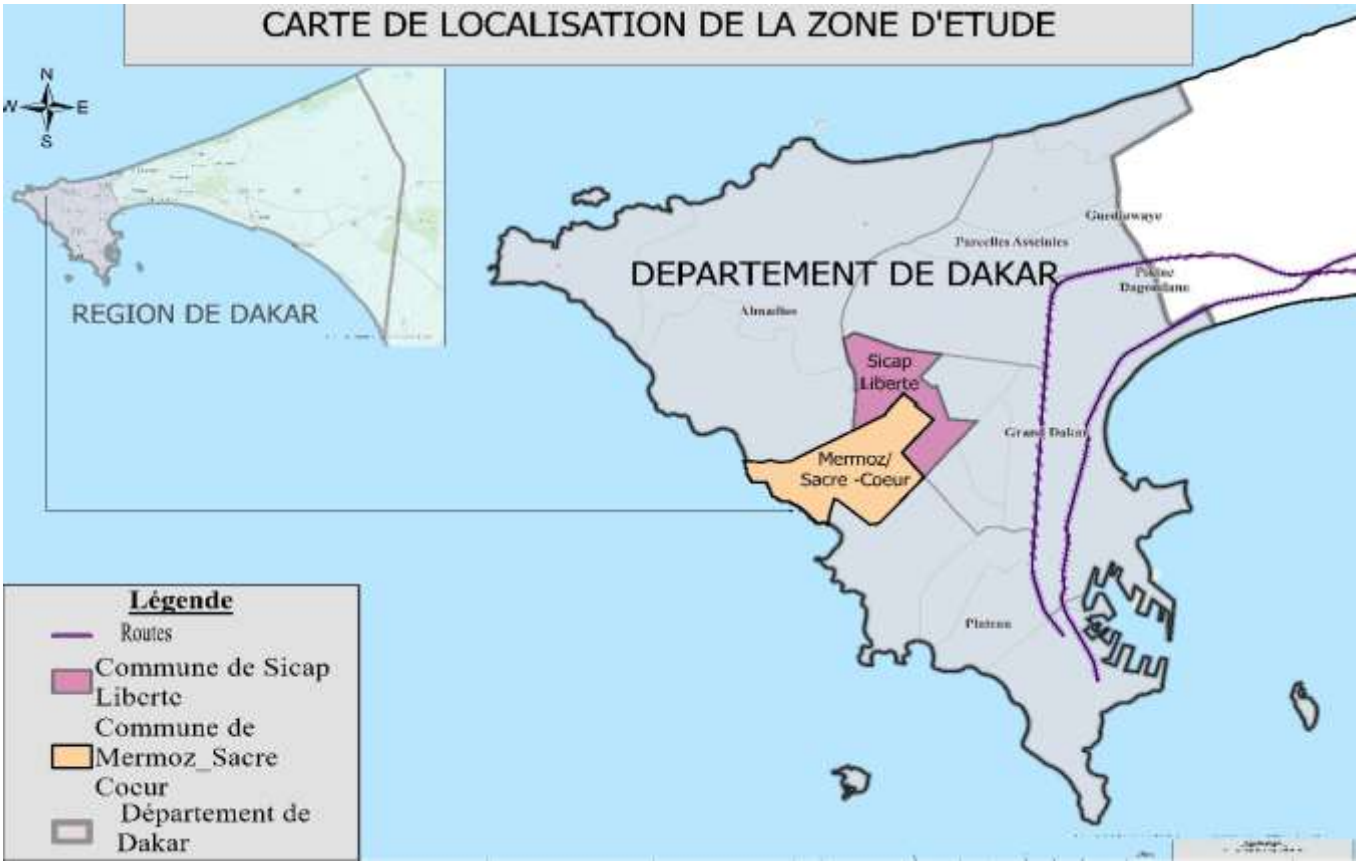
Schéma 5 : conceptualisation du concept de réseau social



Chapitre 2 : Présentation du champ de l'étude

La présentation de la zone d'étude est une étape de la recherche qui consiste à délimiter son espace géographique d'étude. Dans cette étape, il est du ressort du chercheur présenter géographiquement sa zone de recherche, mais aussi les aspects qui caractérisent cet espace et ayant un lien avec son objet d'étude. La complexité de notre problématique de recherche fait que l'étude se déroule à la fois dans le milieu physique et le cyberespace. Dans le milieu physique, nous nous y employons à administrer nos questionnaires à un échantillon d'individu méthodologiquement sélectionné et à y mener des séries d'entretien avec les personnes ressources. Par contre, dans le cyberespace, précisément dans les réseaux sociaux, nous nous employons à observer les dynamiques de ce milieu. Ainsi, vu les difficultés qui présenteraient à nous si l'on menait cette étude sur toute l'étendue du territoire sénégalais, nous avons restreint notre zone de recherche à deux communes du département de Dakar à savoir Mermoz-Sacré cœur et Sicap-Liberté. Le choix de la zone de recherche est délibéré et est surtout fait en fonction de notre connaissance de l'espace et l'accès facile au terrain. L'essentiel même des services de cybersécurité et lutte contre la cybercriminalité se trouve dans le département de Dakar. Ce qui, d'autant plus, nous a motivé à mener l'enquête de terrain dans cette zone. Les communes de Sicap-Liberté et de Mermoz Sacré-Cœur se situe géographiquement au centre-ouest du département de Dakar.

Carte 2 : Carte de localisation de la zone d'étude : communes de Sicap Liberté et de Mermoz Sacré-Cœur



Source : cartographie réalisée par El hadji Mamadou Diakhaby, étudiant en géographie

2.1. La démographie

Selon le dictionnaire multilingue des Nations unies, la démographie est « *une science ayant pour objet l'étude des populations humaines, et traitant de leur dimension, de leur évolution et de leurs caractéristiques généraux, envisagés principalement d'un point de vue quantitatif* ». Cette définition rend compte de trois aspects essentiels quand on définit une population. Ceux-ci ne sont autres que la dimension de la population elle-même, son évolution dans le temps et sa répartition sur la base des critères tels l'âge, le sexe etc. Le département de Dakar dans lequel se trouve notre zone de recherche a une population de 1 182 416 habitants[20].

Le département de Dakar, à l'image de la région elle-même, est un pôle d'attraction pour les migrants internes en provenance d'autres régions du Sénégal à la recherche d'opportunités économiques. De plus, il accueille également des migrants internationaux, notamment des étudiants et des travailleurs étrangers. Les communes de Sicap-Liberté et de Mermoz-Sacré-

[20] ANSD, Recensement général de population et de l'habitat (RGPH5) 2023

Cœur, dans lesquelles nous avons sélectionné notre échantillon d'étude, se retrouvent respectivement avec des poids démographiques de 41079 habitants et 38598 habitants[21]. La commune de Sicap-Liberté est marquée par une forte densité, avec 20539hbts/km2. Sa population est composée de 21692 femmes et de 19387 hommes. Quant à la commune de Mermoz-Sacré-Cœur, elle est marquée par une densité moins forte, soit 6433hbts/Km2. Elle est composée de 20623 femmes et 17975 femmes. Ces communes sont marquées par une forte urbanisation. Elles abritent ainsi plusieurs infrastructures. Parmi celles-ci, nous avons plusieurs institutions financières telles que Ecobank, Orabank, la banque de l'habitat du Sénégal (BHS), la banque sahélo-saharienne pour l'investissement et le commerce. Elles abritent également les sièges sociaux des firmes comme Wave, Orange, Promobile et du groupe Sonatel. Nous y retrouvons aussi des concessionnaires automobiles de grandes envergures telles que Showroom Hyundai et Sogafric Sénégal. La commune de Mermoz-Sacré-Cœur est divisée en deux milieux distincts par la voie de dégagement nord (VDN). D'un côté nous avons Sacré-Cœur et de l'autre se trouve Mermoz. Les communes de Sicap-Liberté et de Mermoz-Sacré-Cœur abritent le centre socio-culturel de Sacré-Cœur et des institutions sportives comme le club de football Dakar Sacré-Cœur, le stadium Marus Ndiaye et le stade Demba Diop.

2.2. Education

L'éducation de qualité est définie à la quatrième place des objectifs de développement durable. Ainsi, le Sénégal, à travers le plan Sénégal émergent (PSE), a lancé le Programme d'Amélioration de la Qualité, de l'Equité et de la Transparence du secteur de l'Education et de la Formation (PAQUET-EF). D'ailleurs ce programme s'inscrit dans un but précis à savoir : « *Un système d'Éducation et de Formation équitable, efficace, efficient, conforme aux exigences du développement économique et social, plus engagé dans la prise en charge des exclus, et fondé sur une gouvernance inclusive, une responsabilisation plus accrue des Collectivités locales et des acteurs à la base* » (ANSD, 2019). A cet effet, la mise en place d'un dispositif éducatif efficace et efficient se présente en une nécessité. Ainsi, le département de Dakar abrite à elle seule quatre cent quatre-vingt (480) établissements primaires dont cent quatre-huit (148) pour le public et trois cent trente-deux (332) pour le public. Pour ce qui est des niveaux moyen et secondaire, nous avons quatre-vingt-onze (91) établissements, dont trente-six (36) publics et cinquante-cinq (55) privés. Quant au moyen-secondaire, le département de Dakar se retrouve avec un total de cent quatorze (114) établissements, dont quinze (15) publics et quatre-vingt-dix-neuf (99) privés. De plus, le département de Dakar enregistre le plus haut taux de réussite

[21] https://www.ansd.sn/donnees-recensements?field_liste_annee_value=2023

au brevet de fin d'études moyen (BFEM) de la région de Dakar, soit 62,8% et deuxième plus haut pour ce qui est du Baccalauréat, soit 52,8% derrière le département de Pikine. (ANSD, 2020-2021)

Pour ce qui est de l'enseignement supérieur, les statistiques sont d'ordre national. Selon l'agence nationale de la statistique et de la démographie (ANSD), cent quarante-sept (147) établissements d'enseignement supérieur ont été dénombrés dans la région de Dakar en 2019. (ANSD, 2020-2021). Les communes de Mermoz-Sacré-Cœur et de Sicap-Liberté abritent plusieurs institutions scolaires et d'enseignement supérieur telles que l'institut africaine de management (IAM), l'école supérieur de génie industriel et de biologie (ESGIB), l'école des techniques internationales du commerce, de la communication et des affaires (ETICCA) etc.

Même si le nombre d'infrastructures scolaires et d'enseignement supérieur est impressionnant et que l'informatique a été intégrée dans le programme de certaines écoles et universités, certaines insuffisances sont à relever. Celles-ci tournent au tour de la sensibilisation et de la formation. Les programmes de sensibles sur la cybercriminalité ou sur les dangers d'internet ne sont pas très pris en compte. Il en est de même pour ce qui est de la formation en cybersécurité.

2.3. L'économie numérique

« *L'économie numérique constitue un domaine transversal qui représente l'ensemble des activités de production, de distribution et de consommation de biens et services ayant trait aux Télécommunications et aux TIC, à leurs usages en tant que cœur ou support dans les processus industriel, économique et sociétal*[22] ». Au Sénégal, l'économie numérique est réglementée par la loi n°2011-01 du 24 février 2011 portant code des télécommunications. Dans une perspective de mettre en place un cadre juridique pour les télécommunications et les technologies de de l'information et de la communication, cette loi promeut un accès facile à ces services et un climat favorable aux investissements qui s'y rapportent.

Aujourd'hui, l'économie numérique au Sénégal est en essor avec la digitalisation des services et administrations. Il l'est encore d'autant plus que le secteur informel a emboité le pas des technologies de l'information et de la communication avec le paiement mobile, les services d'achat, de commande et de réservation en ligne. Les réseaux sociaux ont facilité les lancements d'activités commerciales pour beaucoup de jeunes. Ils permettent à ces jeunes, désireux d'entreprendre de lancer leurs activités aussi diverses soient-elles.

[22] Ministère des postes et de télécommunications, Stratégie Sénégal Numérique 2016-2025, octobre 2016

Ainsi, Dakar détient la plus forte activité de e-commerce dans le pays, avec 61% du trafic total[23]. Ce commerce en ligne s'est accentué avec les réseaux sociaux donnent de la visibilité et facilité de commande et de vente de produits. Cependant, même si les avancés du commerce électronique sont remarquable, la cybercriminalité se présente comme un frein au développement exponentiel de cette activité. Cette dernière met à l'épreuve la confiance des usagers sur les technologies de l'information et de la communication (TIC). Ce qui soulève le problème de la fiabilité d'un cyberespace au Sénégal.

2.4. Professionnalisation des réseaux sociaux (Benhara, 2016)

Les réseaux sociaux professionnels, devenus des outils incontournables pour la visibilité et le réseautage, ont connu une montée en popularité significative, notamment dans un contexte professionnel. Originellement perçus comme des plateformes de divertissement, ils ont évolué vers une dimension professionnelle, surtout avec la généralisation du télétravail due à la pandémie de Coronavirus.

Ces plateformes spécialisées sont conçues pour faciliter le développement de réseaux professionnels, le partage d'informations sur les entreprises, les secteurs d'activité, les métiers, voire les opportunités d'emploi. Les contenus publiés sur ces sites permettent aux recruteurs, aux dirigeants d'entreprises et aux responsables des ressources humaines d'appréhender au mieux les profils des candidats et de les contacter si nécessaire.

L'émergence des médias sociaux professionnels a eu un impact considérablement positif dans le monde de l'entreprise. Ils offrent aux employés et aux chercheurs d'emploi un accès privilégié à des informations essentielles pour rester informés des dernières tendances et des opportunités professionnelles à saisir.

Pour promouvoir une image positive et développer sa visibilité professionnelle, il est essentiel de créer une identité en ligne, une pratique connue sous le nom de Personal Branding. Cette approche consiste à se présenter comme une marque en mettant en avant sa personnalité, ses compétences et ses qualités afin de démontrer sa valeur ajoutée et d'affirmer une identité distincte. Contrairement aux médias traditionnels tels que la télévision, la radio ou la presse, ainsi qu'aux stratégies payantes comme la publicité sur Google Adwords, l'utilisation des réseaux sociaux est gratuite.

[23] https://www.agenceecofin.com/internet/1002-35782-le-profil-detaille-des-nombreux-senegalais-convertis-au-e-commerce

Les réseaux sociaux ne sont pas seulement bénéfiques pour les entreprises, mais ils ont également révolutionné le commerce informel. Récemment, ce commerce s'est tourné vers les réseaux sociaux, qui sont devenus de plus en plus adaptés aux réalités socio-économiques locales. Ces plateformes inspirent les commerçants à adopter de nouvelles pratiques commerciales et favorisent l'émergence de nouveaux acteurs économiques qui étaient auparavant peu visibles.

L'utilisation croissante des réseaux sociaux au Sénégal semble avoir un impact significatif sur le commerce, favorisant notamment le développement du commerce informel. Cette dynamique complexe est le résultat de l'implication de divers acteurs. Dans ce contexte, le gouvernement sénégalais a lancé l'initiative du commerce électronique via la plateforme Trade Point Sénégal dès 1996, en réponse aux directives de la conférence des Nations Unies sur le commerce et le développement de 1992. L'objectif était de faciliter les opérations commerciales en réduisant les formalités administratives et en offrant un cadre publicitaire efficace.

Parallèlement, l'évolution des réseaux sociaux a modernisé les pratiques commerciales des entreprises sénégalaises. Ces dernières adaptent désormais leurs stratégies de marketing et de publicité au contexte numérique, en exploitant les réseaux sociaux pour interagir avec leur public, rester à jour sur les tendances et promouvoir leur marque. Les entreprises ont rapidement saisi les avantages offerts par les réseaux sociaux, notamment leur capacité à toucher un large public à moindre coût. Cette transition vers les réseaux sociaux a permis aux entreprises d'atteindre une clientèle plus vaste tout en augmentant leurs marges bénéficiaires, illustrant ainsi une convergence entre le commerce électronique et les médias sociaux.

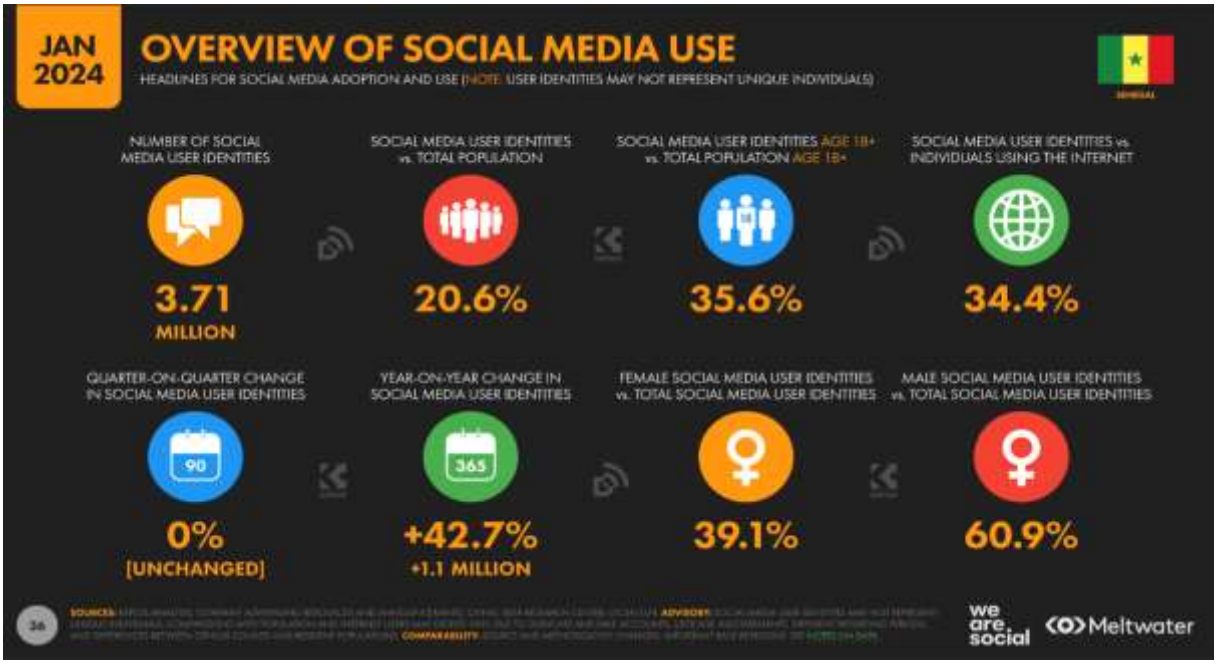
En effet, les réseaux sociaux sont devenus un moyen efficace pour développer son activité commerciale. La publicité sur les médias sociaux est une manière directe d'atteindre un public souhaité. Elle nous permet en effet de cibler de nouveaux clients ou des clients déjà existants. Tous les principaux réseaux sociaux proposent des options de publicité. Ces publicités aident à accroitre la rentabilité mais aussi sont une source de revenus pour les internautes. Des plateformes comme YouTube paient les heures de visionnage ainsi que les publicités intégrées dans les vidéos.

2.5. Présentation des réseaux sociaux au Sénégal

Avec un poids démographique de 18 032 473 habitants (ANSD, Rapport préliminaire RGPH-5, 2023), le Sénégal se retrouve avec 10,79 millions utilisateurs d'internet en janvier 2024 ; soit un taux de pénétration d'internet de 60% (DataReportal, Meltwater, & WeAreSocial, 2024). De

plus, un total de 21,92 millions de connexions mobiles a été comptabilisé au Sénégal en Janvier 2024. Ce qui équivaut à 121,8% de la population totale. Le développement de l'internet mobile au Sénégal connait de beaux jours avec d'importants débits de connexion. La connexion internet mobile via les réseaux cellulaires y est aujourd'hui à une vitesse de 27,16 Mbps. Par contre, la connexion internet fixe est à une vitesse de 21,98 Mbps. Même si les avancés enregistrées dans le domaine du numérique sont important, il reste, cependant, beaucoup de chemin au Sénégal à parcourir.

Image 1 : Répartition des utilisateurs des réseaux sociaux au Sénégal



Source : NOISY DIGITAL https://noisydigital.com/les-reseaux-sociaux-au-senegal-les-chiffres-en-2024/

2.5.1. WhatsApp

Selon le docteur en communication Mamadou Ndiaye du centre d'études des sciences et techniques de l'information (CESTI), WhatsApp est le réseau social le plus utilisé au Sénégal avec plus de huit (8) millions d'utilisateurs[24]. A la différence des autres applications fixant âge particulier pour leurs utilisateurs, WhatsApp peut être utilisé par toute personne disposant d'un smartphone. De par ses fonctionnalités, ce réseau social permet le regroupement virtuel de familles, de membres d'associations, de collègues de travail etc. Au Sénégal, ses usages sont

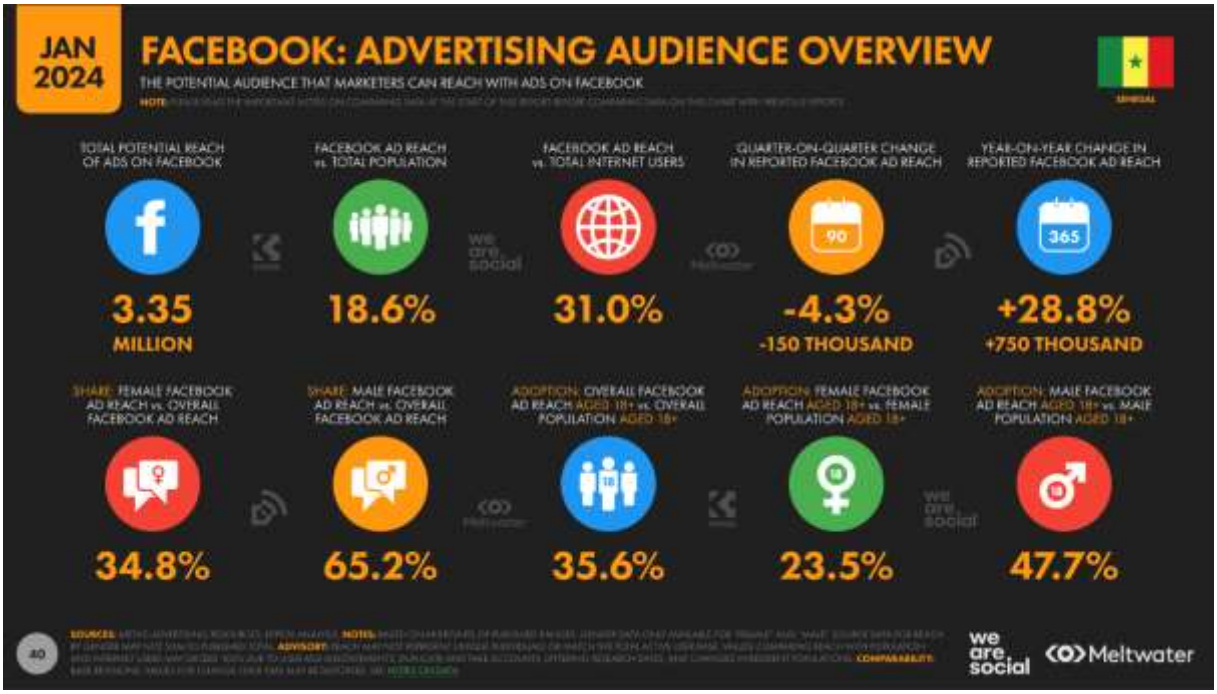
[24] https://www.leral.net/8-millions-d-utilisateurs-WhatsApp-au-Senegal_a238157.html#:~:text=net%2DSi%201%2C5%20milliards,millions%20d'utilisateurs%20au%20S%C3%A9n%C3%A9gal.

plus de l'ordre du maintien et de la création de nouveaux liens sociaux. Cependant, l'application WhatsApp est devenu un outil de commerce en ligne permettant aujourd'hui à bon nombre de sénégalais de faire la promotion de leurs produits. Il est devenu un outil incontournable dans les formes d'entreprenariats. Toutefois, il est à préciser que ce réseau social est également utilisé à des fins cybercriminelles comme la diffusion de fausses nouvelles, l'escroquerie, la diffusion de données personnelles de tout genre, etc.

2.5.2. Facebook

Facebook est une plateforme d'échanges sociales et de communications du groupe Meta dont le propriétaire et fondateur est Mark Zuckerberg. C'est un réseau social très utilisé au Sénégal avec 3,35 millions d'utilisateurs en Janvier 2024. Ce qui représente 18,6% de la population sénégalaise et 31% des 10,79 millions d'utilisateurs d'internet dénombrés en Janvier 2024. Il convient de souligner Meta permet uniquement aux personnes âgées de 13 ans et plus d'utiliser Facebook. De par ses fonctionnalités, Facebook permet à ses usagers de créer des liens et de maintenir ceux déjà existants. Elle permet également à ses utilisateurs de s'intégrer en se créant des amis même s'ils sont virtuels. Les usages ayant évolués, Facebook est devenu plateforme commerciale où chacun peut proposer ses services et se trouver une clientèle. Il est aujourd'hui adapté à la recherche d'emploi et au recrutement. Cependant, même si les potentialités décrites sont tout à fait impressionnantes et légales, ce réseau social renferme des pratiques illégales. Des activités telles que l'escroquerie, l'usurpation d'identité, la prostitution en ligne, le cyber-harcèlement y sont devenues très courantes.

Image 2 : Répartition des utilisateurs de Facebook au Sénégal



Source : NOISY DIGITAL https://noisydigital.com/les-reseaux-sociaux-au-senegal-les-chiffres-en-2024/

2.5.3. YouTube

YouTube est une plateforme d'écoute musicale et de visionnage de clips musicaux, de téléfilms, de séries cinématographiques et de vidéos de tout genre. Le réseau social a eu 3,71 millions d'utilisateurs au Sénégal en Janvier 2024. Ce qui représente 20,6% de la population sénégalaise et 34,4% des 10,79 millions d'utilisateurs d'internet du pays. Ce réseau social est plus utilisé au Sénégal pour le visionnage et la création de contenus. Avec les maisons de productions cinématographiques, théâtrales et musicales, le nombre d'utilisateurs de YouTube augmente d'année en année. De plus, plusieurs métiers ont vu le jour où se sont développés au Sénégal grâce à ce réseau social : youtubeur, influenceur, marketing digital, community manager. Il s'agit des créateurs de contenus, désignés sous le vocable de Youtubeurs. C'est un métier très en vogue, effectué par plusieurs jeunes sénégalais. Cependant, sont observables des usages de ce réseau social socialement et/ou juridiquement répréhensibles. Ces derniers sont de l'ordre des diffusions de fausses nouvelles, des injures et diffamations etc.

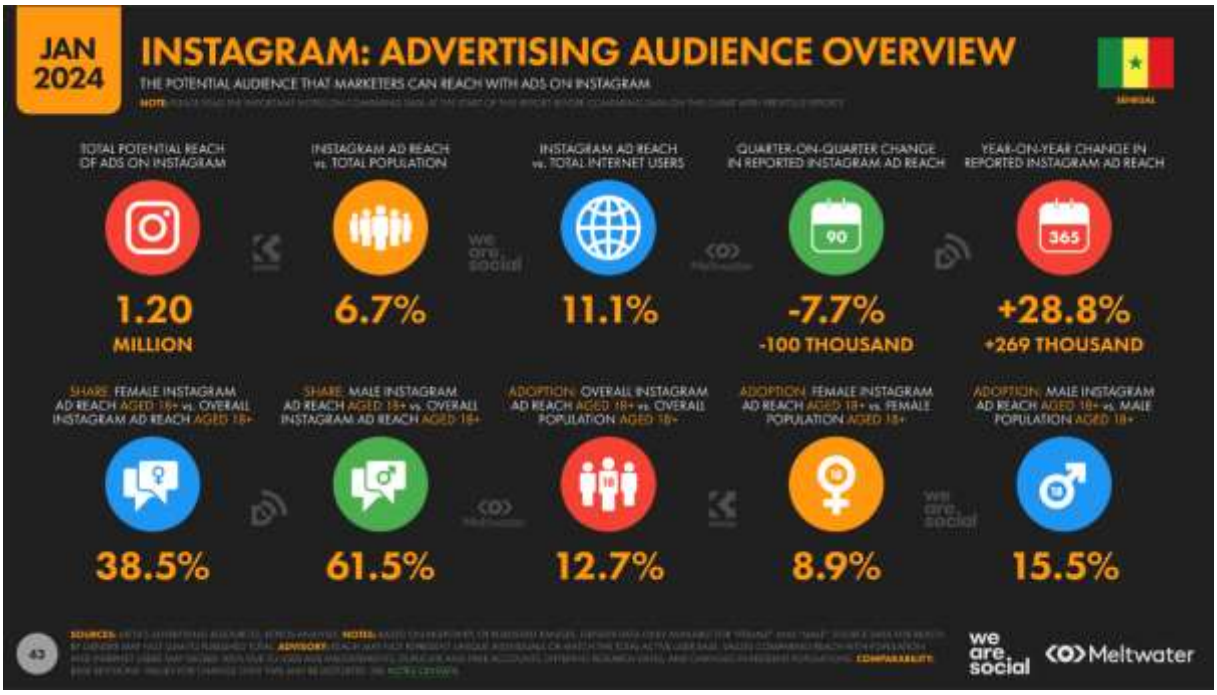
Image 3 : Répartition des utilisateurs de YouTube auSénégal

Source : NOISY DIGITAL https://noisydigital.com/les-reseaux-sociaux-au-senegal-les-chiffres-en-2024/

2.5.4. Instagram

Comme Facebook, Instagram est une propriété du groupe Meta. Il a les mêmes fonctionnalités de messageries instantanées que les autres réseaux sociaux du groupe Meta. C'est l'une des applications les plus déterminantes dans le monde de la publicité et de l'influence. D'ailleurs, des classements des personnalités sont très souvent faits en se basant sur leur nombre d'abonnés. La première place de ce classement est aujourd'hui occupé par le footballeur portugais Cristiano Ronaldo 629 millions d'abonnés répartis dans le monde. Par contre, le joueur de Football Sadio Mané est le sénégalais le plus suivi sur Instagram avec 16,7 millions d'abonnés. Ainsi, le nombre d'utilisateurs du réseau social au Sénégal s'élève à 1,2 millions ; soit 6,7% de la population du Sénégal et 11,1% des 10,79 millions de sénégalais utilisateurs d'internet. Instagram favorise le développement du commerce électronique avec la publicité gratuite. Il permet le partage et la diffusion d'informations et de contenus de tous genres. Cependant, comme dans les autres réseaux sociaux, des usages illégaux y sont observables. Ceux-ci peuvent être de l'ordre du proxénétisme et de la prostitution en ligne, des sextorsions, de la diffusion de données personnelles, de cyber-harcèlement etc.

Image 4 : Répartition des utilisateurs d'Instagram au Sénégal

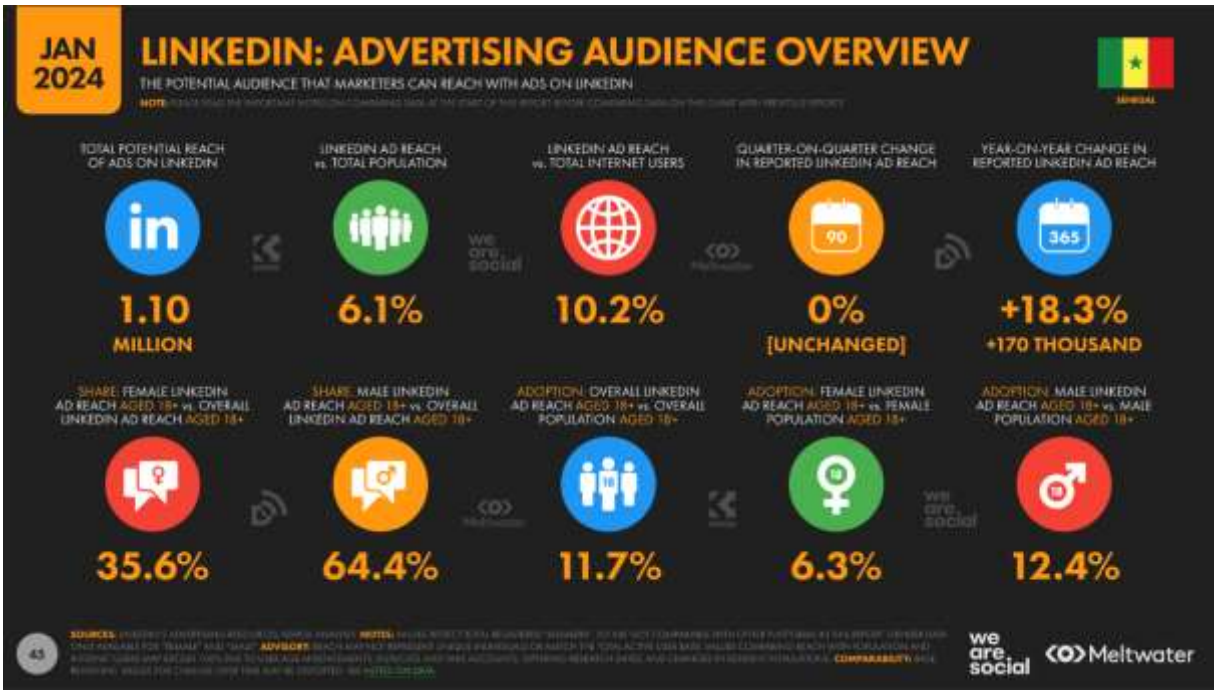


Source : NOISY DIGITAL https://noisydigital.com/les-reseaux-sociaux-au-senegal-les-chiffres-en-2024/

2.5.5. LinkedIn

LinkedIn est un réseau social professionnel qui permet la recherche d'emploi, le recrutement et la valorisation des compétences. Il permet aux demandeurs d'emplois de créer des profils mettant en valeur leurs compétences et expériences. Il permet aussi aux recruteurs et entreprises de faire des appels d'offre ou de la prospection pour détecter de potentiels employés ou collaborateurs. Le nombre d'utilisateurs de LinkedIn au Sénégal s'élève à 1,1 millions ; soit 6,1% de la population du Sénégal et 10,2% des 10,79 millions d'utilisateurs sénégalais d'internet. L'essor de ce réseau social est remarquable du fait des possibilités qu'il renferme.

Image 5 : Répartition des utilisateurs de LinkedIn au Sénégal

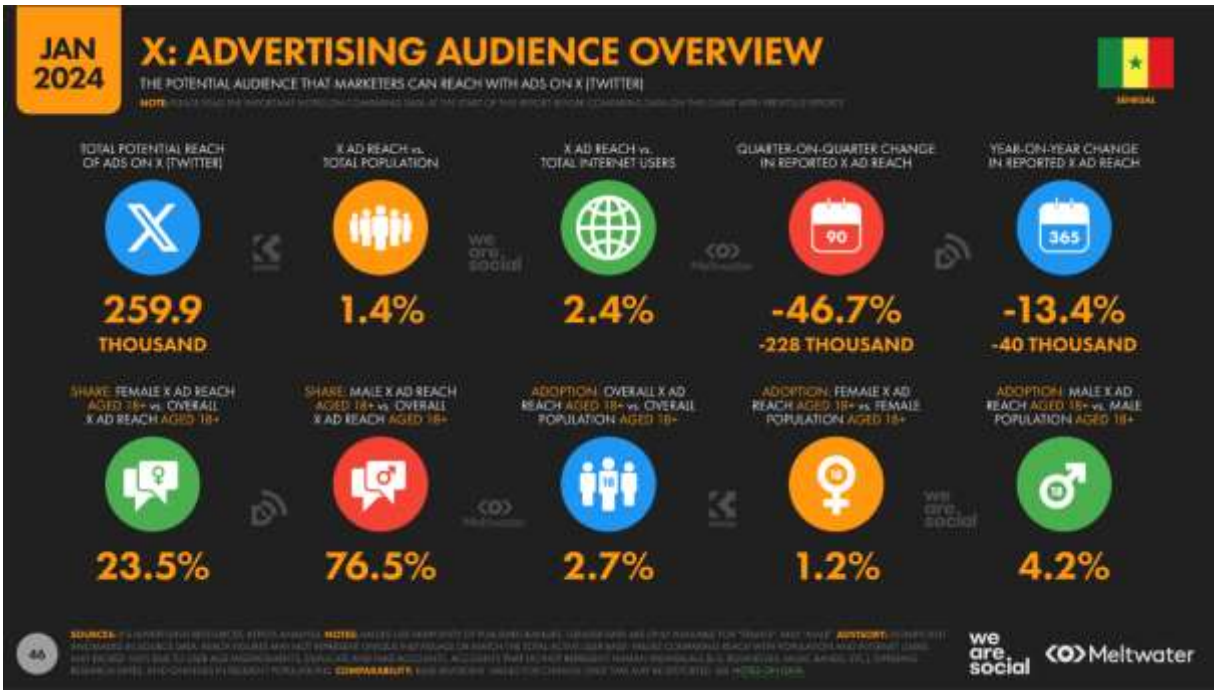


Source : NOISY DIGITAL https://noisydigital.com/les-reseaux-sociaux-au-senegal-les-chiffres-en-2024/

2.5.6. X (Twitter)

Twitter rebaptisé X comptabilise plus 259 mille utilisateurs au Sénégal. Ce qui représente 1,4% de la population du Sénégal et 2,4% des 10,79 millions d'utilisateurs d'internet du pays. Sur ce réseau social, sont observables des activités illégales comme la diffusion de fausses nouvelles, de données personnelles, du cyber-harcèlement etc. Le réseau social X a été une plateforme très utilisée durant la période d'instabilités politiques et sociales qui ont animées le Sénégal de Mars 2021 à Février 2024. Elle a été utilisée comme moyen de dénonciation sur la situation politique et sociale du pays.

Image 6 : Répartition des utilisateurs de X (ex Twitter) au Sénégal



Source : NOISY DIGITAL [*https://noisydigital.com/les-reseaux-sociaux-au-senegal-les-chiffres-en-2024/*](https://noisydigital.com/les-reseaux-sociaux-au-senegal-les-chiffres-en-2024/)

A l'image de la région de Dakar, les communes de Sicap-Liberté et de Mermoz-Sacré-Cœur sont marquées par une forte urbanisation. Elles abritent plusieurs institutions financières, sportives, des entreprises automobiles etc. Elles représentent l'espace physique de notre zone de recherche dans laquelle nous avons effectué nos entretiens et administré notre questionnaire. Quant à la partie virtuelle de notre zone de recherche, elle concerne les réseaux sociaux. Ces derniers sont fortement utilisés au Sénégal pour divers besoins. À l'intérieur de ceux-ci, nous avons procédé à de l'observation directe afin de collecter des données.

2.6. Justification et pertinence du sujet

Dans un monde hyper-connecté et dominé par les réseaux sociaux et l'internet en général, choisir d'étudier la criminalité qui se déroule dans cet univers peut sembler évident pour nous chercheurs en sociologie. Cette évidence est due au fait que cet univers numérique, constitue en partie des réseaux sociaux, est régi par un système de relation entre utilisateurs des plateformes d'échanges.

Avec comme objet d'étude les faits sociaux, il incombe donc au sociologue de s'intéresser à un système d'interactions et de relations tel que les réseaux sociaux. Qui plus est quand se produit dans ce système des actions socialement et/ou juridiquement réprimandées. Ce qui fait de ces

actions des crimes, par conséquent des faits sociaux. Le crime est un fait social auquel la sociologie, comme discipline des sciences sociales, s'est longtemps intéresser pour l'appréhender.

Et pour ce qui est de cet intérêt personnel sur la thématique de la cybercriminalité dans les réseaux sociaux au Sénégal, cela vient d'un constat fait à la fois en tant qu'utilisateur de ces plateformes sociales, mais aussi en tant qu'apprenti sociologue désireux de comprendre les dynamiques de cet espace numérique.

Pour ce qui est de ce constat, nombreux sont les utilisateurs des réseaux sociaux qui disaient avoir été victime de faits qui selon la législation sénégalaise sur le numérique relèvent de la cybercriminalité. Les principaux cas à avoir été constatés sont des escroqueries en ligne, des usurpations d'identité numérique, la diffusion d'images ou vidéos à caractère sexuel.

Face à ces constats, la nécessité d'approfondir la compréhension de ce phénomène s'est manifesté en des questionnements dont la seule façon d'avoir les réponses était d'investir cette problématique à travers des enquêtes sociologiques. Enquêtes qui vont nous permettre de saisir les facteurs explicatifs, la typologie et les représentations sociales au tour de la cybercriminalité dans les réseaux sociaux.

Chapitre 3 : Approche méthodologique de la recherche

Pour appréhender un fait social, le chercheur en sciences sociales en général et en sociologie en particulier fonde son raisonnement sur une base méthodologique très claire et appropriée. C'est cette méthodologie qui confère à la recherche sociologique son caractère scientifique, puisqu'elle fait partie des critères de scientificité.

C'est d'ailleurs sur cette logique que s'inscrit Grawitz en disant : *« la méthode est l'ensemble des opérations intellectuelles par lesquelles une discussion cherche à atteindre les vérités qu'elle poursuit, les démontre, les vérifie* » (Grawitz, 1996). Autrement dit, c'est cette méthodologie qui permet au chercheur d'établir les canevas de recherche, pour ensuite collecter des données qui vont être analysées, pour enfin produire des conclusions explicatives de la problématique de recherche.

En sociologie, deux approches s'offrent généralement aux chercheurs dans le cadre de sa recherche : approche qualitative et celle quantitative. Il lui appartient alors d'utiliser l'une des deux approches ou de procéder peut-être à leur combinaison. Le choix de la méthodologie se fait très souvent par rapport au sujet en question et de ce que l'on veut faire ressortir au cours de sa recherche.

Et vu que notre sujet d'étude est la cybercriminalité dans les réseaux sociaux, nous utiliserons les deux méthodes pour mieux appréhender ce phénomène social. La combinaison des approches de recherche se justifie ici par le fait que pour saisir les formes et les causes de ce phénomène social, l'utilisation à la fois de statistiques et des données qualitatives est la meilleure façon d'atteindre nos objectifs de recherche. La combinaison des approches est désignée sous le vocable de triangulation qui à son tour désigne « *un principe de chevauchement des méthodes visant à mieux percevoir la richesse, la complexité du comportement humain* » (Tine, 2004)

Quant aux représentations sociales, qui relèvent de la perception des individus sur la cybercriminalité dans les réseaux sociaux, l'utilisation de procédé qualitatif semble plus appropriée pour les saisir. Ce cumul méthodologique permet d'appréhender notre sujet dans son ensemble et de l'aborder de façon plus ou moins exhaustive. L'utilisation des deux méthodes fait que notre enquête se déroulera en deux phases distinctes.

Dans la première phase d'enquête, nous utiliserons l'approche quantitative avec laquelle nous nous appuierons sur l'administration de questionnaires pour savoir ce qu'il en est des formes et

des facteurs explicatifs de la cybercriminalité dans les réseaux sociaux. Ces questionnaires seront essentiellement administrés aux utilisateurs des réseaux sociaux.

Puis dans la deuxième phase d'enquête, il sera question de procéder à une série d'entretiens pour saisir non seulement les représentations sociales au tour de la cybercriminalité, mais aussi d'apprécier les motivations des « cybercriminels » ; autrement dit les causes. Ces séries d'entretiens vont permettre de faire le point sur la situation de la cybercriminalité au Sénégal, en mettant en lumière les politiques publiques sur la cybersécurité, de sensibilisation sur la cybercriminalité, sur la législation Sénégalaise en la matière, sur l'appareil juridico-institutionnel sénégalais sur la cybercriminalité. Cela nous permettra aussi sans doute d'avoir accès aux statistiques nécessaires pour saisir les différentes formes de cybercrimes que nous avons sur les réseaux sociaux au Sénégal et à quelle fréquence ils se manifestent.

3.1. Méthodes et techniques de recherche

A cette étape de la recherche, il s'agit de porter un choix sur les méthodes et techniques d'enquête qui conviennent à notre problématique de recherche en vue de collecter les données nécessaires pour l'analyse de notre sujet d'étude. Pour se faire, nous avons choisi des procédés d'investigation tels que : l'enquête exploratoire ou la préenquête, la recherche documentaire, les entretiens, les enquêtes par questionnaires et l'observation.

Avant de procéder à l'enquête de terrain proprement dit, nous avons jugé nécessaire de faire d'abord une recherche documentaire qui nous a non seulement permis de cerner notre objet d'étude à savoir la cybercriminalité dans les réseaux sociaux, mais aussi de faire l'état des lieux de notre problématique de recherche.

La combinaison des approches méthodologiques nous pousse à choisir pour chacune des méthodes de recherche les techniques et outils de collecte de données qui nous permettront d'avoir les éléments nécessaires pour appréhender notre thématique de recherche.

3.1.1. La recherche documentaire

Cette étape de la recherche nous permet en tant que chercheur d'avoir un aperçu sur ce qui a été dit ou fait sur le sujet en question ou sur les thématiques qui s'y rapportent. Ce qui, sans nul doute, oriente notre recherche pour la rendre particulière et originale. Ce qui tout de même est ou doit être la visée de toute production scientifique. Elle doit s'inscrire dans une perspective de faire évoluer et d'apporter une plus-value à ce domaine de recherche.

Pour faire ce travail sur un sujet tel que la cybercriminalité dans les réseaux sociaux, il est primordial de visiter les productions sur le numérique en général, sur le crime et pour plus de spécificité s'intéresser à la littérature sur la cybercriminalité pour comprendre ce phénomène. Une fois cette compréhension faite, l'idée sera maintenant de saisir les particularités de la cybercriminalité dans les réseaux sociaux. Et par particularités, nous voulons souligner les différentes formes de cybercrimes que nous avons dans les réseaux sociaux au Sénégal.

Après avoir visité ces productions antérieures, nous pouvons dire en somme qu'elles ont facilité l'orientation de notre recherche en nous permettant de l'inscrire dans un continuum. Cette phase exploratoire ou recherche documentaire est l'étape la plus longue dans ce travail de recherche parce qu'elle ne se termine pratiquement jamais. Elle s'est déroulée en grande partie sur internet. Par conséquent, nous avons accédé des bibliothèques numériques et des sites de documentation en ligne à savoir : la bibliothèque numérique de l'université Cheikh Anta Diop de Dakar (UCAD), à des sites des documentations comme Google scolar, Semantic scolar, Cairn info, Persée, thèse.fr, OpenEdition… et dans des sites sur les technologies de l'information et de la communication (TIC) comme : OSIRIS et KASPERSKY. Nous avons aussi exploré les rapports des services comme la commission de protection des données personnelles (CDP) et de la division spéciale de cybersécurité de la police (DSC).

Cette étape de la recherche nous a permis de faire un état des lieux sur les formes de cybercrimes tant au niveau international qu'africain, les facteurs cyber-criminogènes et les différentes stratégies de cybersécurité et lutte contre la cybercriminalité. Dans la bibliothèque numérique de l'université Cheikh Anta Diop (UCAD) bibnum.ucad.sn, nous avons consulté des mémoires portant sur la transmission des données et la sécurité de l'information. Ce qui nous a permis d'avoir un aperçu sur les infractions liées à la transmission des données informatiques. Sur le site OSIRIS, nous avons consulté des articles sur la cybercriminalité au Sénégal et recueilli des informations sur l'historicité de ce phénomène. Ce qui nous a permis de faire la chronologie de la législation sénégalaise sur la cybercriminalité en relevant les premières infractions. Sur Kaspersky, nous avons accédé à un ensemble de statistiques sur la cybercriminalité dans le monde et le classement des différents pays selon la fréquence des attaques cybercriminelles.

3.1.2. Le prétest

Le prétest est cette étape de la recherche durant laquelle le chercheur teste ses outils de collecte de données. Pour ce qui est de notre étude, nous avons testé notre questionnaire et un de nos guides d'entretiens qui étaient destinés aux utilisateurs des réseaux sociaux. Ce prétest nous a permis d'affiner nos outils de collecte en relevant les niveaux de pertinence de nos différentes

questions. Pour ce qui est des tests sur nos guides d'entretien, ils nous ont permis de ne pas nous limiter uniquement aux conséquences individuelles de la cybercriminalité dans les réseaux sociaux, mais d'aller plus loin en nous intéressant aux répercussions sociales dans leur généralité.

3.1.3. L'échantillonnage

« *L'échantillon est un sous ensemble de personnes tirées d'une population mère à tel point que les observations faites à partir de ce sous-groupe puissent être généralisées à l'ensemble de la population* » (Tine, 2004). Cette définition de l'échantillon suppose déjà l'usage de techniques d'échantillonnage. Parce que celles-ci confèrent à la recherche une légitimité scientifique.

Même si notre problématique de recherche concerne le Sénégal dans son ensemble, il est clair que nous ne pouvons pas interroger l'ensemble des utilisateurs des réseaux sociaux du Sénégal. D'autant plus que notre champ d'étude se trouve être une partie du département de Dakar. C'est pourquoi il est impératif de définir un échantillon réduit de la population cible. La définition de l'échantillon obéit à plusieurs critères et permet, après enquête, au chercheur de dégager des conclusions qui pourront s'appliquer à l'ensemble de la population ou à la frange de la population concernée.

L'échantillonnage est le procédé par lequel le chercheur fait une sélection des individus à interroger à l'intérieur de sa population mère. Le fait d'interroger ces individus permet au chercheur de comprendre le phénomène social qu'il étudie. C'est d'ailleurs ce que Meynaud et Duclos explique en ces termes : « *La théorie mathématique des probabilités suppose que, pour connaître les événements qui peuvent survenir dans une population donnée, il n'est possible d'étudier ou d'interroger qu'une petite partie de celle-ci, à condition de respecter des règles rigoureuses de sélection de cette fraction de population. Seules garanties de sa représentativité*. » (Meynaud & Duclos, 2007)

Autrement dit, nous devons sélectionner un nombre restreint parmi les utilisateurs des réseaux sociaux au Sénégal. Ce nombre représentatif est par rapport à l'ensemble plus grand c'est-à-dire la population mère.

3.1.3.1. Le choix de la population

Quand on parle de population dans une recherche en sciences sociales, particulièrement en sociologie, on fait allusion à la frange de société qui est directement concernée par la problématique de recherche. Ainsi, dans ce concept de population, nous avons deux niveaux. Le premier niveau, appelé population mère, est l'ensemble plus vaste dans lequel nous

retrouvons le deuxième niveau de population. Elle va toucher à un secteur dans sa globalité. Comme pour notre problématique, cette population mère est constituée de l'ensemble des acteurs qui gravitent autour des technologies de l'information et de communication (TIC).

Pour le second niveau de population, nous avons la population cible, qui est l'unité de recherche restreinte sur laquelle la collecte de données est effectuée. Et pour ce qui est de la cybercriminalité dans les réseaux sociaux, la population cible est par ailleurs déjà définie dans l'intitulé du sujet d'étude. Ce qui fait que notre population cible est l'ensemble des utilisateurs des réseaux sociaux, complété par les instances de régulation, de contrôle et de gestion de la dynamique de ce milieu virtuel relationnel. Autrement dit, nous allons effectuer nous enquêtes non seulement auprès des utilisateurs des réseaux sociaux au Sénégal, mais aussi d'organismes comme la gendarmerie, la police, la commission de protection des données personnelles (CDP) entre autres.

3.1.3.2. La techniques d'échantillonnage

Cette sélection est due au fait que la constitution de l'échantillon d'étude demeure problématique, étant donné que l'on ne maitrise pas la population mère de notre étude. La non maitrise de la population mère réside dans le fait qu'il n'y a pas de statistiques sur le nombre d'utilisateurs de réseaux sociaux résidents dans la ville de Dakar, qui représente notre champ d'étude.

En ce qui concerne notre problématique, à savoir la cybercriminalité dans les réseaux sociaux, nous avons de procéder par une méthode d'échantillonnage non probabiliste en combinant deux techniques.

En premier, nous avons utilisé l'échantillonnage par convenance, qui est une technique où les unités de recherche ou les individus à enquêter sont disponibles et faciles à accéder.

Et comme deuxième technique, nous avons utilisé la technique d'échantillonnage par boule de neige. Celle-ci est basée sur des réseaux de référence dans lequel ce sont les enquêtés qui recommandent à l'enquêteur les personnes à enquêter qui présentent les critères de sélection de la population cible. Nous avons choisi cette technique d'échantillonnage pour avoir accès à un nombre important d'utilisateurs de réseaux sociaux ayant été victimes de cybercrimes sur les réseaux sociaux afin de faire apparaitre la diversité des cybercrimes dans les réseaux sociaux. Et ceci étant donné qu'esquisser les formes de cybercrimes dans les réseaux sociaux se trouve être un des objectifs de cette étude. Même si cette technique d'échantillonnage est très souvent jugée comme comportant plusieurs biais, mais elle est pertinente dans le cas de figure où le

chercheur se retrouve avec une population homogène. Ce qui est le cas pour notre population d'étude qui regroupe l'ensemble des utilisateurs des réseaux sociaux. En raison de la non maitrise de la population d'étude au niveau de notre zone d'étude, nous nous sommes rabattu sur des choix non probabiliste pour déterminer notre échantillon d'étude.

3.1.4. Les techniques de collecte

Les techniques de collecte de données correspondent aux différents procédés par lesquels le chercheur recueille les informations lui permettant de tester ses hypothèses et de répondre à ses questions de recherche.

3.1.4.1. L'histoire de la collecte des données

Dans cette partie, il est question de faire le déroulé de notre collecte de données. C'est-à-dire ce qu'on a eu à faire en tant que chercheur pour parvenir à collecter les données nécessaires pour notre étude. La complexité de notre thématique de recherche, nous amène à mener la recherche à travers deux espaces : milieu physique et milieu virtuel.

L'étape de la recherche qui s'est déroulée dans le milieu physique, c'est-à-dire les communes de Sicap-Liberté et Mermoz-Sacré-Cœur, s'est matérialisée par l'administration de questionnaires et des séries d'entretien. Ainsi, la première chose faite pour cette étude a été d'identifiée les différents acteurs qui gravitent autour de la cybercriminalité au Sénégal. Une fois chose faite, les rencontrer a été l'étape suivante dans le but d'effectuer des entretiens avec eux et d'administrer à notre échantillon d'étude notre questionnaire d'enquête. L'administration du questionnaire s'est faite au bout de deux (2) mois, soit de Septembre à Novembre 2023.

Avec la coopération de ces différents services, nous avons pu avoir des statistiques assez importantes en accédant à leurs rapports. Ces entretiens ont permis de saisir la situation de la cybercriminalité au Sénégal, de la typologie des cybercrimes, des profils de cybercriminels et de victimes etc. C'est ainsi que nous avons effectué des entretiens au niveau de services de cybersécurité et de lutte contre la cybercriminalité. Nous en avons effectué deux au niveau de la Plateforme numérique de lutte contre la cybercriminalité (PNLC), un au niveau de la Division spéciale de cybersécurité (DSC), un autre à la Direction de la police judiciaire (DPJ). Nous avons aussi effectué un entretien au niveau de la Commission de protection des données personnelles (CDP). Ces entretiens ont été menés avec des experts en cybersécurité et de lutte contre la cybercriminalité, pour la majeure partie faisant partie des forces de défense et de sécurité du Sénégal. Les interviews au niveau de ces services ont débuté en Septembre 2023 en raison du contexte politique qui prévalait et se sont achevés en octobre 2023.

Au-delà de ceux-ci, les enquêtes auprès des utilisateurs des réseaux sociaux et d'autres personnes ressources nous ont permis de recueillir des informations très vitales pour cette étude. Ces dernières le sont parce qu'elles représentent les opinions, les expériences de nos enquêtés et aussi leurs représentations par rapport à la cybercriminalité dans les réseaux sociaux. Ces entretiens quant à eux ont débuté un peu plutôt. Il y a eu ceux effectués durant la phase exploration au mois de Juin 2023. La deuxième partie des entretiens s'est déroulée entre Septembre et Novembre 2023 avec essentiellement des utilisateurs de réseaux sociaux.

En revanche, pour ce qui est du milieu virtuel, c'est-à-dire le cyberespace, nous avons utilisé l'observation directe comme technique de collecte de données. Ce qui nous a permis d'observer les victimes de cybercriminalité dans les réseaux sociaux, dans une certaine mesure les cybercriminels et de façon globale les utilisateurs des réseaux sociaux. L'observation s'est faite dans plusieurs réseaux sociaux où nous avons observé les utilisations dans leurs groupes de discussions et à travers leurs différents comptes de réseaux sociaux. Cette étape est sans doute celle de la collecte de données qui a le plus duré. Elle a commencé en juin 2022 et s'est terminée en Mars 2024.

3.1.4.2. Les techniques quantitatives de collecte

La méthodologie de recherche quantitative est appliquée en sciences sociales parce que l'on admet l'idée selon laquelle la réalité peut être mesurée ou quantifiée. En effet ce caractère quantitatif traduit la réalité du phénomène social étudié. Elle permet à travers des valeurs numériques de mettre en relations des variables pour arriver expliquer et comprendre un phénomène social.

Le principe directeur de cette méthodologie de cherche est la représentativité. De ce fait, elle permet au chercheur de catégoriser les particularités qui se sont dégagées à travers les données statistiques issues des réponses de ses enquêtés.

3.1.4.2.1. L'enquête par questionnaire

Le questionnaire est un outil de collecte de données utilisé dans le cadre d'une approche quantitative. L'administration du questionnaire permet au chercheur d'interroger un échantillon plus large de sa population cible. Le questionnaire obéit à une démarche bien structurée avec une chronologie bien déterminée. Il se constitue en une série de question bien structurées et ordonnées que l'on pose à un informateur.

L'administration du questionnaire peut se faire de plusieurs façons. Cependant dans le cadre de notre étude sur la cybercriminalité dans les réseaux sociaux, nous avons opté d'administrer

notre questionnaire de deux manières. La première a été indirecte, c'est-à-dire par le biais d'internet avec la création d'un lien qui permet à nos différentes cibles d'y accéder et de le remplir à leur convenance. Ce qui nous as permis de gagner en rapidité et d'amoindrir notre charge de travail. Et la seconde a été faite physiquement où nous sommes allés sur le terrain pour administrer directement notre questionnaire. L'administration du questionnaire s'est faite auprès d'un échantillon de cent (100) individus. Cette opération n'a nécessité qu'un seul type de questionnaire parce qu'elle n'a concerné que les utilisateurs des réseaux sociaux.

3.1.4.3. Les techniques qualitatives de collecte

L'approche qualitative en sciences sociales permet de saisir une réalité sociale à travers des discours, des perceptions, des témoignages et des représentations. Ce qui implique que les données d'enquête ne seront en aucun cas mesurables, puisque c'est une approche descriptive qui se concentre plus sur les expériences de acteurs sociaux.

Par ailleurs, le principe directeur de cette méthode de recherche est la diversification. Cette dernière implique de recueillir, auprès d'une population bien définie, un ensemble de points de vue. De plus la méthode qualitative est une approche dans laquelle on retrouve des techniques d'enquête qui offrent à l'enquêté la possibilité d'expliquer son point de vue de façon plus explicite. Et pour parvenir à recueillir ces données, le chercheur utilise généralement des techniques de collecte de données telles que l'observation et l'entretien.

Avec cette méthode de recherche, nous avons utilisé essentiellement comme outil d'enquête le guide d'entretien, qui est l'élément primordial pour une bonne application des techniques d'enquêtes qualitatives. Ces dernières s'exécutent sous forme d'entretien. En plus de celui-ci nous avons utilisé la grille d'observation.

3.1.4.3.1. L'enquête par entretien

L'entretien en soi est une technique de collecte de données qualitative qui permet au chercheur d'interagir avec les personnes ressources, capables d'apporter des informations nécessaires à son étude et de façon plus large à sa population cible. Ainsi, Madeleine Grawitz définit l'entretien en le qualifiant de « *technique de recueil de données qui consiste en un procédé d'investigation scientifique utilisant un processus de communication verbale pour recueillir des informations en relation avec le but fixé* » (Grawitz, 1996). L'entretien obéit aux principes de l'interaction nécessaire au bon déroulement de l'interview. Il permet à l'enquêteur d'obtenir des informations sur chaque thématique et au besoin d'approfondir les réponses de ses enquêtés.

L’entretien comporte trois niveaux ou possibilités pour le chercheur. Ce dernier a la possibilité de faire soit un entretien directif ou semi-directif ou encore un entretien libre. Ces types d’entretiens se différencient par les niveaux de libertés qui seront offerts à l’enquêteur et aux enquêtés à travers les différentes questions qu’ils auront à aborder. L’entretien est l’occasion pour l’interlocuteur d’évoquer sa réalité en parlant de ses impressions, représentations et peut être même évoquer ses expériences (récit de vie).

Pour cette étude, nous avons choisi l’entretien semi-directif comme technique de collecte de données. Celui-ci nous permet de donner à nos enquêtés la latitude nécessaire pour qu’ils puissent argumenter leurs propos. Ainsi, nous aurons plus de détails sur les informations et plus de facilité à comprendre leurs points de vue. En tout, nous avons mené dix-sept (17) séries d’entretiens. Au bout de ces séries d’entretiens, nous sommes rendu compte de la redondance des informations recueillies. Ce qui signifie que nous avons atteint la saturation. Cette opération a nécessité l’utilisation deux guides d’entretiens. Le premier est destiné aux agents des services de cybersécurité et de lutte contre la cybercriminalité. Quant au second, il est destiné aux utilisateurs des réseaux sociaux.

Le guide d’entretien est un outil d’enquête qualitative qui permet au chercheur de préparer son entretien. Il permet au chercheur d’établir une ligne directrice au travers de laquelle se dérouleront les entretiens qu’il aura à effectuer sur le terrain. Le guide d’entretien est établi sous forme de thématique. Il regroupe les différents axes que le chercheur veut aborder dans sa recherche. Comme son nom l’indique, il va guider le chercheur lors des entretiens.

Dans cette approche, le guide d’entretien est élaboré sous forme de thématiques, au sein desquelles nous avons différentes variables.

Tableau 7 : Thématiques des guides d'entretien

Thème 1	Rôles et missions des services de lutte contre la cybercriminalité
Thème 2	Situation de la cybercriminalité dans les réseaux sociaux au Sénégal
Thème 3	Les facteurs explicatifs de la cybercriminalité dans les réseaux sociaux au Sénégal
Thème 4	Les formes de cybercrimes dans les réseaux sociaux et les techniques de commission
Thème 5	Les profils des cybercriminels et des victimes
Thème 6	La législation et les politiques publiques sur la cybercriminalité
Thème 7	Les réactions (sociales, juridiques et étatiques)
Thème 8	Les représentations sociales au tour de la cybercriminalité dans les réseaux sociaux au Sénégal
Thème 9	Répercussions sur la vie sociale (privée et publique)

Tableau 8 : Récapitulatif des entretiens effectués

Pseudo	Profession	Sexe	Age (ans)	Statut matrimonial
Commissaire Kandé	Policier/DSC	Homme		
Lt Ndour	Policier/DPJ	Homme		
Lt Niang	Gendarme ingénieur/PNLC	Homme		
S/Lt Kassé	Gendarme technicien/PNLC	Homme		
M. Bakhoum	Agent de la CDP	Homme		
S.D	Etudiant	Homme	37	Marié
T.A.C.	Informaticien	Homme	29	Célibataire
M.M.K	Chauffeur	Homme	26	Célibataire
M.D.F.	Comptable	Femme	40	Divorcée
I.D.	Enseignant	Homme	34	Marié
A.S.	Commerçante	Femme	35	Mariée
A.K.	Informaticien	Homme	32	
N.N.F.	Assistante ressources humaines	Femme	28	Célibataire
K.D.	Etudiant	Homme	20	Célibataire
A.S.	Gérante d'un magasin multiservices	Femme	30	Mariée
A.N.	Etudiante	Femme	33	Célibataire
A.D.	Retraité	Homme	68	Marié

3.1.4.3.2. L'enquête par observation

L'observation est une technique de recherche utilisée en sciences sociales qui permet au chercheur, soit à travers une implication directe à son milieu d'étude soit de façon indirecte, de dégager les particularités, les dynamiques, la structuration entre autres de son milieu et de sa population d'étude.

Pour une problématique telle que la cybercriminalité dans les réseaux sociaux, l'observation est facilitée par le fait qu'en tant que chercheur, nous sommes à la fois sujet et objet de chercheur. En tant qu'utilisateur des réseaux sociaux, nous faisons d'ores et déjà partie de ce système social. Donc, il ne nous reste plus qu'à surfer dans différents réseaux sociaux et comptes d'utilisateurs.

Immersion faite, nous avons remarqué que dans plusieurs réseaux sociaux, certains utilisateurs évoquaient leurs expériences face aux cybercriminels ; tandis qu'au niveau d'autres comptes d'utilisateurs, c'est eux-mêmes qui divulguent les données à caractère personnel de ce que l'on peut appeler les victimes. Pour cette étape d'observation, nous avons utilisé une grille d'observation. Cette dernière concernait essentiellement les formes, les causes, les représentations sociales, les réactions sociales et les répercussions de la cybercriminalité dans les réseaux sociaux au Sénégal.

Tableau 9 : Récapitulatif de la phase d'observation

Réseaux sociaux	Objets d'observation	Durée d'observation
WhatsApp Instagram Facebook Tiktok YouTube X (ex Twitter)	Formes Représentations sociales Réactions sociales Les répercussions sociales	Juin 2022-Mars 2024

3.1.4.3.3. L'enquête par récit de vie

L'utilisation des récits de vie en tant que technique de collecte de données qualitatives nous permet à travers les expériences de nos enquêtés de comprendre notre problématique de recherche. Dans le cadre de notre étude sur la cybercriminalité dans les réseaux sociaux, les récits de vie sont utilisés pour recueillir les expériences des victimes de cette forme de criminalité. Ces dernières nous permettent dans une certaine mesure de comprendre les

motivations des cybercriminels, leurs procédés, d'avoir un aperçu sur certains cybercrimes et pourquoi certains utilisateurs de réseaux sociaux tombent dans les pièges des cybercriminels. Les récits de vie ont concerné principalement les victimes de cybercriminalité dans les réseaux sociaux. De ce fait, nous avons recueilli trois (3) récits de vie. L'un des récits de vie est un cas de sextorsion. Tandis que les deux autres sont des cas d'escroqueries à travers les systèmes pyramidaux.

3.2.1. Le traitement de données

Le traitement et l'analyse de données d'enquête obéissent à un ensemble de procédés et de techniques. Ces derniers permettent au chercheur d'établir en cadre référentiel par lequel traiter et analyser ses données. Cela peut se faire par le biais de différentes techniques.

Pour ce qui est de cette étude sur la cybercriminalité dans les réseaux sociaux, nous avons choisi, après une classification des données qui a été facilitée par la subdivision de notre recherche en thématique, d'utiliser deux techniques de traitement de données.

3.2.1.1. Le traitement de données qualitatives

Le traitement de données qualitatives suppose un repérage et une sélection des éléments significatifs issus des données empiriques. Autrement dit, c'est une technique qui permet au chercheur de repérer, de trier et de classer les informations en différentes catégories. Le traitement de données permet aussi la mise en relation des éléments de réponses des enquêtés afin d'en dégager des unités de sens ou explicatives de notre problématique de recherche.

Puisque le traitement de données suppose un tri et une classification des données en différentes catégories, nous avons procédé à une catégorisation des informations recueillies en fonction de nos thématiques prédéfinies lors de l'élaboration de nos guides d'entretien et des nouvelles unités de sens apparues après l'exploitation des données.

3.2.1.2. Le traitement de données quantitatives

Pour ce qui est des informations émanant de notre questionnaire de recherche, le traitement s'est fait sur la base des variables sociodémographiques pour dégager des tendances sur les profils des victimes, leurs réactions etc. Le traitement des données quantitatives implique au préalable de détecter et de corriger les erreurs, de gérer les valeurs manquantes et de s'assurer de la cohérence des données.

3.2.2. Les méthodes et techniques d'analyse de données

L'analyse des données est un processus qui consiste à organiser, à catégoriser et à interpréter les informations recueillies sur le terrain afin d'en tirer des explications sur le fait social étudié. Elle permet de tirer des conclusions sur notre étude et de répondre à nos différentes questions.

3.2.2.1. Les données quantitatives : l'analyse statistique

Cette technique est utilisée dans le cadre d'une analyse de données émanant généralement d'un questionnaire d'enquête. Ce type d'analyse est important dans la mesure où elle s'inscrit dans une perspective de mise en relation des variables établies par le chercheur avec son questionnaire de recherche.

L'objectif de cette technique d'analyse est de nous permettre en tant que chercheur de dégager des modèles et des tendances sur notre problématique de recherche. Nous obtenons nécessairement ces derniers à la suite de corrélations entre les variables sociodémographiques, d'usages de réseaux sociaux, de fréquence d'utilisation entre autres avec le fait d'être victime de cybercriminalité dans les réseaux sociaux.

Pour établir la corrélation entre ces variables, nous allons utiliser le test de Pearson qui permet de mesurer la relation linéaire entre deux variables continues. Ce qui nous permet de savoir si la relation entre la probabilité d'être victime de cybercriminalité dans les réseaux sociaux et les variables citées précédemment est significative au point d'en déduire une relation de cause à effet. C'est ainsi que nous avons utilisé le logiciel SPSS pour le traitement et l'analyse des données issues des questionnaires administrés à notre échantillon d'étude.

3.2.2.2. Les données qualitatives : l'analyse de contenu

L'analyse de contenu est une technique d'analyse de données très souvent utilisée en sciences sociales. Laurence Bardin la définit comme étant « *un ensemble d'instruments méthodologiques de plus en plus raffinés et en constante amélioration s'appliquant à des discours (contenu et contenant) extrêmement diversifiés. Le facteur commun de ces techniques multiples et multipliées (…) est herméneutique, contrôlé, fondé sur la déduction et l'inférence. En tant qu'effort d'interprétation, l'analyse de contenu se balance entre les deux pôles de la rigueur de l'objectivité et de la fécondité subjective* ». (Bardin, 1977)

L'analyse de contenu se fait essentiellement à travers une catégorisation des données recueillies en des unités de sens ou thématiques prédéterminées ou construites à postériori par le chercheur.

Pour ce qui est de notre problématique de recherche, à savoir la cybercriminalité dans les réseaux sociaux, nous avons entrepris d'exploiter un ensemble de documents, allant d'une importante webographie, à une filmographie, aux rapports des services en charge de la cybercriminalité et de la cybersécurité au Sénégal. L'exploitation de cette webographie et cette filmographie concerne de manière générale l'ensemble des contenus auquel nous avons eu accès et qui se rapporte à la cybercriminalité ou à la technologie numérique dans son ensemble. A cela s'ajoute l'exploitation des différents entretiens que nous avons effectué.

3.2. Les difficultés rencontrées

Il est difficile de faire un travail de recherche scientifique qui soit exempt des difficultés. Aussi minimes soient-elles, mais elles font partie de la recherche et le chercheur est amené à les dépasser dans la mesure du possible.

La première difficulté, à laquelle nous avons été confronté, a été l'accès aux différents services en charge de la cybercriminalité au Sénégal. Cela est dû au fait que l'enquête s'est déroulée durant une période d'instabilité et que cette situation ne permettait non seulement pas d'aller sur le terrain, mais aussi ces services étaient plus focalisés sur la maitrise de cette période de troubles. A cela s'ajoute, les lenteurs sur la programmation de rencontres pour les entretiens avec les agents des différents services.

Hormis cela, nous avons été confronté à des difficultés d'accès aux données statistiques de la plateforme numérique de lutte contre la cybercriminalité (PNLC). La raison évoquée a été que ces données sont confidentielles. Cependant, pour palier à ce contretemps, nous avons effectué des entretiens au niveau de la plateforme numérique de lutte contre la cybercriminalité (PNLC) dans le but d'obtenir les données essentielles pour cette étude.

3.3. Les limites de l'étude

Il est quasiment impossible de faire une étude scientifique sans que celle-ci n'ait ou ne présente des limites. Celles-ci sont le propre même de la recherche, parce qu'en aucun cas, elle ne peut être parfaite. Ce sont d'ailleurs ces limites qui vont nécessairement se présenter en des perspectives pour des recherches futures.

Nous pouvons d'ores et déjà parler de l'absence d'entrevue avec des individus catégorisés comme cybercriminels. Même si nos enquêtes nous ont permis d'avoir ces données et que par nos observations, il nous a été donné d'en observer certains, il aurait été intéressant de s'entretenir avec eux pour parler de leurs motivations.

Nous avons aussi le fait de ne pas présenter des statistiques exhaustives non seulement sur l'état de la cybercriminalité au Sénégal, mais en termes de vulnérabilités basées sur le genre. Cela est dû au fait qu'il n'y a pas une centralisation des statistiques sur la cybercriminalité.

Deuxième partie : Analyses et interprétations des résultats

L'analyse et l'interprétation des résultats constituent cette étape de la recherche qui permet au chercheur de répondre à ses différentes questions de recherche. Cette partie de la recherche est exécutée sous forme de thématiques prédéfinies dans l'élaboration des outils de collecte de données ou ressortant à l'issu des enquêtes de terrain. Les techniques d'analyse et de traitement de données, telles que l'analyse de contenu et l'analyse statistique nous permettent de dégager les éléments constitutifs des thématiques abordées. Ainsi, pour cette recherche, nous allons aborder huit (8) thématiques que nous avons regroupé en cinq (5) chapitres.

Le premier chapitre de cette partie fait état des caractéristiques de la population d'étude. Dans le deuxième chapitre, nous abordons la situation de la cybercriminalité au Sénégal.

Dans le troisième chapitre, qui constitue un des points phares de notre étude, nous esquissons les différentes formes des cybercrimes que nous retrouvons dans les réseaux sociaux au Sénégal. Esquisser celles-ci, nous amène à une compréhension des facteurs explicatifs de la cybercriminalité dans les réseaux sociaux à Sénégal. Ce qui nous amène à traiter dans le quatrième chapitre les facteurs explicatifs de la cybercriminalité dans les réseaux sociaux au Sénégal, ainsi que les profils des cybercriminels et des victimes.

Dans le cinquième chapitre, est fait l'esquisse des représentations sociales, des réactions sociales et des répercussions de la cybercriminalité dans les réseaux.

Chapitre 4 : Caractéristiques de la population d'étude

Avec le questionnaire de recherche, nous procédons à une caractérisation de l'échantillon d'étude. Celle-ci permet au chercheur de faire une corrélation entre les différentes variables caractéristiques de l'échantillon. La corrélation des variables, à son tour, permet au chercheur de dégager des tendances sous la base de statistiques pour comprendre son objet d'étude.

4.1. Répartition de la population en fonction du sexe

L'usage des réseaux sociaux n'est pas spécifique à un sexe. C'est pourquoi, l'échantillon doit être représentatif pour les deux sexes. Cela peut permettre de dégager des tendances sur la catégorie la plus vulnérable face à chaque forme de cybercriminalité dans les réseaux sociaux.

L'échantillon pour l'étude de la cybercriminalité dans les réseaux sociaux au Sénégal sous l'approche quantitative a été structurée en fonction du sexe de sorte à mettre en évidence une représentativité significative des hommes et des femmes. C'est la raison pour laquelle parmi les cent (100) individus à qui nous avons soumis notre questionnaire de recherche, cinquante-quatre (54) sont des hommes et les quarante-six (46) restants représentent les femmes.

Graphique 1 : Répartition de l'échantillon en fonction du sexe des enquêtés

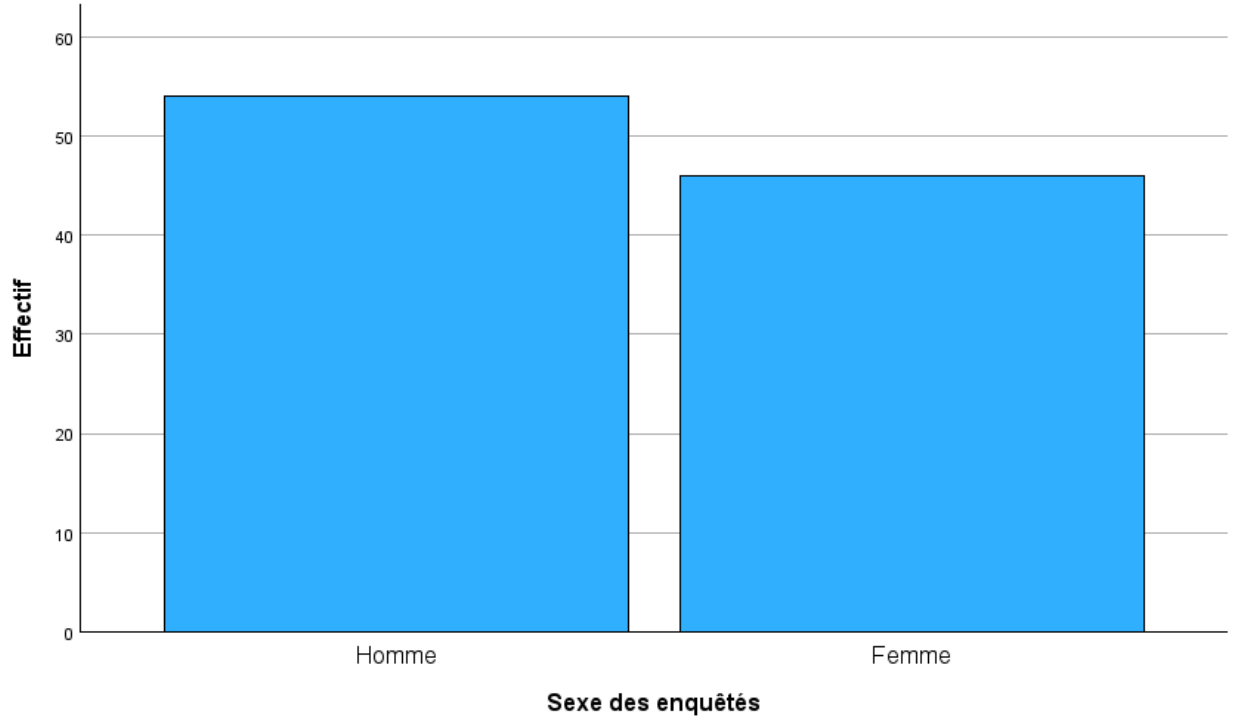


Tableau 10 : Tableau croisé entre le sexe des enquêtés et le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux

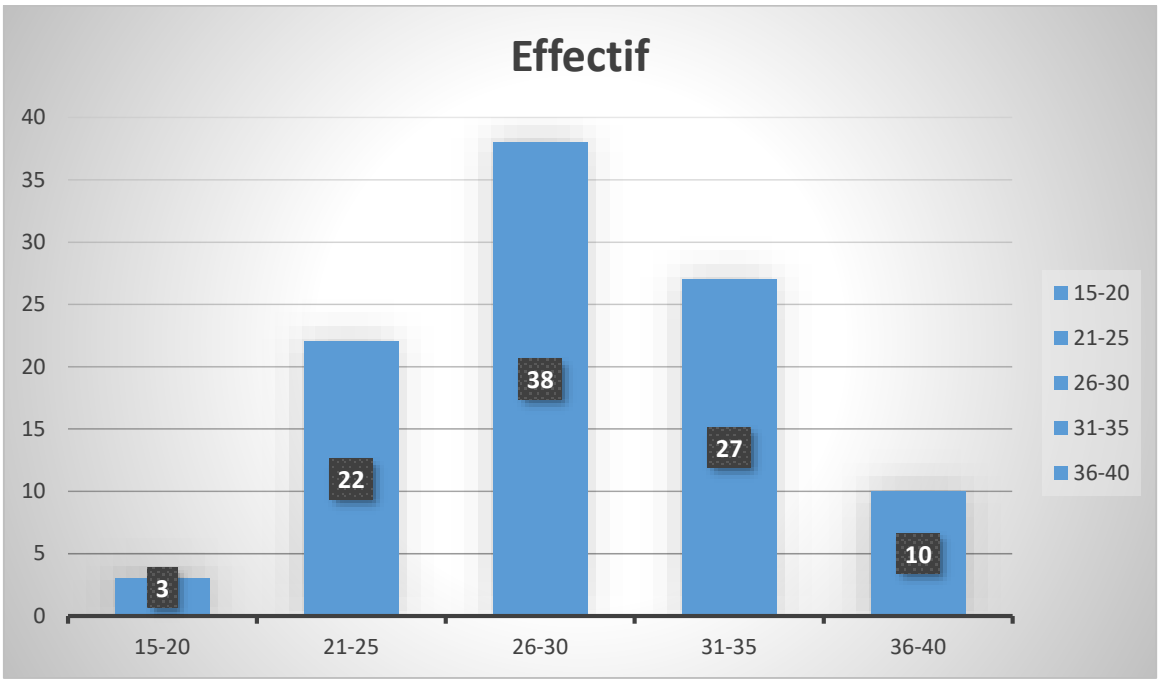
		Etre victime ou non de cybercriminalité dans les RS		
Effectif		Oui	Non	Total
Sexe des enquêtés	Homme	24	30	54
	Femme	14	32	46
Total		38	62	100

Les résultats obtenus à la suite de l'exploitation des données de terrain montrent que parmi les trente-huit (38) victimes de cybercriminalité dans les réseaux sociaux parmi nos enquêtés, vingt-cinq (24) sont des hommes et que les quatorze (14) autres représentent les femmes.

4.2. Répartition de l'échantillon selon l'âge

Comme technologies, les réseaux sociaux sont utilisés par quasiment toutes les classes d'âge. Cependant, pour cette étude, nous avons essentiellement mis la focale sur un échantillon d'individus ayant un âge compris entre quinze (15) et quarante (40) ans. Ce qui représente une population assez jeune.

Graphique 2 : Répartition de l'échantillon en fonction de l'âge des enquêtés



Source : enquête de terrain Diouf Septembre 2023

Sur un échantillon de cent (100) individus, nous avons enquêté trois (3) qui sont âgés entre 15-20 ans, vingt-deux (22) âgés de 21-25 ans, trente-huit (38) âgés de 26-30 ans, vingt-sept (27) âgés de 31-35 ans et dix (10) âgés de 36-40 ans. Cependant, l'âge moyen des enquêtés est 29 ans.

Tableau 11 : Tableau croisé entre l'âge des enquêtés et le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux

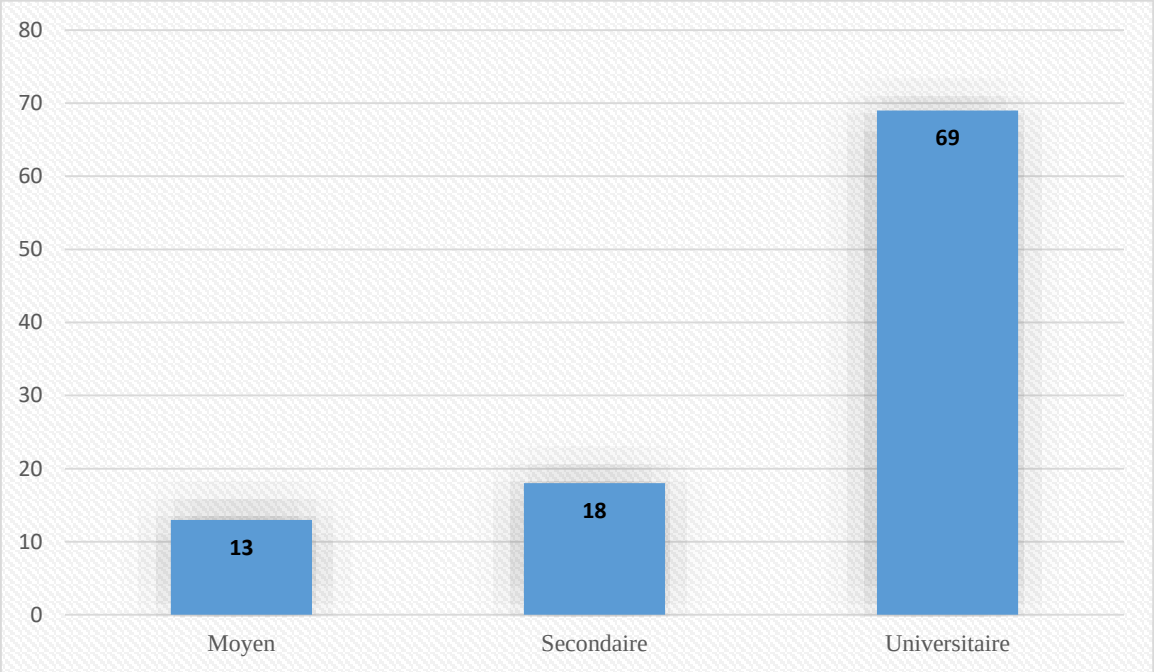
		Etre victime ou non de cybercriminalité dans les RS		
Effectif		Oui	Non	Total
Age des enquêtés	15-20	0	3	3
	21-25	7	15	22
	26-30	12	26	38
	31-35	12	15	27
	36-40	7	3	10
Total		38	62	100

Ces statistiques sur la répartition des victimes selon l'âge nous montrent que tous les utilisateurs des réseaux sociaux peuvent être victime de cybercriminalité. Cependant, il est clair que les jeunes sont plus victimes de cybercriminalité dans les réseaux sociaux parce qu'ils constituent la majorité des utilisateurs de ces technologies. Comme présenté par ces statistiques, les victimes de cybercriminalité dans les réseaux sociaux parmi les individus de l'échantillon ont un âge compris entre 21 et 40 ans. Ceci étant dit, les effectifs deux (2) classes d'âges 26-30 ans et 31-35 ans sont majoritairement plus élevés. Chacune de ces deux classes est représentée par douze (12) victimes parmi les trente-huit victimes de notre échantillon d'étude. Nous avons, parmi nos vingt-deux (22) enquêtés âgés de 21-25 ans sept (7) qui sont victimes de cybercriminalité dans les réseaux sociaux. Parmi nos dix (10) enquêtés âgés de 36-40 ans sept (7) d'entre eux ont été victimes de cybercriminalité dans les réseaux sociaux.

4.3. Répartition de l'échantillon en fonction du niveau d'étude

Par rapport au niveau d'étude, nous avons un échantillon réparti comme suit : soixante-neuf (69) enquêtés ayant effectués un cursus universitaire, dix-huit (18) pour le niveau secondaire et treize (13) pour le niveau moyen.

Graphique 3 : Répartition de l'échantillon en fonction du niveau d'étude



Source : enquête de terrain Diouf Septembre 2023

Tableau 12 : Tableau croisé entre le niveau d'étude des enquêtés et le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux

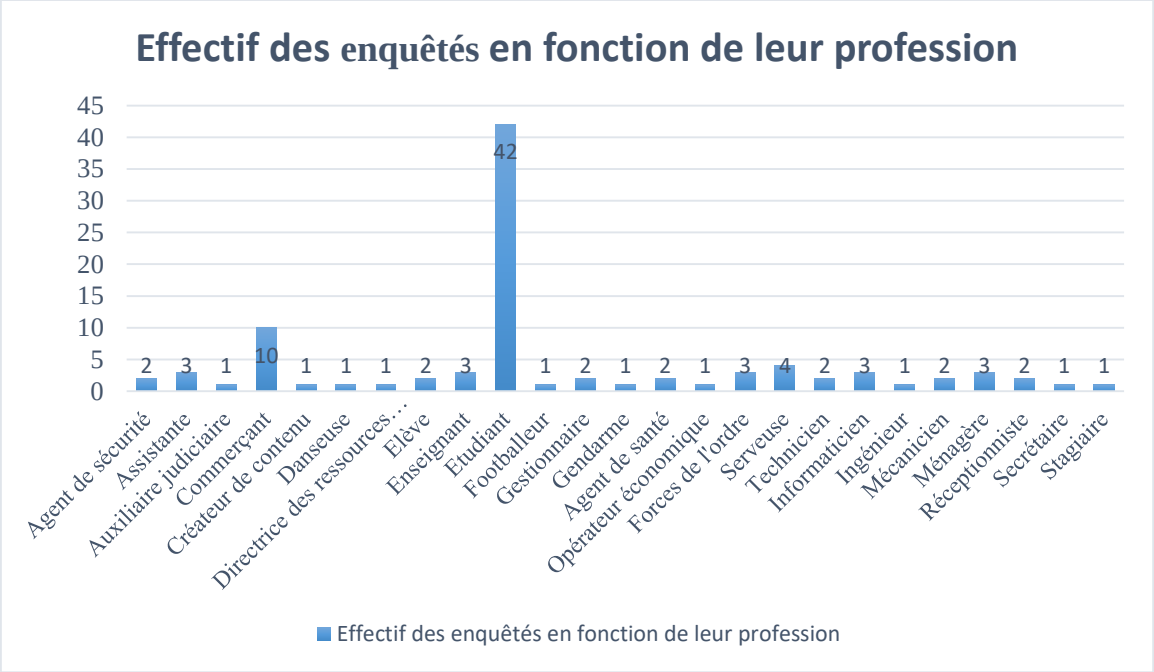
Effectif		Etre victime ou non de cybercriminalité dans les RS		
		Oui	Non	Total
Niveau d'étude des enquêtés	Moyen	5	9	14
	Secondaire	9	15	24
	Universitaire	24	38	62
Total		38	62	100

Ces résultats révèlent une prédominance des victimes avec un niveau d'étude supérieur (universitaire) avec vingt-quatre (24), soit 63,15% sur les trente-huit (38) victimes enquêtées. Parmi les victimes avec un niveau d'étude secondaire (lycée), neuf (9) ont été victimes de cybercriminalité dans les réseaux sociaux, soit 23,69%. De ce fait, les cinq (5) enquêtés restants à avoir été victimes de cybercriminalité dans les réseaux sociaux ont un niveau d'étude moyen (collège), soit 13,16%.

4.4. Répartition de la population en fonction de la profession

Pour des raisons de représentativité, nous avons pris en compte plusieurs catégories socioprofessionnelles. Cette approche s'explique par le fait que la cybercriminalité dans les réseaux sociaux est un fait social dont les victimes ne peuvent être rangées dans une ou deux catégories professionnelles. A travers ses différentes formes, la cybercriminalité dans les réseaux sociaux touchent pratiquement tous les secteurs d'activité et de la vie sociale et par conséquent tous les catégories socioprofessionnelles.

Graphique 4 : Répartition de l'échantillon d'étude en fonction de la profession des enquêtés

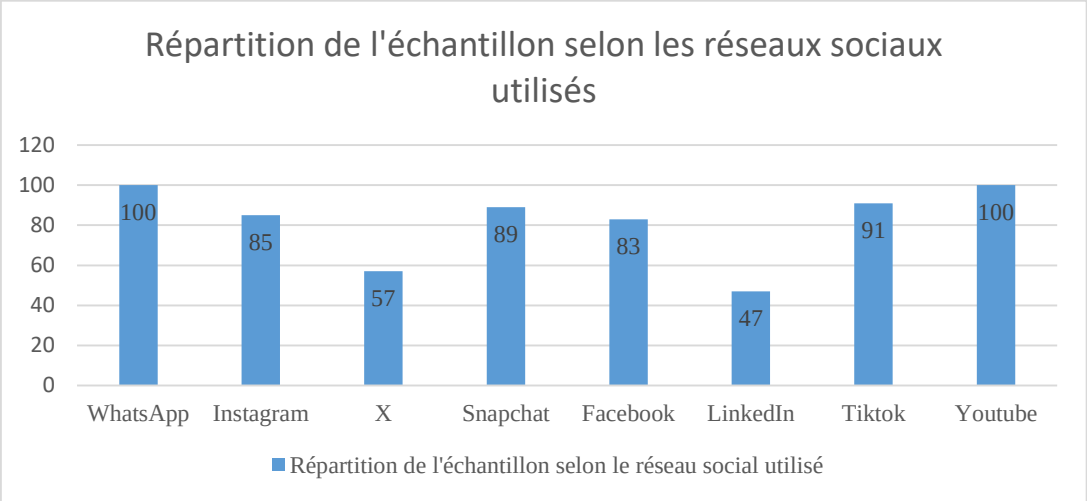


Source : enquête de terrain Diouf Septembre 2023

4.5. Répartition de l'échantillon selon les réseaux sociaux utilisés

Faire la répartition de l'échantillon en fonction des réseaux sociaux nous permet non seulement de savoir ceux qui sont les plus utilisés mais aussi de dégager une tendance sur le type de réseau social utilisé et le fait d'être victime de cybercriminalité.

Graphique 5 : Répartition de l'échantillon en fonction des réseaux sociaux utilisés



Ces statistiques nous montrent que l'ensemble de nos enquêtes utilise les réseaux sociaux WhatsApp et Youtube. Les autres réseaux sociaux, n'étant pas utilisés par tous, sont répartis selon notre échantillon comme suit : Instagram quatre-vingt-cinq (85) utilisateurs, X cinquante-sept (57) utilisateurs, Snapchat quatre-vingt-neuf (89) utilisateurs, Facebook quatre-vingt-trois (83), LinkedIn quarante-sept (47) utilisateurs et Tiktok quatre-vingt-onze (91). Le réseau social WhatsApp est sans doute le plus utilisé parce qu'il constitue le moyen de communication par essence sur avec l'apparition des groupes d'échanges générationnels, familiales, d'études, d'intérêt etc. Quant à Youtube, il est utilisé dans le cadre de visionnage de séries télévisées, de documentaires, matchs sportives ou de vidéos sur d'autres centres d'intérêt.

Tableau 13 : Tableau croisé entre le réseau social sur lequel l'enquêté a été victime et le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux

Effectif

		Etre victime ou non de cybercriminalité dans les RS		
		Oui	Non	Total
Réseau social sur lequel l'enquêté a été victime		0	62	62
	Facebook	8	0	8
	Instagram	9	0	9
	Snapchat	3	0	3
	Tiktok	4	0	4
	X	1	0	1
	WhatsApp	11	0	11
	Youtube	2	0	2
Total		38	62	100

Source : enquête de terrain Diouf Septembre 2023

Ces résultats font état des différents réseaux sociaux sur lesquels les individus de notre échantillon ont été victimes de cybercriminalité. Ces réseaux sociaux sont les plus utilisés dans le monde. Sur trente-huit (38) cas de cybercriminalité dans les réseaux sociaux, nous avons :

Onze (11) cybercrimes subis par nos enquêtés à travers le réseau social WhatsApp ;

Neuf (9) cybercrimes via le réseau social Instagram

Huit (8) cybercrimes sur le réseau social Facebook

Quatre (4) à travers le réseau social Tiktok

Trois (3) sur le réseau social Snapchat

Deux (2) via le réseau social Youtube

Un (1) via le réseau social X (Twitter)

Le fait que nous ayons plus de cybercrimes sur le réseau social WhatsApp est dû au fait que le cybercriminel a à sa portée une manne importante de cibles en mettant en place une arnaque plausible qui puisse être partagée dans les groupes de discussion que les utilisateurs du réseau social mettent en place. Comme ce fut le cas avec les arnaques de Tesco Boutique ou de Petronpay, dont la plupart des victimes en ont entendu parler via leurs groupes de discussion sur WhatsApp.

Tableau 14 : Tableau croisé entre le type de cybercrime et réseau social sur lequel l'enquêté a été victime

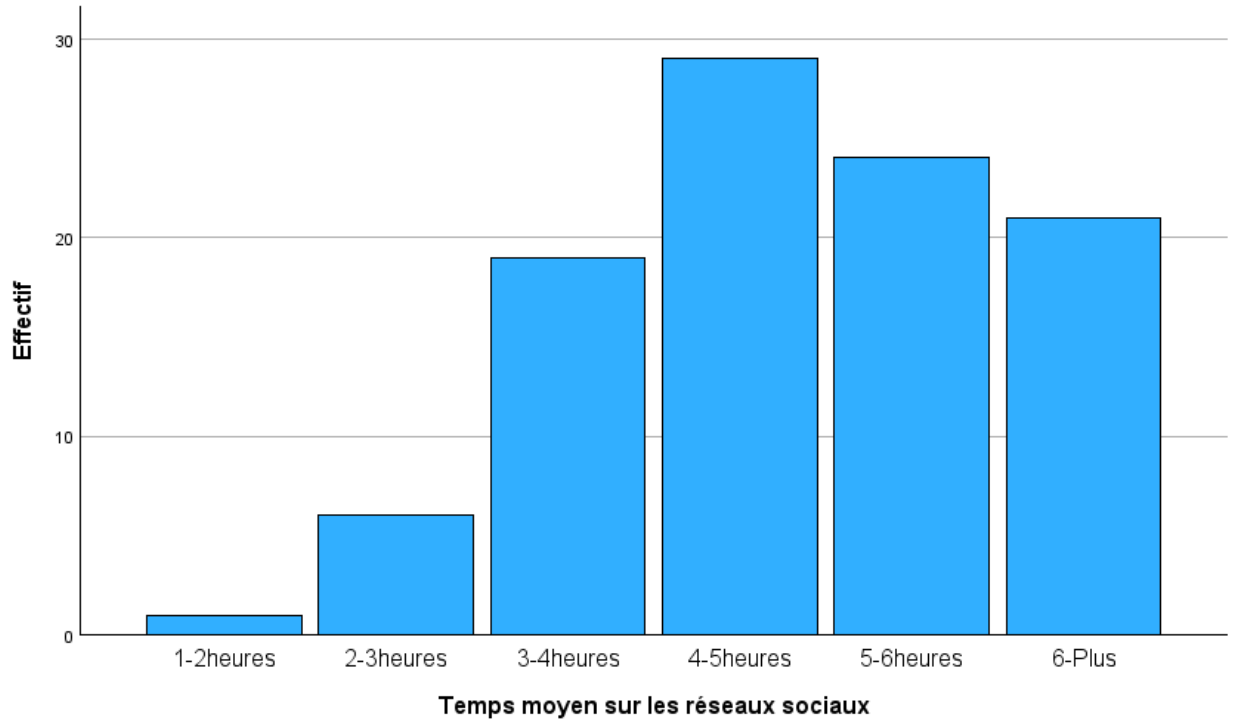
		Total	Facebook	Instagram	Snapchat	Tiktok	Twitter	WhatsApp	YouTube	
Genre de cybercrime dont l'enquêté est victime		62	0	0	0	0	0	0	0	62
	Atteinte à l'image	0	1	2	0	2	0	0	0	5
	Cyber-harcèlement	0	0	2	0	0	1	0	0	3
	Diffusion d'images pornographiques	0	1	0	3	2	0	2	2	10
	Escroquerie	0	2	0	0	0	0	6	0	8
	Piratage	0	4	2	0	0	0	0	0	6
	Sextorsion	0	0	3	0	0	0	3	0	6
Total		62	8	9	3	4	1	11	2	100

Source : Enquête de terrain Diouf septembre 2023

4.6. Répartition de l'échantillon en fonction du temps moyen par jour sur les réseaux sociaux

Même si le temps moyen de connexion est utilisé comme corolaire dans l'explication de la cybercriminalité, ce n'est pas pour autant que celle-ci est plausible. Il est plus pertinent de dire qu'il est plus probable d'interagir avec un cybercriminel mais cela ne fait pas de ces personnes plus sujets à être victimes de cybercriminalité dans les réseaux sociaux.

Graphique 6 : Répartition de l'échantillon en fonction du temps moyen sur les réseaux sociaux (par semaine)



Source : enquête de terrain Diouf Septembre 2023

Ces résultats sur le temps moyen que nos enquêtés passent sur les réseaux sociaux en fonction du fait d'être victime de cybercriminalité dans les réseaux sociaux montrent que parmi :

Sept (7) enquêtés qui passent 2 à 3 heures sur les réseaux sociaux deux (2) ont été victimes de cybercriminalité ;

Sur vingt-trois (23) enquêtés qui passent 3 à 4 heures sur les réseaux sociaux, cinq (5) ont été victimes de cybercriminalité ;

Sur trente enquêtés qui passent 4 à 5 heures les réseaux sociaux, huit (8) ont été victimes de cybercriminalité ;

Sur vingt-deux (22) enquêtés qui passent 5 à 6 heures sur les réseaux sociaux, quatorze (14) ont été victimes de cybercriminalité ;

Sur dix-sept enquêtés qui passent en moyenne 6 heures ou plus sur les réseaux sociaux, neuf (9) ont été victimes de cybercriminalité.

Tableau 15 : Corrélation entre le temps moyen sur les réseaux sociaux et le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux

		Etre victime ou non de cybercriminalité dans les RS	Temps moyen sur les réseaux sociaux
Etre victime ou non de cybercriminalité dans les RS	Corrélation de Pearson	1	-,300**
	Sig. (bilatérale)		,002
	N	100	100
Temps moyen sur les réseaux sociaux	Corrélation de Pearson	-,300**	1
	Sig. (bilatérale)	,002	
	N	100	100

La corrélation est significative au niveau 0.01.

La corrélation de Pearson entre le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux et le temps moyen passé sur les réseaux sociaux est de -0,300. Cette corrélation est statistiquement significative, ce qui indique une relation significative entre ces deux variables.

Une corrélation de -0,300 suggère une relation négative modérée entre ces deux variables. En d'autres termes, cela signifie que plus le temps passé sur les réseaux sociaux est élevé, moins il est probable d'être victime de cybercriminalité dans ces réseaux sociaux, et vice versa. Cependant, il est important de noter que la corrélation ne détermine pas de relation de cause à effet entre ces variables. Ce qui peut être déduit de la moyenne de temps passé sur les réseaux sociaux est la probabilité d'être confrontée à de la cybercriminalité. Parce que selon le

Lieutenant Niang de la plateforme numérique de lutte contre la cybercriminalité (homme 38 ans) « *ce qui peut sauver les usagers des réseaux sociaux est leur niveau de conscience et une bonne hygiène cyber* »

4.7. Répartition de l'échantillon sur les victimes de cybercriminalité dans les réseaux sociaux

Sur un échantillon de cent (100) personnes enquêtés, trente-huit (38) ont été victimes de cybercriminalité dans les réseaux sociaux. Ces victimes peuvent être catégorisées selon l'âge, le sexe, le niveau d'étude, la profession etc.

Graphique 7 : Répartition de l'échantillon en fonction du fait d'être victime ou non de cybercriminalité dans les réseaux sociaux

Source : enquête de terrain Diouf Septembre 2023

Chapitre 5 : Situation de la cybercriminalité au Sénégal

L'universalité d'internet fait de la cybercriminalité un phénomène mondial. Par conséquent, elle devient l'affaire de tous les États du monde subissant les progrès du numérique, particulièrement des technologies de l'information et de la communication. Le Sénégal comme toutes les nations du monde est confronté à la criminalité numérique.

De ce fait, elle s'est dotée d'un ensemble de lois qui s'inscrit dans une logique de lutte contre la cybercriminalité. Ces différentes lois sont venues renforcer le code de procédure pénal par lequel l'Etat du Sénégal se base pour identifier les différentes infractions, mais aussi les sanctions à considérer. Donc, les lois sur la cybercriminalité se sont inscrites dans cette même perspective en définissant et en catégorisant les différentes infractions cyber, pour enfin établir les différentes sanctions.

Parler de la situation de la cybercriminalité au Sénégal revient à faire une description exhaustive de la lutte contre ce phénomène en faisant un état des lieux sur le cadre juridique et institutionnel, les politiques publiques et l'efficacité de la lutte contre ce phénomène. Cela nous permet de savoir ce qui se fait en matière de lutte contre la cybercriminalité au Sénégal et comment elle se fait. Pour se faire, le recueil de données auprès des services de cybersécurité et de lutte contre la criminalité sur internet est primordial.

Tableau16 : Les acteurs de la cybercriminalité au Sénégal

Acteurs	Caractéristiques	Enjeux	Atouts	Handicaps	Stratégies
Cybercriminels	Expertise	Satisfaction personnelle	Techniques d'anonymisation Ingénierie sociale	La sophistication moyens et techniques d'identification L'empreinte numérique	Création de faux compte Utilisation de VPN pour masquer sa position L'ingénierie sociale
Forces de défense et de sécurité (DSC, PNLC, CDP)	Statut, Expertise et Légitimité	Maintien du sentiment de sécurité Protéger les personnes et les biens	Dispositifs de pistage des activités numériques suspectes	L'anonymat des cybercriminels	Cyber surveillance Veille numérique
Les ministères (intérieur, forces armées, justice, télécommunications)	Statut, Expertise et Légitimité	Sécurité des personnes et de leurs biens Respect des lois et règlements en vigueur Un cyberespace sûr	Ressources pour surveiller et traquer les malfaiteurs	L'anonymat des cybercriminels	Durcir la cyber-surveillance et les sanctions Renforcements techniques et dispositifs de lutte contre la cybercriminalité
Les Juges	Légitimité et expertise du fait des textes juridiques	Justice et sécurité sociale	La cyber-législation	Manque de preuves matérielles du fait de l'immatérialité du crime	Intransigeance dans l'application de la loi et de la répression
Les victimes	Pas ou très peu expertise La peur, l'inconfort	La réputation, les biens personnels, la sécurité	Protection en cybersécurité Avoir une bonne hygiène cyber	Manque de connaissance en cyber sécurité La tentation ou la crédulité	Prudence Utilisation de logiciels de protection Avoir une culture de dénonciation Connaissances en cybersécurité
Utilisateurs des réseaux sociaux	Peu ou pas d'expertise pour une partie Sentiment d'insécurité	La sécurité physique et de propriété	Protection en cybersécurité Bonne hygiène cyber Prudence	Failles de l'internet La tentation	Faire une formation en cyber sécurité Prudence Utilisation de logiciels de protection

Ce tableau est une manifestation du jeu de pouvoirs des acteurs de la cybercriminalité au Sénégal. Ces acteurs, à travers leurs pouvoirs, essaient d'exercer leur autorité pour maitriser leur environnement. Dans ce cas de figure, l'environnement est le cyberespace. Les autorités étatiques sont dans une perspective de maitrise et de mise en place d'un cyberespace sûr et confiant permettant aux différents utilisateurs de surfer en toute sécurité. Cependant, il y a un groupe d'individus dont l'atteinte des besoins et la réalisation des aspirations se heurtent à la perspective des autorités étatiques. Ce qui fait que chaque acteur ou groupe d'acteurs va mettre en place un ensemble de stratégies lui permettant d'atteindre ses objectifs. Les autorités étatiques (ministères et services spécialisés dans la cybersécurité et la lutte contre la cybercriminalité), investis de légitimité juridique mettent en place des lois et politiques allant dans le sens de sécuriser le cyberespace sont confrontés aux cybercriminels qui jouissent des avantages technologiques, combiné à l'ingénierie sociale.

5.1. Dispositifs de lutte contre la cybercriminalité au Sénégal

Comprenant les dangers que représente la cybercriminalité et surtout les enjeux que pose la cybersécurité, les États ont procédé à l'adoption de plusieurs lois visant à lutter contre les exactions commises à travers les technologies de l'information et de la communication.

Le Sénégal s'est inscrit dans cette dynamique en mettant en place non seulement une législation pour la réglementation de l'usage des technologies de l'information et de la communication, mais aussi d'un appareil institutionnel pour la promotion de la cybersécurité et pour la lutte contre la cybercriminalité.

5.1.1. Le cadre législatif national

Au niveau national, le Sénégal s'est doté d'un cadre juridique presque intégral ; pas seulement de lutte contre la cybercriminalité, mais d'encadrement des phénomènes qui touchent la société de l'information.

5.1.1.1. Loi n°2008-08 du 25 Janvier 2008 portant sur les transactions électroniques

Cette loi portant sur les transactions électroniques s'inscrit, de façon globale, dans la perspective à favoriser le développement du commerce par les technologies de l'information et de la communication en posant les bases.

La transaction électronique est définie, à travers cette loi, comme étant « *tout ce qui porte sur la production, la promotion, la vente, la distribution des produits et les échanges par les réseaux de télécommunications et informatiques* ».

La visée de cette loi est d'assurer la sécurité et le cadre juridique nécessaires à l'émergence d'un commerce électronique fiable au Sénégal. Une définition claire du commerce en ligne a été établie dans le but de définir le champ d'application de la présente loi.

Le commerce en ligne y est abordé comme étant « *l'activité économique par laquelle une personne propose ou assure, à distance et par voie électronique, la fourniture des biens et la prestation de service* »[25].

Par extension, le commerce en ligne concerne aussi « *les services tels que ceux consistant à fournir des informations en ligne, des communications commerciales, des outils de recherche, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations même s'ils ne sont pas rémunérés par ce qui les reçoivent* »[26].

5.1.1.2. Loi n°2008-10 du 25 Janvier portant sur loi d'orientation sur la société de l'information

Le sommet mondial de la société de l'information (SMSI), lancé par l'organisation des nations unies (ONU) en 2003, a permis l'élaboration de la loi d'orientation sur la société de l'information. Ce sommet avait pour objectif :

> De déterminer une stratégie commune pour faciliter l'utilisation des technologies de l'information et de la communication (TIC) afin que le bénéfice puisse rejaillir sur la prospérité économique, le développement des savoirs, le renforcement de la paix et la promotion de la démocratie ; de réduire la fracture numérique par une promotion massive de l'utilisation des technologies de l'information et de la communication (TIC) par les couches les plus défavorisées de la population.[27]

C'est pourquoi l'instauration d'une législation qui s'inscrivait dans la même perspective que le sommet mondial de la société de l'information était plus qu'évidente. Mise au point en 2008, la loi d'orientation sur la société de l'information (LOSI) se veut de :

- Définir les grands objectifs et orientations de la société de l'information au Sénégal et compléter la législation actuelle en matière de technologies de l'information et de la communication (TIC)

[25] Loi n°2008-08 du 25 Janvier 2008 portant sur les transactions électroniques
[26] *Ibid.*
[27] Loi n°2008-10 du 25 Janvier portant sur loi d'orientation sur la société de l'information

- ❖ Définir un cadre général axé essentiellement sur la liberté, la sécurité et la solidarité, ainsi que tous les autres principes fondamentaux complémentaires à la société sénégalaise de l'information (SSI)
- ❖ Identifier les droits, rôles et responsabilités des divers acteurs (Etat, société civile, secteur privé, individu) et proposer des mesures incitatives minimales

Ces différents objectifs tendent à la mise place d'un cadre propice à l'utilisation des technologies de l'information et de la communication (TIC).

En son principe n°5, la loi d'orientation sur la société de l'information établit la collaboration entre les acteurs nationaux, régionaux et internationaux pour la mise en œuvre d'une politique de coopération judiciaire et sécuritaire orientée vers la sécurité des personnes et des ressources de la société de l'information et la lutte contre la cybercriminalité.

Au chapitre 5 de la présente loi qui aborde les droits, rôles et responsabilités des acteurs, en son article 9 est mis en avant la prise de mesures appropriées, notamment préventives pour promouvoir la paix et pour empêcher les utilisations abusives des technologies de l'information et de la communication.

5.1.1.3. Loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité

Celle-ci traite d'une part, des infractions spécifiques aux Technologies de l'information et de la communication, de l'adaptation de certaines incriminations et de certaines sanctions aux technologies de l'information et de la communication et d'autre part, de l'aménagement de la procédure classique par rapport aux technologies de l'information et de la communication et de l'adoption d'une procédure spécifique aux infractions liées aux données à caractère personnel.

Cette loi prévoit d'incriminer tous les comportements cybercriminels, qu'ils aient pour objets ou pour moyens les technologies de l'information et de la communication (TIC). Elle prévoit aussi les pouvoirs des autorités judiciaires, des magistrats, des officiers de police judiciaire, si bien qu'aujourd'hui, un officier de police judiciaire peut perquisitionner un système informatique, fouiller un système ou un serveur pour y rechercher des données utiles à l'enquête. Il en est de même pour un juge d'instruction. Celui-ci peut également intercepter des données informatiques.

5.1.1.4. Loi n°2008-12 du 25 Janvier 2008 portant sur la protection des données à caractère personnel

Cette loi a vu le jour quand les données à caractère personnel se sont révélées très convoitées. C'est la raison pour laquelle « *leur traitement doit se dérouler dans le respect des droits et libertés fondamentales, de la dignité des personnes physiques* »[28].

La loi sur la protection des données à caractère personnel a pour base les principes directeurs de la réglementation des fichiers informatisés contenant des données à caractère personnel édictés par l'Assemblée Générale de l'organisation des nations unies (ONU) en 1990, les exigences européennes en matière de transfert de données vers des pays tiers et les principes fondamentaux consacrés par la loi d'orientation sur la société de l'information. Elle a l'ambition de combler le vide juridique en matière de protection des données à caractère personnel. Et par là, elle a institué une autorité administrative indépendante dénommée la commission de protection des données personnelles (CDP), qui a pour rôle de réglementer le traitement des données personnelles.

A travers cette autorité administrative, la loi sur la protection des données à caractère personnel met en place un dispositif de lutte contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel. Par extension, elle garantit le respect des libertés et droits fondamentaux des personnes pour tout traitement de données à caractère personnel.

5.1.2. Cadre institutionnel

L'élaboration d'une législation adéquate aux technologies de l'information et de la communication a lancé la création d'institutions de lutte contre la cybercriminalité. Ses institutions, dans leurs prérogatives, se sont inscrites non seulement dans la lutte contre les infractions numériques, mais aussi dans la connaissance et la maitrise de celles-ci. Par extension, l'Etat du Sénégal, à travers ses différentes législations et institutions en la matière, s'est lancé dans la mise en place de politiques de cybersécurité efficaces et efficientes.

5.1.2.1. La commission de protection des données personnelles (CDP)

La Commission de protection des données personnelles (CDP) est une autorité administrative indépendante instituée par la loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel. Elle est chargée de vérifier la légalité de la collecte et du

[28] Loi n°2008-12 du 25 Janvier 2008 portant sur la protection des données à caractère personnel

traitement des données personnelles des sénégalais et de s'assurer que toutes les précautions sont prises pour qu'elles soient sécurisées. Elle est composée de onze (11) membres choisis en raison de leurs compétences juridiques et/ou techniques :

- Trois (3) membres désignés par le président de la République
- Un commissaire du gouvernement qui est désigné par le Premier ministre
- Un (1) député désigné par le Président de l'Assemblée nationale
- Deux (2) membres de la Cour suprême
- Un membre de l'ordre des avocats
- Un membre de l'organisation de défense des droits de l'homme
- Le directeur général de Sénégal Numérique (SENUM) ex ADIE (agence de l'informatique de l'État
- Un membre du patronat

Leur mandat est de quatre (4) ans renouvelables une fois.

La commission de protection des données personnelles (CDP) dispose d'un budget autonome dont les fonds sont alloués par le ministère de l'économie et des finances

Elle est investie de trois (3) principales missions :

- Une mission de veille, de sensibilisation, de conseils et de propositions :

La commission de protection des données personnes veille à ce que les traitements de données s'effectuent conformément à la loi sur la protection des données à caractère personnel.

Elle conseille les personnes et les organismes qui ont recours aux traitements des données à caractère personnel, met à la disposition du gouvernement toute suggestion susceptible de simplifier ou d'améliorer le cadre législatif ou réglementaire sur le traitement des données à caractère personnel et sensibilise les personnes concernées et les responsables de traitements de données à caractère personnel de leurs droits et obligations.

- Une mission d'instruction de dossiers sur :

Les formalités préalables (déclarations et demandes d'autorisation) aux traitements de données à caractère personnel

Les réclamations, pétitions et plaintes relatives aux traitements des données à caractère personnel et elle informe les auteurs des suites données à celles-ci

L'autorisation des transferts transfrontaliers de données à caractère personnel

- ❖ Une mission de contrôle et d'investigation qui s'articule autour de :

Informer le procureur de la République des infractions dont elle a connaissance.

Charger ses membres ou agents de procéder à des vérifications sur tout traitement de données à caractère personnel et d'obtenir les copies de tout document utile à sa mission.

Prononcer si nécessaire des sanctions à l'encontre des responsables de traitement de données à caractère personnel[29].

5.1.2.2.La division spéciale de cybersécurité (DSC)

La division spéciale de cybersécurité, en remplacement de la brigade spéciale de lutte contre la cybercriminalité (BSLC), est un service d'expertise de la Police nationale. Elle est par conséquent sous l'autorité du Ministère de l'intérieur. Elle a été créée en 2013, mais ne sera autonome qu'en 2017. Son siège se trouve à la direction de la Police judiciaire (DPJ).

En tant que service d'expertise en matière de cybersécurité et de lutte contre la cybercriminalité, la division spéciale de cybersécurité (DSC) a pour missions de :

- ❖ Recueillir des renseignements judiciaires pour les enquêtes impliquant les technologies de l'information et de la communication
- ❖ Procéder une veille opérationnelle pour suivre les tendances cybercriminelles
- ❖ Enquête et de répression de la cybercriminalité
- ❖ Assistance technique auprès des commissariats et aux autres divisions

5.1.2.3.La plateforme numérique de lutte contre la cybercriminalité (PNLC) 2016

La plateforme numérique de lutte contre la cybercriminalité est un pôle d'expertise numérique de la gendarmerie nationale. Elle est sous l'autorité du ministère des forces armées. En tant que service d'investigation, elle est chargée de conduire des enquêtes judiciaires et de recueillir des renseignements criminels.

Dans le cadre de l'exécution de ses missions, elle effectue une veille opérationnelle pour suivre les tendances en matière de cybercriminalité, en identifiant les différentes familles d'infractions cybercriminelles que l'on rencontre le plus souvent au Sénégal et en Afrique. Au-delà de ces missions, la plateforme numérique de lutte contre la cybercriminalité s'attèle à déceler les

[29] *Source : Entretiens avec le Commissaire Kandé de Division spéciale de cybersécurité (DSC) et avec le Lieutenant Ndour de la direction de la police judiciaire (DPJ)*

modes opératoires émergentes et la typologie des auteurs et des victimes. Cependant, les victimes ne peuvent y déposer directement plaintes. Elles peuvent le faire au niveau des brigades territoriales, qui à leur tour transmettent à la plateforme numérique pour les besoins d'enquête.[30]

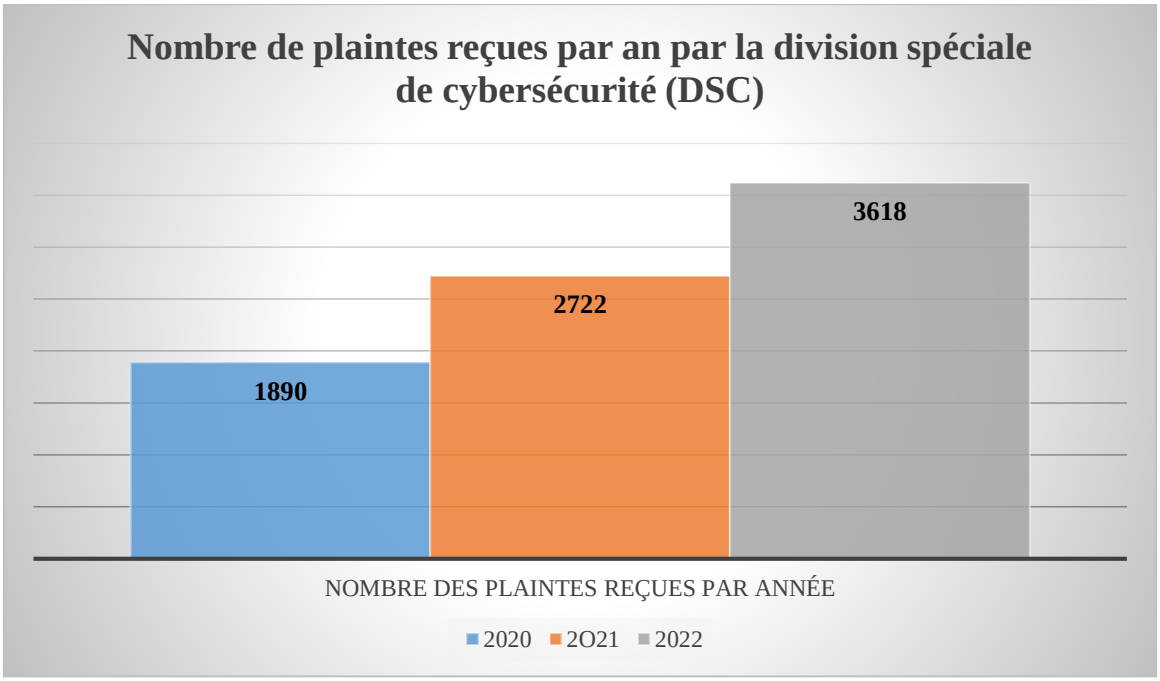
5.2.Statistiques sur la cybercriminalité au Sénégal

Les statistiques sur la cybercriminalité nous permettent de saisir l'ampleur du phénomène et nous rendent compte de l'efficacité de la lutte contre la criminalité sur internet. Ces statistiques concernent les plaintes reçues par les services en charge de cybercriminalité et les déferrements de cybercriminels. Toutefois, les données sur les plaintes et les signalements de cas de cybercriminalité enregistrés sont loin de décrire la réalité sur l'ampleur de cette criminalité. En réalité, une manne importante de cybercrimes non rapportés aux autorités est à prendre en compte. D'ailleurs, lors de l'entretien, Kandé (Homme, Commissaire à la DSC) souligne que « *40 à 60% des victimes de cybercriminalité dans les réseaux sociaux ne portent pas plainte à cause des menaces de divulgation de données personnelles* ». Même si les statistiques sur la cybercriminalité au Sénégal semblent impressionnantes, il se trouve Niang (Homme, Lieutenant PNLC) que « *la cybercriminalité au Sénégal est dans un état embryonnaire* ». Autrement dit, la situation de la cybercriminalité au Sénégal n'est pas alarmante comme dans certains pays d'Afrique ou dans le monde.

[30] *Source : Entretiens avec le Lieutenant Niang et le Sous-lieutenant Diatta de la plateforme numérique de lutte contre la cybercriminalité*

5.2.1. Les plaintes reçues

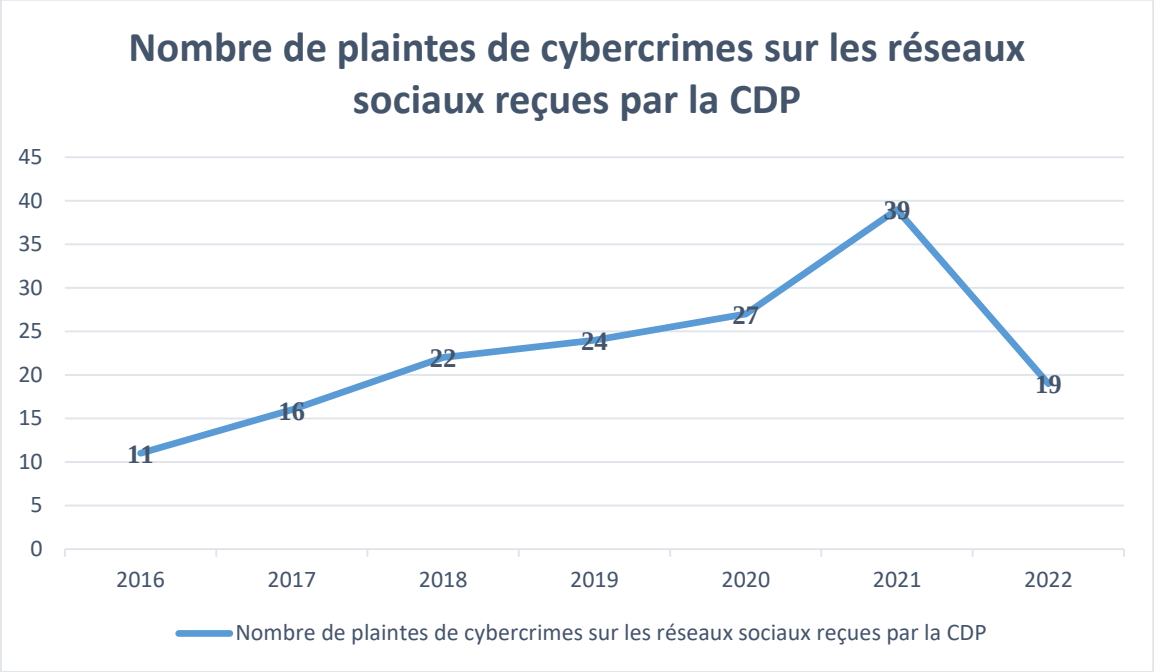
Graphique 8 : Évolution des plaintes reçues par la division spéciale de cybersécurité (DSC) de 2020 à 2022.



Source : Division spéciale de cybersécurité (DSC)

La division spéciale de cybersécurité, en tant qu'organe de contrôle et de lutte contre la cybercriminalité au Sénégal, reçoit un bon nombre de plaintes s'affairant à ce phénomène. Entre 2020 et 2022, la division spéciale de cybersécurité (DSC) a reçu huit mille deux cent trente (8230) plaintes portant sur la cybercriminalité. A travers ces chiffres, nous pouvons constater une importante augmentation du nombre de plaintes reçues par année au cours de ce cycle de trois ans. De 2020 à 2021, la division spéciale de cybersécurité est passée de 1890 à 2722 plaintes reçues, soit un taux d'évolution de 44%. La même marge d'évolution est aussi constatable pour ce qui est de 2021 et 2022. Les plaintes reçues durant cette période par la division spéciale de cybersécurité sont passées de 2722 à 3618, soit un taux d'évolution de 32,93%.

Graphique 9 : Evolution des plaintes de cybercrimes dans les réseaux sociaux reçues par la commission de protection des données personnelles (CDP) de 2016 à 2022

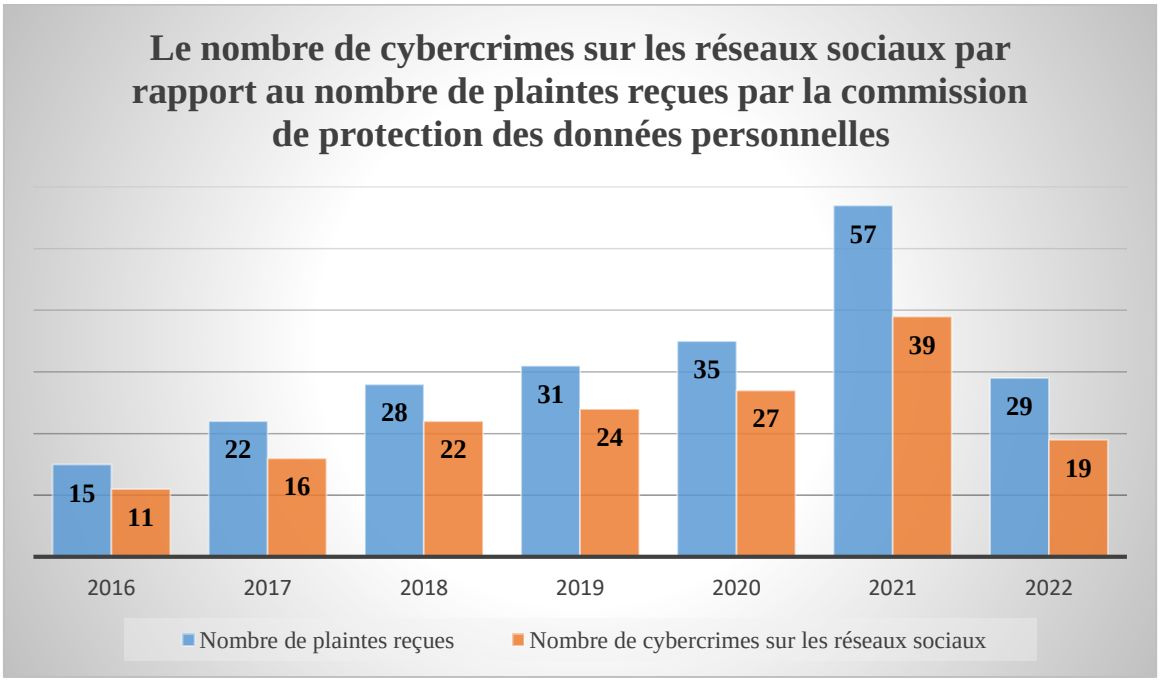


Source : Commission de protection des données personnelles (CDP)

En tant qu'organe de contrôle sur le traitement de données à caractère personnel, la commission de protection des données personnelles (CDP) reçoit des plaintes et signalements qui après étude peuvent constituer des infractions cybercriminelles. Cependant, les infractions de nature cybercriminalité dans les réseaux sociaux sont très significatives par rapport au nombre des plaintes et signalements que la commission reçoit. Entre janvier 2016 et Décembre 2022, elle a enregistré cent cinquante-huit (158) plaintes et signalements de cybercrimes dans les réseaux sociaux. Une forte augmentation des plaintes et signalements reçus est à souligner, puisqu'elle en enregistrait une douzaine par an pour les deux premières années, pour en arriver à une vingtaine par an pour les trois années suivantes et pour enfin en recevoir une trentaine par an en la période de 2021. Cependant, une baisse des plaintes et signalements considérable est notée au cours de l'année 2022 par rapport à l'année précédente. Y apporter une explication claire devient problématique étant donné qu'il est difficile de mesure l'ampleur des infractions cybercriminelles dans les réseaux sociaux, puisque ce n'est pas tous les cybercrimes qui sont rapportés aux instances de contrôle et de lutte de la cybercriminalité. Raison pour laquelle, il est difficile voire impossible de dire si c'est parce que les utilisateurs ont adopté une meilleure hygiène cyber, ou que les institutions en charge de la lutte contre la cybercriminalité ont fait un

travail remarquable au point de dissuader les cybercriminels, ou encore qu'il y ait une raison supplémentaire.

Graphique 10 : Nombre de plaintes de cybercrimes dans les réseaux sociaux par rapport au nombre de plaintes de cybercriminalité reçues par la commission de protection des données personnelles (CDP) de 2016 à 2022

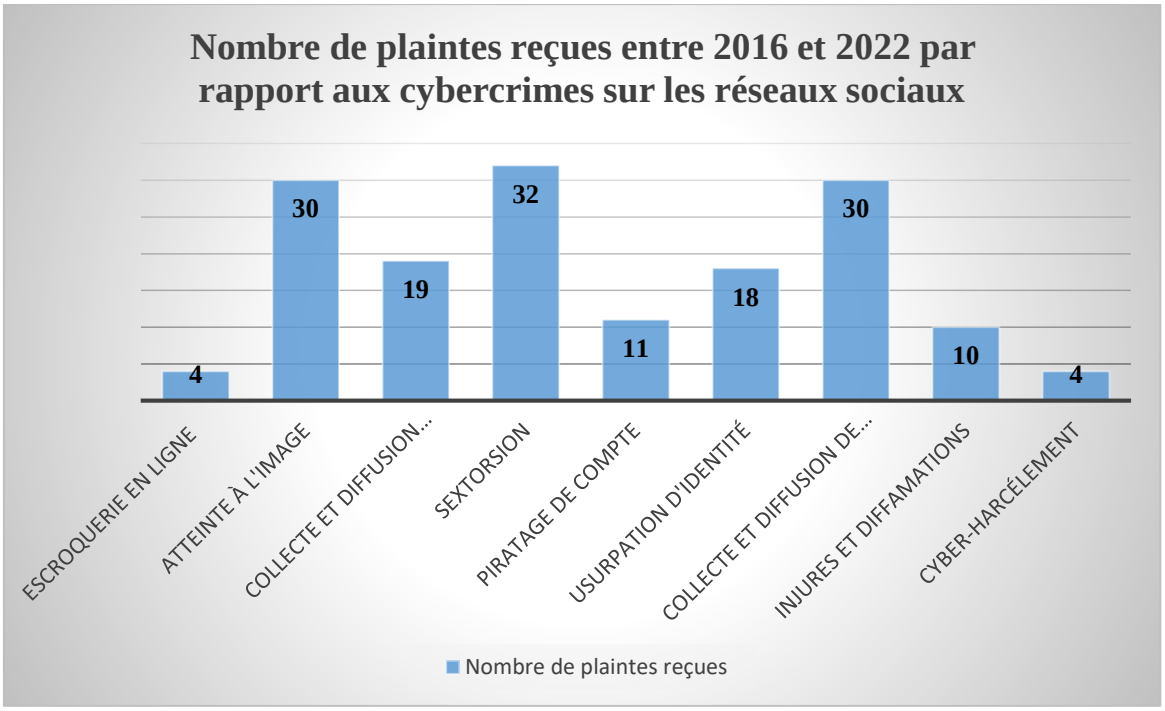


Source : Commission de protection des données personnelles

Etant un des organes de contrôle social en matière de traitement des données à caractère personnel, la commission de protection des données personnelles (CDP) reçoit et traite un nombre important de plaintes et de signalements impliquant l'utilisation ou traitement des données à caractère personnel que ce soit au niveau des entreprises ou que cela concerne simplement les particuliers. De 2016 à 2022 la commission de protection des données personnelles a reçu 217 plaintes liées au traitement des données à caractère personnel dont les 158 sont des plaintes de cybercrimes dans les réseaux sociaux, soit 72,81%. Ce qui explique à quel point le crime est présent dans les réseaux sociaux et nous conforte dans les observations qui nous ont menées au choix de cette étude. De ces dernières ressortent l'idée d'une forte présence d'infractions cybercriminelles dans les réseaux. Au regard de ces statistiques et des estimations sur les cybercrimes non signalés, il est évident que ce phénomène criminel gagne du terrain.

En prenant en compte le genre pour le profil cybercriminel, les statistiques de la division spéciale de cybersécurité (DSC) de la police rendent compte de l'importante supériorité des hommes mis en accusation pour cybercriminalité par rapport aux femmes. Au cours de l'année 2021, cent quatre-vingt-cinq (185) hommes contre cinquante-six (56) femmes ont été conduits devant le parquet pour des faits de cybercriminalité au Sénégal.

Graphique 11 : Nombre de plaintes reçues selon type de cybercrime par la commission de protection de données personnelles (CDP) de 2016 à 2022



Source : Commission de protection des données personnelles (CDP)

De 2016 à 2022, la commission de protection des données personnelles (CDP) a reçu cent cinquante-huit plaintes de cybercriminalité dans les réseaux sociaux dont : quatre (4) pour escroquerie en ligne, trente (30) pour atteinte à l'image, dix-neuf pour collecte et diffusion d'images pornographiques, trente-deux (32) pour sextorsion, onze (11) pour piratage de comptes de réseau social, dix-huit (18) pour usurpation d'identité, trente (30) pour collecte et diffusion de données personnelles, dix (10) pour injures et diffamations, quatre (4) pour Cyber-harcèlement.

Même si ces chiffres sur les plaintes et déferrements sont représentatifs, il n'en demeure pas moins que la majeure partie des cas de cybercriminalité ne sont pas signalés auprès des instances de veille et de lutte contre cette criminalité. Cela s'explique par le fait que certaines victimes ont peur du regard et des jugements dont ils peuvent faire l'objet. De plus, les menaces de

divulgation de la part des cybercriminels empêchent certaines victimes à porter plainte surtout pour ce qui est des cybercrimes impliquant des données personnelles à caractère sexuel. D'ailleurs c'est ce que le Lieutenant Niang de la plateforme numérique de lutte contre la cybercriminalité (PNLC) souligne en ces termes : « *la plupart des victimes ne portent pas plainte parce qu'ils ont peur que les gens sachent ce qu'ils ont fait ou ont peur d'être jugées* » A cela s'ajoute, le fait que des services de veille et de lutte contre la cybercriminalité, comme la commission de protection des données personnelles (CDP), ne sont pas connus du grand public.

Tableau 17 : Récapitulatif des types de données sur la cybercriminalité

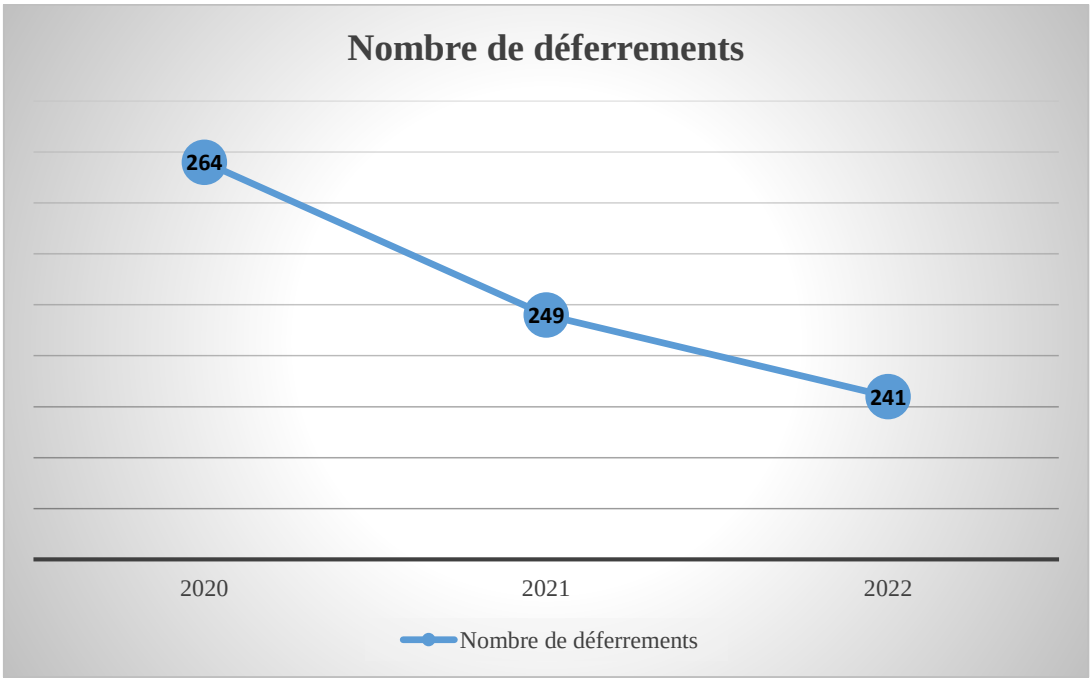
Données officielles	Chiffres noires
Les plaintes et signalements de cybercrimes au niveau des services de cybersécurité et de lutte contre la cybercriminalité (Base de données cybercriminelles)	L'ensemble des cybercrimes non rapportés aux instances de lutte contre la cybercriminalité

Ce tableau est un récapitulatif des types de données sur la cybercriminalité. Il met en évidence cette partie invisible des chiffres utilisés pour faire état de la situation de la cybercriminalité.

5.2.2. Les déferrements

Les déferrements sont constitués des statistiques sur les cybercriminels arrêtés par les services de lutte contre la cybercriminalité au Sénégal. Ces statistiques sont classées en fonction du sexe, de la nationalité et des années. La classification des déferrements par année permet de marquer l'évolution de la cybercriminalité au Sénégal.

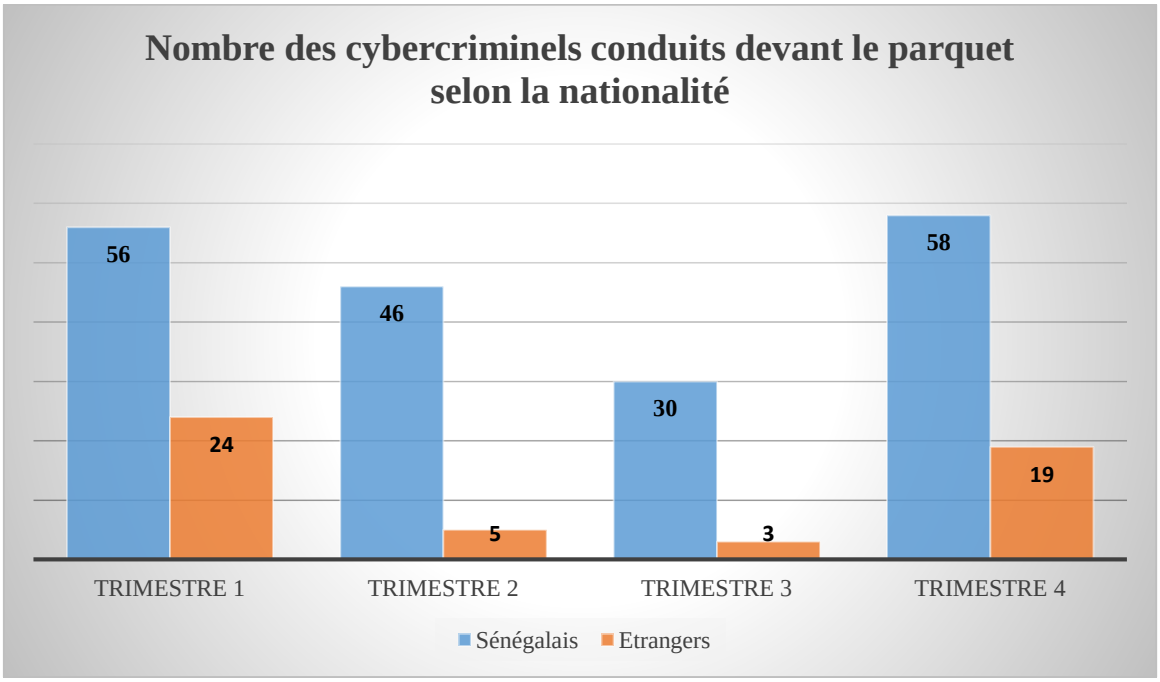
Graphique 12 : Nombre de déferrements effectués par la division spéciale de cybersécurité de 2020 à 2022



Source : Division spéciale de la cybersécurité (DSC)

Même si le nombre de cybercriminels déferrés diminue d'année en année, il faut quand-même souligner l'importance de ces chiffres. Ces derniers mettent en évidence l'ampleur de la cybercriminalité au Sénégal. Sur une période de trois (3) ans, sept cent cinquante-quatre (754) personnes ont été déférées par la division spéciale de cybersécurité (DSC) de la police suite à des actes de cybercriminalité. Ces chiffres étant celles d'une seule structure de lutte contre la cybercriminalité, rend compte de l'envergure de la cyber-délinquance, mais aussi de la lutte à son encontre.

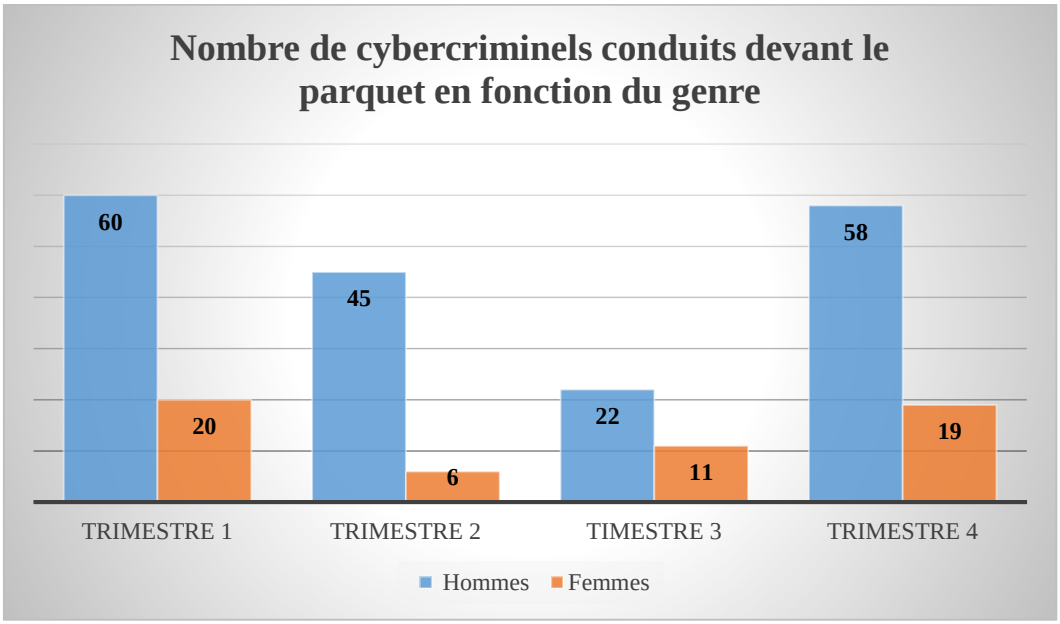
Graphique 13 : Nombre de déferrements selon la nationalité par la division spéciale de cybersécurité (DSC) en 2022



Source : Division spéciale de la cybersécurité (DSC)

Même si les statistiques montrent une forte supériorité de cybercriminels sénégalais conduits devant le parquet, il convient de souligner le nombre important de cyber-délinquants étrangers. Ce qui rend compte du caractère transnational de la cybercriminalité. Les cybercriminels de nationalité étrangère opérant à partir du territoire sénégalais se constituent pour la plupart du temps en réseau. « *C'est ainsi qu'en août 2021, après de longues investigations menées par la brigade de la Zone Franche Industrielle de Mbao, trente-deux (32) cybercriminels de nationalité étrangère ont été mis hors d'état de nuire au cours d'une opération d'envergure, conduite avec le soutien technique de la plateforme numérique de lutte contre la cybercriminalité (PNLC) et un renfort de l'Escadron de Surveillance et d'intervention de Diamniadio. Cette opération a également permis la saisie de quarante (40) ordinateurs portables, quarante-cinq (45) téléphones mobiles et cinq (5) modems. Face à la cybercriminalité qui établit de plus en plus ses quartiers dans la banlieue de Dakar, la Gendarmerie nationale entend renforcer les moyens de surveillance et de contrôle pour démanteler ces groupes spécialisés dans les attaques via internet* ». (Niang, Otonkala, Kpeto, & Yaffa, 2022)

Graphique 14 : Nombre de déferrements en fonction du sexe par la division spéciale de cybersécurité (DSC) en 2022



Source : Division spéciale de cybersécurité (DSC)

5.3.Les politiques publiques

La lutte contre la cybercriminalité passe par la mise en place de stratégies efficientes et efficaces. Ces dernières se traduisent sous forme de politiques publiques nationales ou internationales. Le Sénégal, à travers son acte gouvernemental du Plan Sénégal Émergent (PSE), s'est inscrit dans une volonté d'établir une société du numérique. Cette numérisation implique l'utilisation des technologies de l'information et de la communication dans tous les secteurs d'activités et de l'administration. Pour se faire, établir un cadre général devient plus que nécessaire. C'est dans ce contexte que la stratégie nationale de cybersécurité a été mise en œuvre. Elle est une mise en application de la stratégie Sénégal Numérique 2025 (SN2025). Celle-ci est une politique de modernisation de l'économie du Sénégal.

5.3.1. La stratégie nationale de cybersécurité SNC2022

La stratégie nationale de cybersécurité (SNC2022) articule la vision du Sénégal en matière de cybersécurité en traduisant les objectifs de la stratégie « Sénégal numérique 2025 » (SN2025). Cette dernière promeut la mise en place d'un cyberespace sûr et confiant, d'où le slogan « En 2020 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous »[31]. Cette vision s'organise autour de cinq grands objectifs :

[31]STRATÉGIE NATIONALE DE CYBERSÉCURITÉ DU SÉNÉGAL (SNC2022)

- Dans un premier temps, le Sénégal a entrepris un renforcement du cadre juridique et institutionnel de la cybersécurité en raison de la complexité et de la nature des infractions dans le cyberespace. Ce renforcement juridique et institutionnel s'est matérialisé par la création d'unités spéciales de lutte contre la cybercriminalité dont la commission de protection de données personnelles (CDP), la division spéciale de cybersécurité (DSC), la plateforme numérique de lutte contre la cybercriminalité (PNLC), la direction générale du chiffre et de la sécurité des systèmes d'information (DCSSI). A cela s'ajoute la mise en place de lois investissant ces instants de pouvoirs légitimes dans la lutte contre la cybercriminalité.
- La protection des infrastructures d'informations critiques (IIC) et des systèmes d'information permet à l'Etat du Sénégal d'avoir le contrôle de ses infrastructures mais aussi la maitrise de l'information et les conditions dans lesquelles elle est utilisée.
- La promotion d'une culture de cybersécurité est capitale dans la lutte contre la cybercriminalité. Cette promotion se traduit par une sensibilisation des acteurs publics et privés et les particuliers et leur capacitation en cybersécurité. Sans la promotion d'une culture de cybersécurité, la lutte contre la cybercriminalité serait vouée à l'échec. Parce que l'efficacité des services de cybersécurité ne saurait à elle seule être suffisante dans cette lutte. L'efficacité des politiques de cybersécurité demande à la fois implication et collaboration des acteurs publics et privés et les particuliers. Ces derniers doivent être sensibilisés au point de développer une hygiène cyber, c'est-à-dire de bons réflexes.
- Le renforcement des capacités et connaissances techniques en cybersécurité dans tous les secteurs est essentiel en raison de la vitesse d'évolution des technologies numériques et des techniques cybercriminelles. La formation des acteurs sur les tendances technologiques et cybercriminelles leur permettra d'être à jour dans la lutte contre la cybercriminalité.
- La participation aux efforts régionaux et internationaux est évident en raison du caractère transnational de la cybercriminalité. Elle permet de mettre en place des politiques de cybersécurité plus efficientes. Parce que les initiatives régionales et internationales permettent aux États d'agir au-delà de leurs frontières dans la traque des cybercriminels. Elles permettent aussi un partage de compétences entre États.

Source : Stratégie nationale de cybersécurité SNC2022

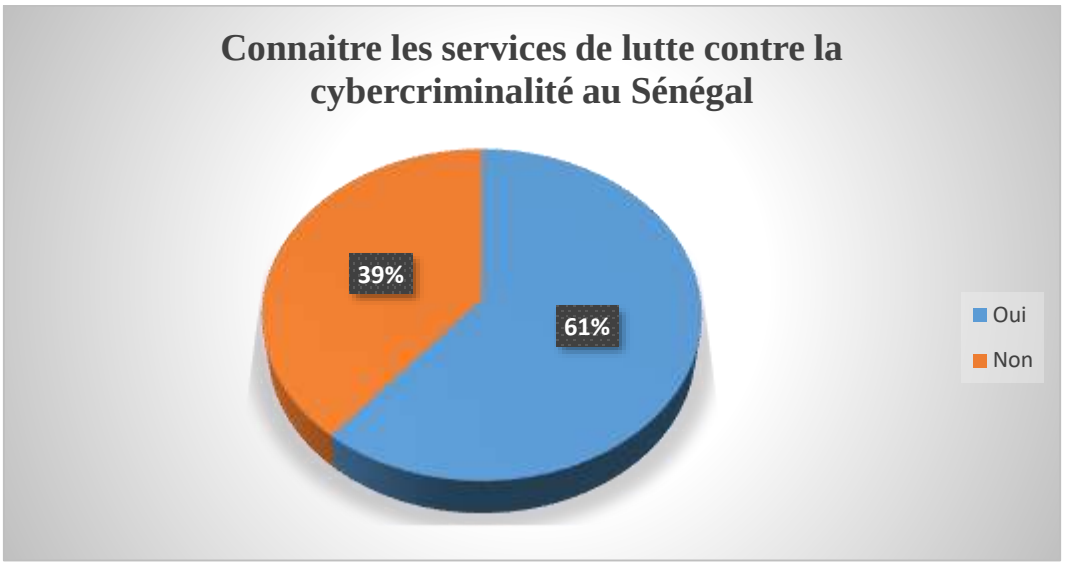
5.3.2. Les limites des politiques publiques de lutte contre la cybercriminalité

L'absence ou manque d'initiatives ou de politiques publiques en termes de sensibilisation sur la cybercriminalité de manière générale ou spécifiquement réseaux sociaux est une remarque un peu plus générale au Sénégal. Que ça soit du côté des utilisateurs, la quasi-totalité de nos enquêtés disent ne pas avoir connaissance d'une quelconque politique de sensibilisation sur la cybercriminalité. Cet état de fait a été aussi souligné au niveau des services de lutte contre la cybercriminalité. Le Lieutenant Niang de plateforme numérique de lutte contre la cybercriminalité (PNLC) nous le fait remarquer en disant que « *nous n'avons pratiquement pas de politiques de sensibilisation des utilisateurs des réseaux sociaux au Sénégal. A part ce qu'on fait en interne qui ne concerne que les agents de la gendarmerie* ». Sur cette même logique, poursuit Ndour (Lieutenant DPJ, homme, 41 ans) en disant « *la sensibilisation se fait quand les victimes viennent porter plainte. Après les avoir entendus, on les sensibilise pour qu'elles aient une meilleur hygiène cyber* ».

Il en de même au niveau des autres services, même si la division spéciale de la cybersécurité (DSC) profite des occasions qui se présentent à elle, c'est-à-dire l'animation de panel sur les technologies de l'information et de la communication (TIC), pour sensibiliser les utilisateurs en particulier les jeunes. D'ailleurs, Kandé (commissaire à la DSC, homme) le souligne en ces termes : « *Au cours de l'année 2023, nous avons animé des conférences dans les lycées Mariama Ba, John Fitzgerald Kennedy et Yeumbeul pour sensibiliser les jeunes des dangers liés au réseaux sociaux et à internet* ».

Ce que, d'ailleurs, nos données d'enquête illustrent. Sur les cent (100) individus composant notre échantillon d'étude, aucun n'a connaissance d'un quelconque programme gouvernemental de sensibilisation sur la cybercriminalité dans sa générale ou spécifique aux réseaux sociaux. Ce qui rend compte des limites des politiques publiques de cybersécurité et de lutte contre la cybercriminalité au Sénégal.

Graphique 16 : Connaissance des services de lutte contre la cybercriminalité au Sénégal



Source : Enquête de terrain Diouf 2023

Même si 61% de nos enquêtés connaissent les services en charge de la lutte contre la cybercriminalité au Sénégal, le pourcentage d'enquêtés ne le connaissant pas reste significatif. Ce qui peut avoir un impact considérable sur le nombre de cybercrimes rapportés à ces services, par conséquent sur la quantification de la cybercriminalité au Sénégal. De plus, cela va jouer aussi sur l'efficacité de la lutte contre la cybercriminalité étant donné les personnes ne connaissant pas ces services ne pourront pas consentir aux efforts de lutte contre la cybercriminalité.

5.4. Coopération entre différents acteurs de la cybercriminalité

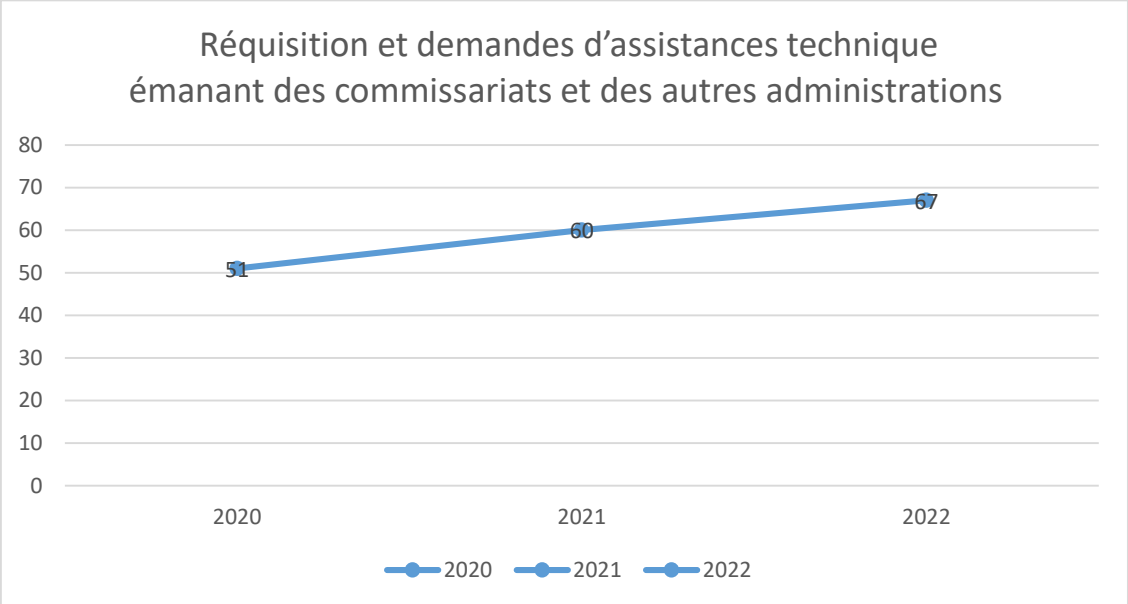
La lutte contre la cybercriminalité ne peut être l'affaire d'une seule institution ou d'un seul Etat. Le fait qu'elle touche pratiquement tous les secteurs d'activités implique nécessaire la coopération d'une multitude d'acteurs. De plus les législations en matière de lutte contre la cybercriminalité, qu'elles soient au niveau national, sous régional, continental ou international s'inscrivent dans une logique de coopération du fait du caractère transnational de la cybercriminalité. C'est dans cette perspective que des conventions internationales et des directives communautaires ont institué cette coopération à travers leurs ratifications par les États.

5.4.1. Coopération entre les acteurs nationaux

La lutte contre la cybercriminalité n'est pas une mince affaire et ne peut se faire par un petit groupe d'acteurs. Pour arriver à certains résultats, les services étatiques de lutte contre la

cybercriminalité ont non seulement besoin de collaborer entre eux, mais de faire appel à d'autres services publics et privés. Cette collaboration se fait pour la plupart du temps à travers des réquisitions envoyées par les services n'étant pas dans les dispositions de mener des enquêtes de cybercriminalité. C'est le cas de la commission de protection des données personnelles, qui, pour les plaintes de cybercriminalité qu'elle reçoit, accompagne les plaignants pour la procédure à suivre mais pour les enquêtes s'en remet au bureau du procureur et de la division spéciale de cybersécurité (DSC). Les demandes d'assistance des autres services autres de police ou des administrations sont généralement formalisées par une réquisition judiciaire, prescrivant la réalisation d'actes précis. Ainsi, lorsqu'une analyse de données informatiques, l'extraction de données téléphoniques ou encore des opérations de recouvrements de données effacées sont demandées, le chef de service de la division spéciale de cybersécurité (DSC) saisit le Laboratoire national d'analyse technico-numérique, aux fins de la réalisation d'actes techniques demandées. Parfois, c'est l'assistance physique des enquêteurs de la division qui sera requise en amont, au moment des perquisitions ou d'actions menées par un autre service.

Graphique 17 : Réquisitions et demandes d'assistance technique émanant des commissariats et des autres administrations à la division spéciale de cybersécurité (DSC)



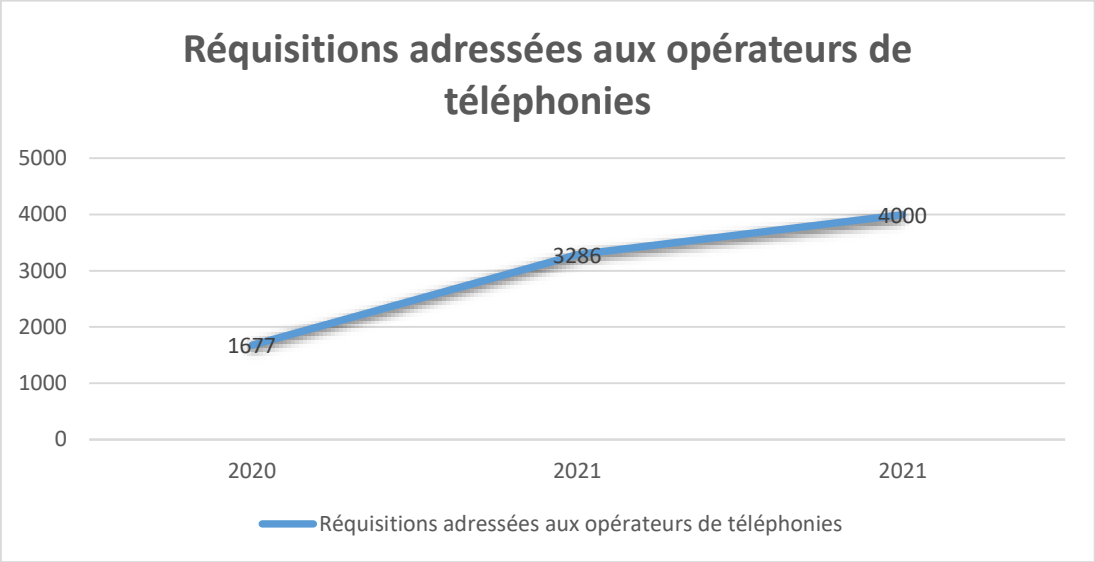
Source : Division spéciale de la cybersécurité (DSC)

Il en va de même pour les services de la gendarmerie comme les brigades territoriales, qui doivent faire appel à la plateforme numérique de lutte contre la cybercriminalité (PNLC) pour

toute enquête impliquant un réseau informatique. Parce que celle-ci étant l'instance d'expertise et technique habilitée à procéder des enquêtes sur internet et sur des supports numériques.

Il y a aussi les cas de figure où se sont les services étatiques de lutte contre la cybercriminalité qui saisissent d'autres acteurs dans le cadre de leurs enquêtes. Ce sont les cas de figure où les services comme la police ou la gendarmerie envoient des réquisitions aux opérateurs de téléphonies, de transfert d'argent et aux administrations.

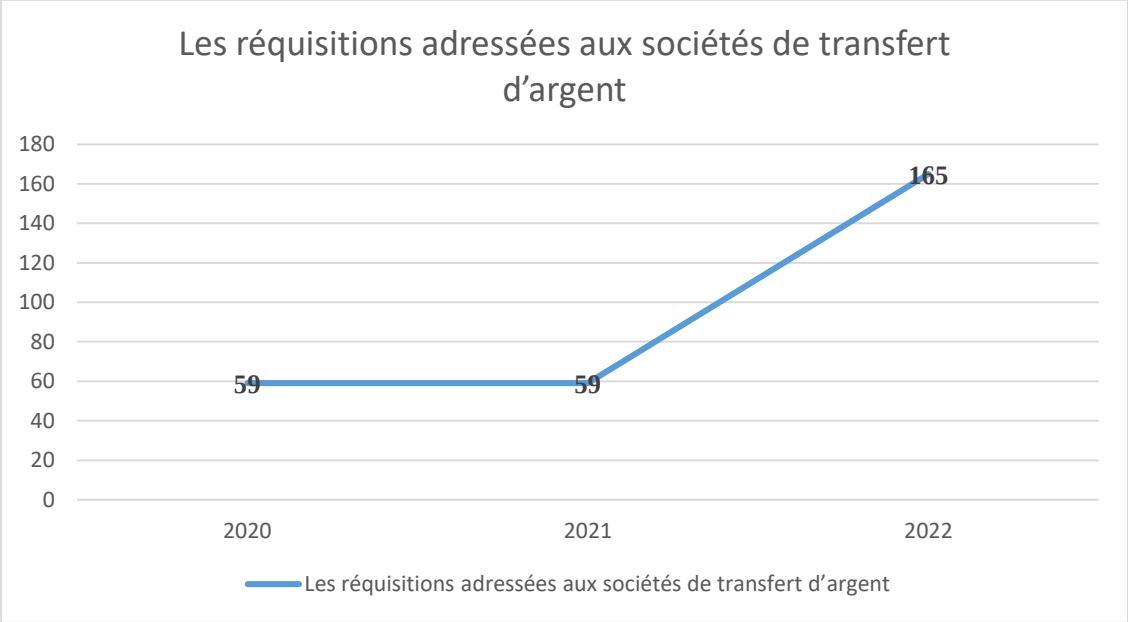
Graphique 18 : Réquisitions adressées aux opérateurs de téléphonies par la division spéciale de cybersécurité (DSC) de 2020 à 2022



Source : Division spéciale de la cybersécurité (DSC)

Avec les règles d'identification des numéros de téléphone attribués aux utilisateurs, les instances de contrôle et de répression de la cybercriminalité au Sénégal peuvent saisir les opérateurs de téléphonie pour leur faciliter l'identification et la traque des cyber-délinquants.

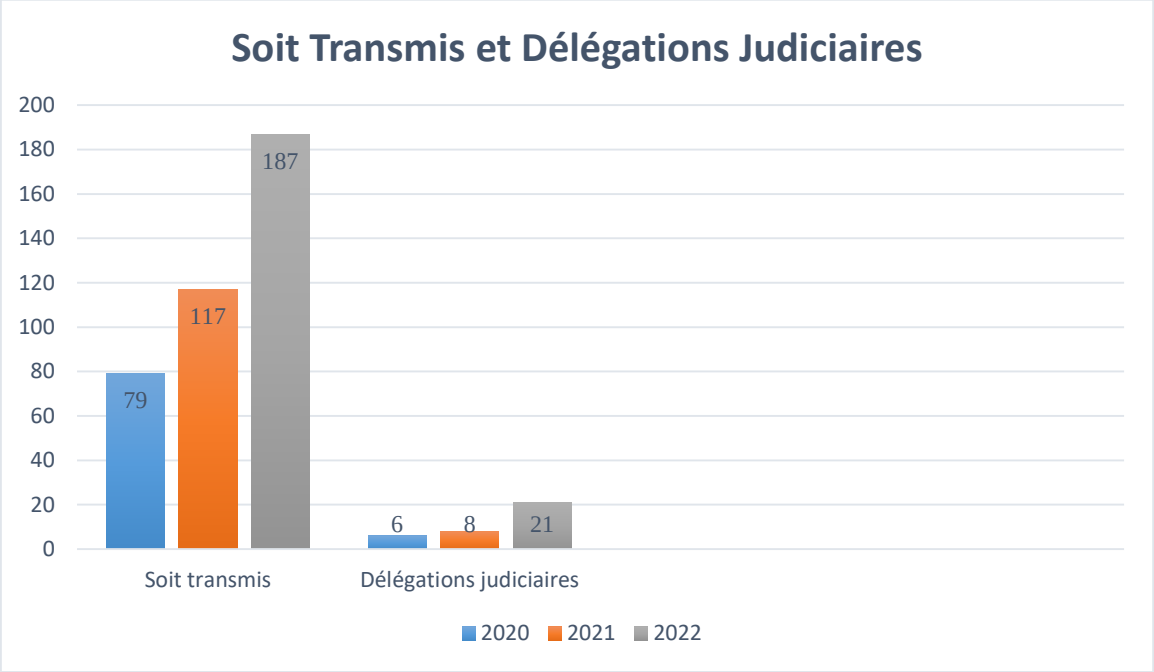
Graphique 19 : Réquisitions adressées aux sociétés de transfert d'argent par la division spéciale de cybersécurité (DSC) de 2020 à 2022



Source : Division spéciale de la cybersécurité (DSC)

Comme pour les opérateurs de téléphonies, les services de contrôle et de répression de la cybercriminalité au Sénégal réquisitionnent aussi les opérateurs de transfert d'argent pour leur permettre de suivre les transactions issues des activités cybercriminelles. En faisant cela, ces services peuvent remonter jusqu'aux cybercriminels et par là, procéder à des mises en accusations et à de possibles inculpations.

Graphique 20 : Évolution du nombre de Soit Transmis et de délégations judiciaires de 2020 à 2022



Source : Division spéciale de la cybersécurité (DSC)

Les cas de soit transmis et de délégations judiciaires concernent l'ensemble des plaintes venant pour la plupart du temps du bureau du procureur et de la commission de protection des données personnelles (CDP). Ils transmettent à la division spéciale de cybersécurité (DSC) les plaintes nécessitant une expertise pour la collecte de preuves numériques, d'identification des cybercriminels pour d'éventuelles poursuites ou mises en accusation. Cela fait état une fois de plus de la collaboration entre les acteurs nationaux dans le cadre de la lutte contre la cybercriminalité au Sénégal.

5.4.2. Coopération sous régionale

Au niveau sous régionale, la CEDEAO (Communauté Economique des États de l'Afrique de l'Ouest), à travers ses directives et actes additionnels, est l'acteur majeur de la coopération entre les États membres dans le cadre de la lutte contre la cybercriminalité.

Comme première initiative communautaire, on peut se référer à l'Acte additionnel A/SA 1/01/10 relatif à la protection des données à caractère personnel en zone CEDEAO (Communauté Economique des États de l'Afrique de l'Ouest). IL fut adopté lors de la 37e session de la conférence des chefs d'état et de gouvernement le 16 février 2010 à Abuja (Nigeria). Il a pour objet la mise en place par chaque État membre d'un cadre légal de protection

de la vie privée et professionnelle consécutive à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel, sous réserve de la protection de l'ordre public.

De plus, il y a la Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO qui a pour objet l'adaptation du droit pénal de fond et la procédure pénale des États membres de la CEDEAO au phénomène de la cybercriminalité. Elle est applicable à toutes les infractions relatives à la cybercriminalité dans l'espace de la communauté, ainsi qu'à toutes les infractions pénales dont la constatation requiert la collecte d'une preuve électronique.

En plus de ces mécanismes, la CEDEAO et de l'UEMOA disposent d'autres moyens et dispositions de coopération en matière de lutte contre la cybercriminalité

- Stratégie de la CEDEAO en cybersécurité et lutte contre la cybercriminalité

La CEDEAO a mis en place une stratégie régionale pour renforcer la cybersécurité et combattre la cybercriminalité, en harmonisant les législations des États membres. Elle vise à protéger les données personnelles, promouvoir une utilisation sécurisée de l'internet, et établir des normes de sécurité. La stratégie favorise également la coopération interétatique pour une réponse coordonnée aux menaces cybernétiques.

- Politique de la CEDEAO sur la protection des Infrastructures Critiques (IC)

La CEDEAO a développé une politique pour protéger les infrastructures critiques contre les menaces cyber et physiques, en définissant des cadres de gestion des risques et de résilience. Cette politique soutient la mise en place de mesures de sécurité pour assurer la continuité des services essentiels. Elle encourage également la coopération régionale et le partage d'informations pour renforcer la protection des infrastructures sensibles dans toute la région.

La CEDEAO et l'UEMOA coopèrent étroitement pour lutter contre la cybercriminalité en Afrique de l'Ouest, en mettant en place plusieurs mécanismes, moyens et dispositions stratégiques. La CEDEAO a établi une stratégie de cybersécurité et de lutte contre la cybercriminalité, qui promeut la coopération régionale, le renforcement des capacités et l'échange d'informations entre les États membres. Cette stratégie est complétée par des initiatives de protection des infrastructures critiques, incluant la coordination entre forces de sécurité et institutions nationales et régionales.

L'UEMOA soutient ces efforts par des programmes de formation et des partenariats visant à harmoniser les législations, assurer la protection des données, et encourager des collaborations transfrontalières pour améliorer la prévention et les réponses aux cybermenaces.

La coopération technique et opérationnelle au sein de la CEDEAO et de l'UEMOA joue un rôle crucial dans la lutte contre la cybercriminalité. Les deux organisations facilitent l'assistance technique, l'échange d'expertise et le déploiement de programmes conjoints pour renforcer les capacités opérationnelles des États membres. Cela inclut l'organisation d'exercices de simulation, la formation des forces de l'ordre et des acteurs judiciaires, et la mise en place de réseaux d'échange d'informations sécurisés. Ces efforts visent à améliorer la coordination transfrontalière et à assurer une réponse rapide et efficace aux incidents cybernétiques dans la région.

Il y a AfricaCERT qui joue un rôle central dans la coopération en matière de cybersécurité en Afrique. En tant qu'organisation, AfricaCERT coordonne les efforts des équipes nationales et régionales de réponse aux incidents de sécurité informatique (CSIRT) à travers le continent. Ses principales contributions incluent :

- Renforcement des capacités : AfricaCERT organise des formations et des ateliers pour améliorer les compétences techniques des CSIRT africains, favorisant ainsi une réponse efficace aux cybermenaces.
- Partage d'informations : En facilitant l'échange de renseignements sur les menaces et les vulnérabilités, AfricaCERT aide les pays membres à anticiper et à atténuer les risques cybernétiques.
- Harmonisation des pratiques : L'organisation promeut l'adoption de normes et de meilleures pratiques communes, renforçant ainsi la résilience collective face aux cyberattaques.
- Collaboration régionale et internationale : AfricaCERT sert de pont entre les CSIRT africains et les organisations internationales, telles que l'Organisation internationale de la Francophonie (OIF) et l'Union internationale des télécommunications (UIT), facilitant une coopération globale en matière de cybersécurité.

5.4.3. Niveau africain ou continental

La convention de l’union Africaine (UA) sur la cybersécurité et la protection des données à caractère personnel a été adoptée lors de la 23^{e} session ordinaire du sommet de l’Union

Africaine (UA). Ce sommet s'est tenu les 26 et 27 juin 2014, regroupant les chefs d'Etat et de gouvernement de l'Union Africaine (UA).

La Convention vise à « *renforcer et harmoniser les législations actuelles des États membres et des Communautés Economiques Régionales (CER) en matière de technologies de l'information et de la communication (TIC)* »[32], dans le respect des libertés fondamentales et des droits de l'Homme et des Peuples. Elle vise également à créer « un cadre normatif approprié correspondant à l'environnement juridique, culturel, économique et social africain » et souligne que la protection des données personnelles et de la vie privée est un « enjeu majeur de la société de l'information » ; tout traitement de données personnelles doit respecter un équilibre entre libertés fondamentales, promotion et usage des techniques de l'information et de la communication (TIC), intérêts des acteurs publics et privés.

L'adoption de la Convention s'inscrit dans la continuité des engagements des États membres pour une harmonisation des cyber-législations africaines.

5.4.4. Coopération internationale

La coopération internationale sur la cybersécurité et sur la lutte contre la cybercriminalité est instituée par la convention de Budapest. Cette dernière s'inscrit dans la perspective de mettre en place « une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace[33] ». Ce qui passe par l'adoption d'une législation efficiente et l'amélioration de la coopération internationale. Cette dernière est plus que nécessaire du fait du caractère transnational de la cybercriminalité.

Le Sénégal ratifie la convention le 01 Décembre 2016, faisant de lui le 50^{e} Etat membre. La ratification de cette convention permet aux autorités judiciaires et policières du Sénégal d'obtenir une assistance des États membres et des acteurs globaux d'internet. Cette assistance des acteurs globaux permet à nos autorités en matière de lutte contre la cybercriminalité de procéder à des retraits de contenus illicites diffusés à travers les réseaux sociaux et la suppression ou la restitution de comptes piratés aux utilisateurs.

La Convention de Budapest, ou Convention sur la cybercriminalité, définit plusieurs éléments clés de la coopération internationale pour lutter contre la cybercriminalité :

[32] La Convention du 23 juin 2014 sur la cybersécurité et la protection des données à caractère personnel.
[33] Convention sur la cybercriminalité Budapest, 23.11.2001

- Assistance mutuelle rapide: La convention établit des procédures pour une assistance rapide entre États, y compris la collecte et la conservation rapide des preuves électroniques.
- Échange d'informations: Elle encourage les pays signataires à partager les informations essentielles, notamment sur les menaces et les cyberattaques, afin de mieux prévenir et enquêter sur les cybercrimes.
- Accès transfrontalier aux données: La convention introduit des mesures pour accéder légalement aux données stockées dans d'autres pays, facilitant ainsi les enquêtes transfrontalières.
- Points de contact 24/7: Les États membres sont tenus de désigner des points de contact opérationnels disponibles 24h/24 pour répondre rapidement aux demandes urgentes.
- Harmonisation législative: La convention encourage les pays à harmoniser leurs lois nationales pour créer une base commune dans la criminalisation des actes de cybercriminalité, ce qui facilite la coopération juridique.

5.4.5. Les limites de la coopération entre les acteurs

Avec les différentes conventions sur la cybercriminalité signées et ratifiées par plusieurs États, l'on pourrait croire que la coopération entre les acteurs ne connaitrait pas de limites. Cependant certains facteurs entravent le bon déroulement de cette coopération. Ce qui fait que certains cybercriminels ne soient pas traduits en justice.

Il est important de prendre en compte l'aspect territorial de la cybercriminalité pour les cas de cybercrimes dans les réseaux sociaux au Sénégal non résolus et dont les cybercriminels sont hors du pays. Il est clair que la définition de ce qui est cybercriminel ou non dépend de la législation en vigueur dans le pays où se trouve le cybercriminel en question. Même si les conventions de Budapest au niveau international, de Malabo au niveau africain et les directives et actes additionnels de la CEDEAO (communauté économique des États de l'Afrique de l'ouest) au niveau sous régional instituent la coopération entre États dans la lutte contre la cybercriminalité, il n'en demeure pas moins que celle-ci se heurte à la spécificité législative nationale en terme de cybercriminalité.

En se référant aux cas de cybercriminalité tels que les injures et les diffamations que nous avons au Sénégal, ils ne sont pas pour autant considérés comme de la cybercriminalité dans les pays occidentaux. Elles relèvent dans ces derniers de la liberté d'expression.

> Si nous prenons l'exemple des personnes qui insultent le Président de la République ou les personnalités religieuses, mais qui ne trouvent sur le territoire national, ils ne peuvent pas être inquiétés tant qu'ils sont à l'étranger. Dès que nous transmettons une demande à nos homologues du pays où se trouve cette personne, la réponse qui revient sans cesse après étude du dossier est que c'est de la liberté d'expression, donc ils ne peuvent pas donner suite à notre demande. (Commissaire Kandé de la division spéciale de cybersécurité)

C'est pourquoi il est évident de souligner l'opposition entre le caractère transnational de la cybercriminalité et la territorialité des actes posés par les cybercriminels. Celle-ci rend difficile voire impossible la coopération entre les États.

Cette coopération, qui se traduit par l'entraide judiciaire, n'est possible que s'il y a ce que l'on appelle la « double criminalité ». Autrement dit, le fait que l'infraction cybercriminelle soit considérée comme telle dans les deux pays. Nonobstant cela, l'impossibilité de procéder à des poursuites judiciaires se présente.

S'agissant de la coopération entre les acteurs nationaux, elle présente aussi des limites. Les réquisitions des services tels que la plateforme numérique de lutte contre la cybercriminalité (PNLC) ou la division spéciale de cybersécurité (DSC) auprès des administrations ne sont pas souvent prises en compte ou n'ont pas de suite. C'est ce qui signifie Niang (Lieutenant à la PNLC, homme) en ces termes « *c'est difficile d'enquêter sur les cas d'escroquerie des plateformes d'investissement. Ils ont des agréments des ministères. Pendant les enquêtes, on nous balade. Personne ne veut répondre à nos questions. Ils te disent va voir telle personne. Cette personne aussi te renvoie vers un autre ou dit qu'il n'en sait rien* ». Ce qui rend compte de la non effectivité de la coopération entre les acteurs nationaux. De plus, la centralisation des données au niveau des unités dédiées à la cybersécurité et à la lutte contre la cybercriminalité reste problématique étant donné que les unités territoriaux (brigades de gendarmerie ou commissariats de Police) ne partagent pas leurs données avec celles-ci. D'ailleurs, Niang (Lieutenant à la PNLC, homme) le signifie en ces termes « *les brigades territoriales nous demandent assistance pour les affaires de cybercriminalité ou pour des preuves numériques mais ne nous font pas de retour à la fin de leur enquête* ». Ce qui ne permet effectivement pas une centralisation des données.

Chapitre 6 : Les formes de cybercrimes dans les réseaux sociaux au Sénégal

La cybercriminalité dans sa généralité ou dans sa spécification aux réseaux sociaux n'est pas uniforme. En réalité, nous retrouvons des formes très divers. Cette diversité est caractérisée à la fois par les techniques et méthodes de commission d'actes cybercriminels, mais aussi de la législation du pays dans lequel se déroule l'infraction.

Dans la législation sénégalaise, on remarque une volonté de définition du phénomène cybercriminel mais aussi une catégorisation des différentes infractions cybercriminelles. Cette catégorisation implique d'établir ce en quoi consiste chaque forme de cybercrimes, la peine et l'amande encourue en cas de commission. Et c'est sur cette base que nous avons procédé pour l'analyse des différentes formes de cybercrimes que nous avons dans les réseaux sociaux au Sénégal.

Pour ce qui est de la typologie de la cybercriminalité dans les réseaux sociaux, nous retrouvons deux types de cybercrimes. Nous avons les infractions spécifiques aux réseaux sociaux et celles qui y sont adaptées. C'est d'ailleurs ce que l'experte internationale en cybersécurité Solange Ghernaouti dit en ces termes : *« Désormais, les technologies informatiques et les télécommunications sont cibles de malveillance et des moyens pour commettre des actions illicites. Elles permettent de réaliser de nouveaux délits, mais aussi des délits classiques »* (Ghernaouti-Hélie, 2009)

Les infractions spécifiques aux réseaux sociaux sont constituées de l'ensemble des cybercrimes dont l'exécution n'aurait été possible sans l'utilisation d'internet et plus précisément des médias sociaux. Ces types de cybercrimes sont caractérisés exclusivement par l'utilisation des données à caractère personnel de la ou des victimes.

Contrairement à celles-ci, les infractions adaptées aux réseaux sociaux sont constituées des crimes pour lesquelles l'utilisation de l'internet est un élément principal de la commission. Elles sont en effet facilitées par internet et les réseaux sociaux. Ce sont des infractions classiques qui existaient avant l'avènement de l'internet, mais elles ont été transposées dans le monde du numérique. Cette adaptation au numérique apporte une touche de facilité dans la commission et une possibilité d'impunité des actes dans la mesure où les poursuites ne sont pas toujours évidentes.

Nonobstant cela, il est aussi possible de procéder à une autre forme catégorisation des cybercrimes. Celle-ci va se faire en procédant à une classification des cybercrimes à travers ce

qu’il convient d’appeler leur nature. Par nature, nous faisons allusion à ce en quoi implique le cybercrime. C’est-à-dire ce qu’il touche vraiment.

La catégorisation des cybercrimes à travers leur nature nous permet de les classer en trois groupes : les infractions économiques et financières, les infractions sur la bonne vie et la réputation et les infractions sur l’atteinte à l’Etat, à l’extrémisme, au terrorisme.

Cette catégorisation est aussi basée sur l’objectif et/ou la finalité du cybercrime, même si certaines infractions cybercriminelles peuvent avoir la même finalité sans pour autant être de même nature.

Tableau 18 : Tableau croisé entre le type de cybercrime dont l'enquêté est victime et le fait d’être victime ou non de cybercriminalité dans les réseaux sociaux

		Etre victime ou non de cybercriminalité dans les RS		
Effectif		Oui	Non	Total
Genre de cybercrime dont l'enquêté est victime		0	62	62
	Atteinte à l'image	5	0	5
	Cyberharcélement	3	0	3
	Diffusion d'images pornographiques	10	0	10
	Escroquerie	8	0	8
	Piratage	6	0	6
	Sextorsion	6	0	6
Total		38	62	100

Source : enquête de terrain Diouf Septembre 2023

Les cybercrimes dans les réseaux sociaux auxquels sont confrontés les individus composants notre échantillon d’étude ne sont pas uniformes. Sur les trente-huit (38) victimes de cybercriminalité dans les réseaux sociaux, nous avons :

Cinq (5) cas d'atteintes à l'image

Trois (3) cas de cyber-harcèlement

Dix (10) cas de diffusions d'images pornographiques

Huit (8) cas d'escroqueries en ligne

Six (6) cas de piratages de compte de réseau social

Six (6) cas de sextorsion

6.1. Les infractions économiques et financières

Les infractions économiques et financières concernent l'ensemble des cybercrimes dont la finalité est le profit ou le gain financier.

6.1.1. L'escroquerie

> C'est le fait, par toute personne, d'employer des moyens frauduleux quelconques pour se faire remettre ou délivrer des fonds ou choses ayant une valeur pécuniaire. L'usage d'un faux nom, d'une fausse qualité peut ainsi se faire à travers les médias sociaux avec une usurpation d'identité. L'escroquerie en ligne n'est pas considérée comme un crime distinctif, mais couvre une série d'actions illégales et illicites qui sont commises dans le cyberespace (Niang, Otonkala, Kpeto, & Yaffa, 2022).

Cette forme de cybercriminalité n'a pas vu le jour avec les réseaux sociaux. Elle se déroulait et continue de se dérouler dans le milieu social physique. Cependant, elle a été adapté aux réseaux sociaux et est aujourd'hui facilitée par celles-ci.

L'escroquerie en ligne s'est accentuée ces dernières années au Sénégal avec les systèmes pyramidaux dont beaucoup de sénégalais sont victimes aujourd'hui. Ces jeunes sont pour la plupart du temps attirés à travers les réseaux sociaux ou par une connaissance. Les escrocs utilisent un système d'arnaque appelé pyramide de Ponzi[34], basé sur le fait d'attirer des investisseurs en leur promettant des rendements élevés sur leurs investissements. Cependant, au lieu de générer des bénéfices légitimes à partir d'activités commerciales ou d'investissements, l'opérateur du schéma utilise l'argent des nouveaux investisseurs pour verser des rendements aux anciens. Ce fut le cas avec les plateformes d'investissement comme Petronpay et Tesco Boutique. Ces derniers, à travers les opérateurs de transfert d'argent ont escroqué d'importantes

[34] La pyramide de Ponzi est un montage financier frauduleux basé sur la rémunération des investisseurs avec les investissements des nouveaux entrants

sommes d'argent aux différentes personnes qui y ont investi en désactivant leurs plateformes sans avertir les investisseurs ou les rendre leur argent.

Cas illustratif d'escroquerie

Affaire Graine : Conduite au parquet des nommés **A.D, S.D, M.D.F, A.S, A. D, M.L.S et A.S** pour des faits d'association de malfaiteurs en relation avec une entreprise criminelle transfrontalière, escroquerie en bande organisée et/ou complicité (escroquerie à la graine), blanchiment de capitaux.

Dans la période de septembre 2018 au mois de janvier 2022, la Division Spéciale de Cybersécurité a reçu entre autres, quarante-et-une (41) plaintes formulées contre inconnus devenus les susnommés, pour escroquerie en bande organisée et ou complicité d'escroquerie à la graine.

Du résumé de celles-ci, les arnaqueurs contactent via WhatsApp les plaignants à partir de lignes étrangères et/ou via mails en se présentant comme un proche ou une ancienne connaissance et finissent par gagner leur confiance. De suite, ils leur proposent pour la plupart un business relatif à une activité d'exportation de graines (aubépines, argan, de Voacanga, moringa…) ou de sèves d'aloé Véra provenant du Mali, au profit d'une entreprise parisienne ou anglaise de fabrication de médicaments à base de plantes africaines, servant à lutter contre le cancer, le sida et le diabète entre autres maladies.

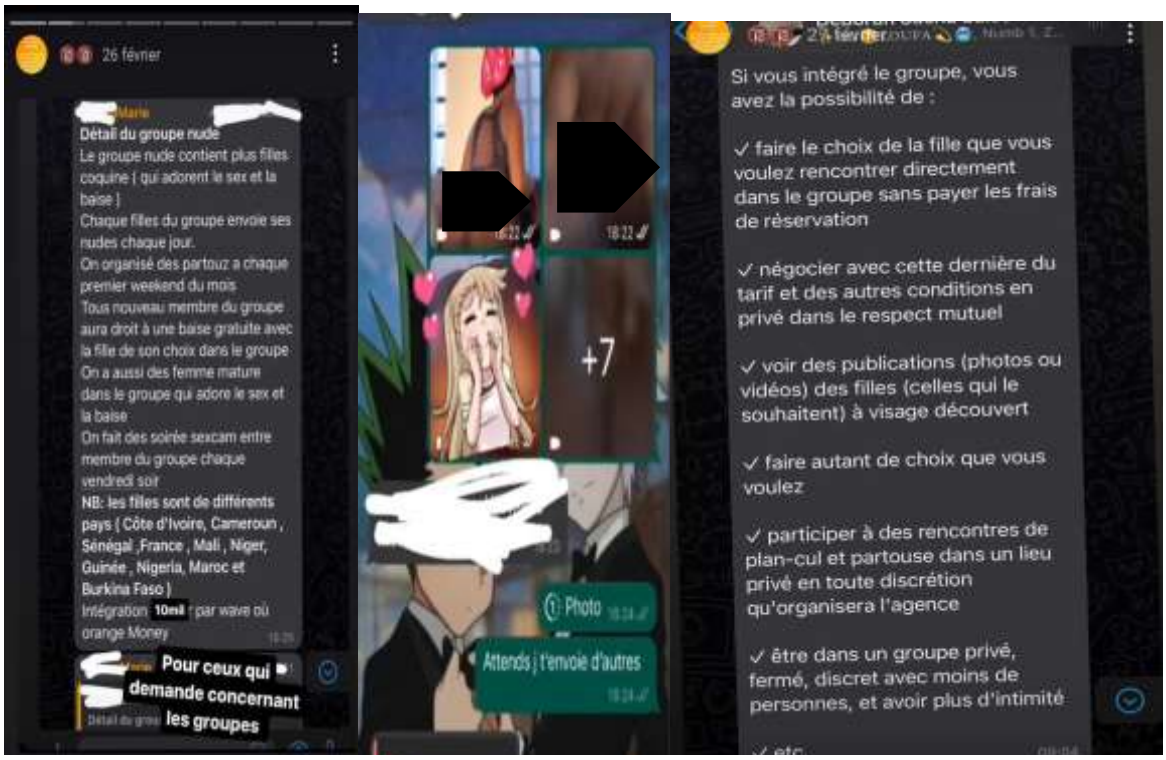
Consécutivement, les arnaqueurs mettent en rapport les plaignants avec leurs supposés associés, spécialisés dans l'achat de ces plantes africaines. Dès lors, une relation d'affaires portant sur l'achat des sachets de graines avec des prix unitaires déjà fixés débute. Sur ces entrefaites, plusieurs versements ont été effectués par les victimes à la demande de leurs interlocuteurs via les réseaux de transfert d'argent Orange money, Wave, Western Union, Ria, Money Gram sur des comptes ciblés

6.1.2. Proxénétisme et prostitution en ligne

Il s'agit d'une tendance récurrente au niveau des médias sociaux. A l'ère du numérique, le racolage sur la voie publique a été délaissé au profit d'une quête de clients à travers les réseaux sociaux. Ce type d'infraction est associé à l'atteinte à l'image étant donné que les données à caractère personnel telles que des images et/ou vidéos de plusieurs utilisateurs sont utilisés sur les sites internet ou pages de réseaux sociaux par des proxénètes ou entremetteurs. Cette forme de cybercriminalité n'a pas vu le jour avec internet ou les réseaux sociaux. Elle s'est adapté aux

technologies numériques au point de constituer des réseaux à grande échelle. Le proxénétisme ou la prostitution en ligne est très souvent précéder d'une usurpation d'identité. C'est-à-dire l'usage de faux profils pour attirer une certaine clientèle. C'est d'ailleurs ce qu'avance Niang (Homme, Lieutenant à la PNLC) « *c'est une pratique qui est devenu très courante aujourd'hui. La plupart des comptes sont des faux profils et ils utilisent des photos de plusieurs filles pour attirer une certaine clientèle* ».

Image 7 : Capture d'écran d'un compte de prostitution en ligne et de proxénétisme



Source : Capture d'écran d'un groupe de prostitution et de proxénétisme sur Instagram

6.1.3. La sextorsion

La sextorsion est une forme de criminalité numérique basée sur le chantage sous menace de divulgation de données à caractère personnel comme des images, enregistrements audio et/ou vidéos. Les cas de sextorsion les plus fréquents et qui sont rapportés au niveau des services de cybersécurité et/ou de lutte contre la cybercriminalité ont pour objectif une compensation financière. Cependant il y a des cas de sextorsion où l'objectif du cybercriminel est une compensation sous forme de faveurs sexuelles. Il demande à sa victime des faveurs sexuelles sous peine de divulguer ses vidéos et/ou images à caractère sexuel. Dans la plupart des cas de sextorsion, les cybercriminels utilisent des faux profils pour appâter leurs victimes. Ces dernières étant des hommes, les cyber-délinquants se font passer pour des femmes et avec de

l'ingéniosité ils arrivent à installer un climat de confiance au point que les victimes partagent des images en nue avec eux ou se mettent dans cette situation permettant de collecter des données à caractère personnel à travers des appels vidéo. Une fois cela fait, les cybercriminels passent aux menaces de divulgation sur internet. Ce qui constitue le principe de la sextorsion. C'est-à-dire cette coercition exercée par le cybercriminel sur sa victime.

Il existe tout de même d'autres cas de sextorsion où le cybercriminel, au lieu de faire preuve de ruse auprès de sa victime, obtient ses données à caractère personnel par le biais d'une tierce personne ou par un accès frauduleux à un système informatique.

Cas illustratif 1

La CDP a reçu une plainte de Monsieur A.B contre X pour collecte illicite de ses données personnelles. La personne mise en cause l'a menacé de publier lesdites données. Dans sa plainte, Monsieur A.B décrit ainsi les faits : croyant parler à une personne de genre féminin, il s'est trouvé piégé, lors d'un appel vidéo, avec un dénommé Coralie sur Instagram. Ce dernier a fait des captures et a mis son visage avec des images obscènes. La personne le menace de les publier s'il ne payait pas la somme de 350000fr.

Le mise en cause a, en effet, publié une vidéo de 2 mn que certains des amis de M. AB ont reçu. En application des articles 16-2c et 75 de la loi n°2008- 12 du 25 Janvier 2008 portant protection des données à caractère personnel, la CDP a transmis la plainte au Procureur de la République ainsi qu'à la Division Spéciale de la Cybersécurité (DSC) de la police pour enquête et suites à donner.

Source : Commission de protection des données personnelles (CDP)

Cas illustratif 2 :

Madame S.F.D a saisi la CDP d'une plainte contre « KOCC », relative à la publication de sa vidéo. Il ressort des informations transmises par la plaignante qu'un dénommé « KOCC », administrateur de la page Seneporno, aurait publié sa vidéo sans son consentement et lui aurait demandé de lui verser une somme d'argent de 300 euros. Ainsi, au regard de l'article 16 et 75 de la loi 2008- 12 du 25 janvier 2008 portant sur la protection des données à caractère personnel et des articles 363 bis, 431-19, 431-59 de la loi n°2016-29 du 08 novembre 2016 modifiant la loi n°65-60 portant Code pénal, la CDP a transmis la plainte au Procureur de la République et à la Division Spéciale de la Cybersécurité (DSC) de la police pour suites à donner

Source : Commission de protection des données personnelles (CDP)

6.1.4. Le piratage

Le piratage d'un compte de réseau social ou d'un site internet est une forme de cybercriminalité à laquelle les cybercriminels ont recours pour escroquer de l'argent en usurpant l'identité du propriétaire, pour du chantage, ou pour des revendications politiques. Que ce soit les gouvernements, les entreprises ou les particuliers, toutes les catégories d'utilisateurs de réseaux sociaux sont victimes de ce type de cybercrime. D'ailleurs, en Mai 2023, le gouvernement du Sénégal a été la cible d'une forme de piratage qui a paralysé tous les sites internet gouvernementaux. Cette attaque a été revendiqué par le groupe *Anonymous* sous couvert d'idéologie politique. Cette cyberattaque a été perpétrée durant une période d'instabilité politique et sociale. En soutien à la population sénégalaise, le groupe *ANONYMOUS* a piraté les sites internet gouvernementaux en exigeant que la démocratie sénégalaise soit laissée intacte.


RÉPUBLIQUE DU SÉNÉGAL

Un Peuple – Un But – Une Foi

COMMUNIQUÉ

Dakar, le 27 mai 2023

Le groupe de hackers « the Mysterious Team » a déclaré sur les réseaux sociaux avoir attaqué les sites web des services publics du Sénégal utilisant le domaine gouv.sn (géré par SENUM). Après vérification, il s'agit d'une Attaque DDOS.

Pour rappel, une DDOS est une attaque informatique qui consiste à submerger un réseau avec des quantités massives de trafic en saturant la bande passante de la ressource du site attaqué. Les grandes quantités de trafic lancées sur le site empêchent les utilisateurs légitimes d'accéder à l'application ou au service.

Sur les réseaux sociaux, les auteurs de l'attaque se font passer pour le groupe de hackers "Anonymous", connu pour avoir atteint d'autres infrastructures d'Etat dans le monde.

La SENUM SA chargée de la gestion du domaine Gouv.sn a mobilisé toute ses équipes pour permettre aux usagers de ces sites institutionnels d'accéder aux services en ligne dans les plus brefs délais.

Abdou Karim FOFANA
Ministre du Commerce, de la Consommation et des PME
Porte-parole du Gouvernement

6.2. Les infractions sur la bonne vie et la réputation

Comme pour leur désignation, les cybercrimes de cette nature ont trait à l'image et la réputation de l'individu. Internet et les réseaux sociaux ont faire naitre le concept de e-réputation, qui désigne la réputation d'une personne ou d'une entreprise dans le cyberespace. Elles sont constituées d'atteintes à l'image et à la vie privée de l'individu.

6.2.1. Collecte et diffusion de données à caractère personnel

Il s'agit d'une infraction très fréquente sur internet ou les réseaux sociaux qui consiste à recueillir par un moyen frauduleux des données à caractère personnel. Cette infraction implique une absence totale de consentement de la victime. Ce qui rend compte de son caractère frauduleux. Ce type de cybercrime attrait à la collecte, puis à la diffusion d'informations se rapportant à une personne. Ces informations peuvent être des vidéos, images, des sons ou autres par lesquelles la personne peut être directement ou indirectement identifiée.

6.2.2. Collecte et diffusion d'images pornographiques

Ce type de cybercrime est très fréquent sur les réseaux sociaux. Elles consistent à diffuser sur une ou des plateformes de réseaux sociaux des contenus (images, vidéos) jugés socialement et/ou juridiquement contraires aux bonnes mœurs. Dans certains cas de figure, elle est désignée sous l'appellation de « Revenge porn[35] », parce qu'étant le fruit d'un ancien partenaire ou amant. C'est d'ailleurs ce que Ndour (Lieutenant à la DPJ, homme) explique en ces termes : « *ce type d'infraction, je l'appelle l'infair play parce qu'après la séparation l'un des partenaires, mécontent de la situation, essaie de se venger en publiant lui-même ou en vendant les photos et vidéos de son partenaire* ». Ce type d'activité est devenu monnaie courant au Sénégal. La publication de vidéos à caractère sexuel est de plus en plus remarquable sur les réseaux sociaux surtout en période de fête. Que soit avant le Ramadan ou avant l'année scolaire avec le fameux « *teudj saison*[36] » ou que soit en période de fêtes durant laquelle les jeunes organisent des sorties et célébrations pendant lesquelles leurs ébats sexuels sont filmés et divulgués dans les réseaux sociaux. Ces vidéos d'ébats sexuels diffusés dans les réseaux sociaux sont désignées sous le vocable de « lomotif » en référence à l'application de montage de vidéos et d'images.

[35] Le « Revenge porn » est une vengeance par divulgation d'images à caractère pornographique.

[36] « Teudj saison » est une tendance des jeunes sénégalais à se rencontrer à la veille du Ramadan ou avant le début de l'année scolaire pour des besoins d'intimité ou pour des parties sexuelles.

Image 8 : Capture d'écran d'une diffusion d'images pornographiques

Source : Capture d'écran sur site internet https://www.koldanews.com/2020/05/27/scandale-cite-mixta-les-auteurs-du-lomotif-qui-a-secoue-la-toile-arretes-a1186354.html

Cas illustratif 1 : Affaire Sacré Cœur

Les nommés **J.B.F, A.Y.B.S, A.D et Y.K.R** ont été déféré au parquet pour Outrage public à la pudeur, attentat à la pudeur sur mineure de plus de 13 ans en bande organisée, collecte illicite, stockage et diffusion de données à caractère personnel, production, enregistrement, mise à disposition et transmission d'une image présentant un caractère de pornographie enfantine, par le biais d'un système informatique et/ou complicité.

La Division Spéciale de Cybersécurité (DSC) a reçu d'une personne anonyme, la publication sur les réseaux sociaux, d'une vidéo à caractère pédopornographique, propre à heurter la sensibilité et la moralité publique, qui implique une bande organisée d'élèves, supposés pensionnaires du collège d'enseignement privé Sacré Cœur de Liberté 5 et dont la victime serait une mineure. A la lecture de cette image avilissante qui laisse présager que la victime est une adolescente, on remarque clairement qu'elle a été contrainte physiquement à passer à l'acte indécent, sous les yeux menaçants d'autres jeunes.

Ce type d'infraction cybercriminelle est aussi commis par des cyber-délinquants désigner sous le vocable de brouteur[37]. Ceux-ci sont pour la plupart de nationalité étrangère.

6.2.3. Le cyber-harcèlement

Le cyber-harcèlement ou harcèlement en ligne est une tendance à harceler, intimider, menacer ou humilier une personne en utilisant les réseaux sociaux. Il se manifeste sous forme de remarques ou critiques désobligeantes, d'envois incessants de messages ou de diffusions d'informations dans le but de nuire à une personne. C'est une pratique de plus en plus courante, qui est caractérisée par le « Bodyshaming[38] ». Elle se manifeste également sous forme de critiques acerbes sur les traits physiques d'un individu. Elle est devenue une pratique très courante en raison de l'imposition des critères de beauté. Le cyber-harcèlement se manifeste également sous forme d'intimidation par le biais de d'insultes, de propos diffamatoires, et de diffusions de fausses nouvelles. Ce qui peut être synonyme d'attaques en vers un individu ou un groupe d'individus pour différentes raisons.

6.2.4. Usurpation d'identité numérique

Elle se caractérise par l'utilisation de données personnelles d'une autre personne sans son accord dans le but de nuire à sa réputation ou pour un motif purement pécuniaire. Il s'agit d'une pratique récurrente dans les réseaux sociaux où il est dénoté des milliers de faux comptes. La finalité peut aussi être de déstabiliser une institution ou une entreprise.

[37] Un brouteur est un arnaqueur opérant sur les réseaux sociaux. Sa technique consiste à séduire sa victime pour lui extorquer de l'argent, parfois même à la convaincre de se déshabiller devant une webcam puis de la faire chanter en menaçant de diffuser la vidéo.

[38] Le Bodyshaming est un terme anglais qui désigne la tendance à faire des remarques sur le physique d'une personne qui peut créer chez elle un mal-être.

Image 9 : capture d'écran d'une tentative d'escroquerie en ligne

Source : https://www.dakaractu.com/Usurpation-d-identite-Un-arnaqueur-se-fait-passer-sur-Facebook-pour-le-directeur-des-douanes-Abdourahmane-Dieye-en_a238733.html

Un individu se faisant passé pour le directeur général de la douane sénégalaise a créé une page sur le réseau social Facebook à travers laquelle il propose sous l'autorité du directeur une vente aux enchères de véhicules dont les frais d'inscription s'élèvent à 100000 FCFA.

6.2.5. Les infractions de presse

Il s'agit d'infractions commises par tous moyens de diffusion publique. Les informations peuvent donc transiter par les médias sociaux. A titre d'exemple nous pouvons citer les injures, les diffamations, la diffusion de fausses nouvelles, l'offense au Chef de l'Etat, etc.

6.2.5.1. La diffusion de fausses nouvelles

En ce XXIe siècle, les informations circulent à une vitesse exponentielle. Avec internet et les réseaux sociaux, n'importe qui peut passer une information à travers les technologies de l'information et de la communication. Une fois divulguée, l'information est très vite relayée au point d'être virale. Raison pour laquelle, il est coutume de retrouver dans les médias sociaux des informations de nature infondée. Ces dernières, au Sénégal, comme dans plusieurs nations du monde, se manifestent sous forme de diffusion de fausses nouvelles et rentrent dans le cadre des infractions catégorisées de cybercriminalité. Elles se manifestent sous forme de propagande, de désinformation et/ou de diffamation. La diffusion de fausses nouvelles, en tant qu'infraction cybercriminelle, consiste à une diffusion d'informations sur une personne, organisation et/ou sur une situation quelque conque qui ne soient aucunement fondées.

Image 10 : capture d'écran d'une diffusion de fausses nouvelles

Source : Tiktok, compte de Samy Dia

Sur ce compte Tiktok, un utilisateur sous une fausse identité, crée des frayeurs injustifiées en annonçant la mort de plusieurs célébrités sénégalaises alors que celles-ci sont bien vivantes.

Cas illustratif de diffusion de fausses nouvelles

Affaire P.I.G Conduite au Parquet du nommé P.I.G pour les faits de diffusion de fausses nouvelles et modification de données informatiques

Des personnes malintentionnées s'adonnent à des détournements de premières pages (« unes ») de quotidiens d'information très suivis au Sénégal, pour diffuser de fausses informations. Dans le cadre de sa mission quotidienne de veille, de recherches et de lutte contre la cybercriminalité, la Division Spéciale de Cybersécurité (DSC) a investi les sites d'information en ligne concernés, aux fins de démasquer les personnes qui se cacheraient derrière de faux comptes sur les réseaux sociaux, pour commettre leur forfait.

Les investigations techniques effectuées à cet effet ont permis de constater qu'un compte anonyme dénommé « L'Obs », créé le 07/07/2022, relaye de fausses informations, sous la bannière de Quotidien d'informations, qui peuvent être sources de confusion et de décrédibilisation des journaux visés. Il s'agit principalement du quotidien d'information « L'Observateur » et d'autres journaux, tel que « Le Quotidien ».

Dans le même ordre d'idées, des comptes sur les réseaux sociaux impliqués dans la diffusion de ces pages d'accueil falsifiées ont été identifiés.

Source : Division spéciale de la cybersécurité (DSC)

Source : capture d'écran https://www.youtube.com/watch?v=UyW7GN7oF9c

6.2.5.2. Injures et diffamations

Les injures et diffamations sont une catégorie des cybercrimes adaptée aux réseaux sociaux. Les injures sont des propos offensants tenus à l'égard d'une personne. Sur les réseaux sociaux, celles-ci sont exprimées généralement à travers des publications sous forme de vidéos, images ou textes. La diffamation quant à elle est le fait de diffuser des informations fausses à l'égard d'un individu, une organisation ou une institution.

Affaire B.D : Le nommé C.A.M a été déféré pour les faits de diffamation via les médias de diffusion de masse, diffusion de fausses nouvelles et offense au Chef de l'Etat.

Sur instruction, verbale du Procureur, de diligenter une enquête, suite à la tenue par le nommé C.A.M via plusieurs chaines YouTube lors d'un rassemblement politique, des propos qui sont de nature à diffamer et à offenser Monsieur le Président de la République.

Source : Division spéciale de la cybersécurité (DSC)

6.3. Les atteintes à l'Etat, à l'extrémisme et au terrorisme

Ces formes de criminalité sont connues dans l'espace physique. Elles ont été adapté à internet et au réseaux sociaux. Par le biais des technologies de l'information et de la communication, il est plus facile d'atteindre un grand public avec de simples messages sur les plateformes de réseaux sociaux. Que ce soit pour le recrutement ou pour l'endoctrinement, le cyberespace constitue un terrain idoine. Ces types de cybercriminalité se manifestent sous forme d'incitation à la violence à l'encontre d'une race, d'un Etat, une institution etc.

6.3.1. L'incitation à la violence

L'incitation à la violence est une forme de criminalité qui n'a peut-être pas vu le jour avec internet et les réseaux sociaux, mais elle est accentuée avec l'avènement de ces derniers. Au Sénégal, ce type de cybercriminalité intervient pour la plupart du temps lors des événements politiques ou lorsque se produisent des événements impliquant les milieux politiques. L'incitation à la violence est caractérisée par le fait que des messages sur les réseaux sociaux puissent être source de soulèvements et des heurts.

6.3.2. La Xénophobie

La Xénophobie est un sentiment d'opposition voire de haine envers les étrangers. Ces personnes caractérisées de xénophobe se justifient à travers leur nationalisme, c'est-à-dire leur volonté de préservation de leur 'authenticité'. La xénophobie se manifeste sous forme de messages haineux (vidéos, écrits…) sur groupe d'individus ou une communauté en raison de leur origine, race, religion etc.

La xénophobie est définie par la législation sénégalaise en ces termes :

> Est raciste et xénophobe en matière des technologies de l'information et de la communication : tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes[39]

Même si ce n'est pas une forme de cybercriminalité très fréquente dans le cyberespace sénégalais, il n'en demeure pas moins que des sentiments de nature xénophobe sont aujourd'hui observables. Ces derniers sont à l'endroit de la communauté guinéenne résidant au Sénégal. Ces messages sont pour la plupart du temps partagés à travers le réseau social Tiktok. Cette situation s'est d'autant plus manifestée durant la coupe d'Afrique des nations (CAN) de l'année 2023 qui s'est déroulée en Côte d'Ivoire entre janvier et février 2024.

D'ailleurs un tiktokeur[40] très suivi manifeste ce sentiment en ces termes « dagno wara guéné ndéye ndéring[41] yeup deuk bi ». (Tons, homme, 37 ans) Autrement dit « on doit expulser tous les guinéens de notre pays ».

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

[40] Un tiktokeur est un créateur de contenu sur le réseau social tiktok

[41] Ndéring est une désignation péjorative pour qualifier les peuls de la Guinée

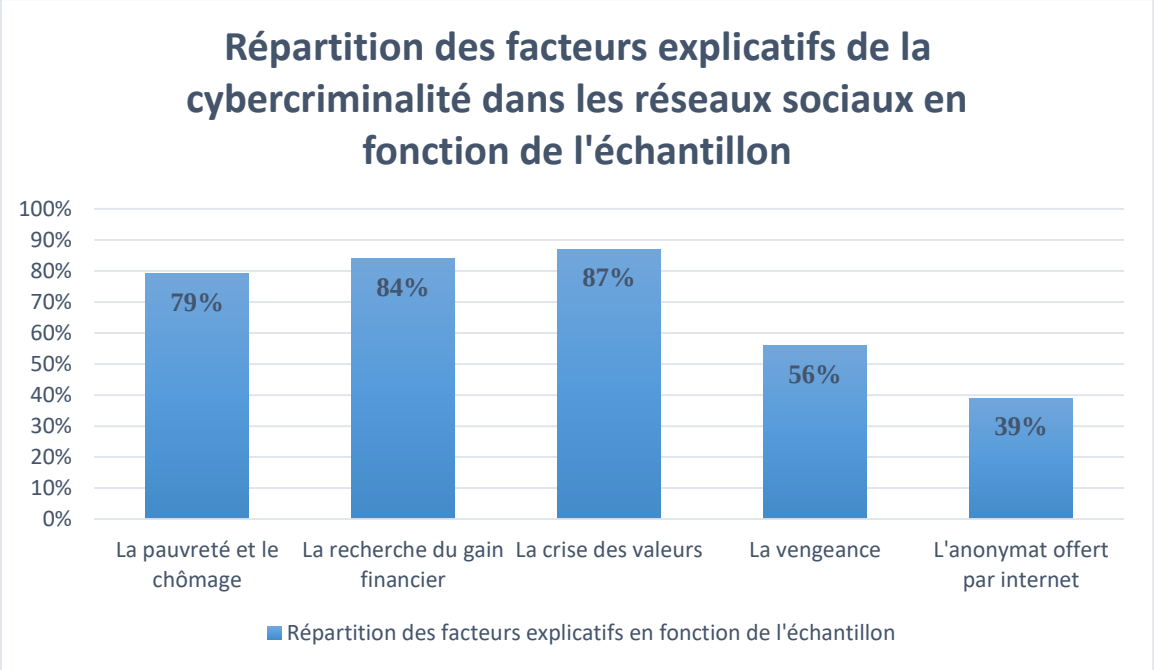
Chapitre 7 : Les facteurs explicatifs de la cybercriminalité sur les réseaux sociaux et les profils des cybercriminels et des victimes au Sénégal

Après que nos enquêtes nous ont permis de faire la typologie des cybercrimes dans les réseaux sociaux et même temps leur classification en différentes familles, nous pouvons maintenant parler des facteurs explicatifs de la cybercriminalité dans les réseaux sociaux. Parler directement des causes sans pour autant procéder à cette classification des cybercrimes sur les réseaux sociaux manquerait de pertinence dans la mesure où nous retrouvons sur les plateformes d'échanges sociales différents types de cybercriminels avec des motivations bien spécifiques, même si dans certains cas de figure elles demeurent les mêmes. Les facteurs explicatifs de la cybercriminalité dans les réseaux sociaux sont évoqués soit comme étant d'une initiative individuelle, soit de facteurs extérieurs à l'individu.

A la différence du milieu social physique dont les normes et conduites sociales paraissent un peu plus rigide, le cyberespace quant à lui n'est pas un système social aussi bien articulé. Chaque élément du système utilise les technologies numériques et leurs possibles selon ses priorités et possède sa propre dynamique.

7.1. Les facteurs explicatifs de la cybercriminalité dans les réseaux sociaux au Sénégal

Graphique 21 : Répartition des facteurs explicatifs de la cybercriminalité dans les réseaux sociaux en fonction de l'échantillon d'étude



Source : enquête de terrain Diouf Septembre 2023

7.1.1. La recherche du gain financier

L'idée selon laquelle la société fonctionne selon l'approche de Charles Darwin, qui met en avant la théorie de la sélection naturelle[42], apparait avec Herbert Spencer dont les travaux permettent de ne plus focaliser l'explication du phénomène criminel sur les conditions physiques de l'individu ou sur son anatomie, mais plutôt sur la vie sociale ou l'organisation sociale. C'est pourquoi l'idée d'un darwinisme social a été mis en avant pour comprendre le comportement de l'individu en société ou au sein du groupe social. D'ailleurs Martine Kaluszynski s'inscrit sur cette même logique en disant : « *la société est un organisme soumis aux mêmes lois que les organismes vivants. La réalité humaine n'est qu'une lutte incessante dont l'issu naturelle est la survie du plus apte* ». (Kaluszynski, 2005)

Ce darwinisme social permet d'étayer cette idée selon laquelle les cybercriminels se lancent dans la cybercriminalité dans les réseaux sociaux à la recherche du gain financier. Les utilisateurs des réseaux sociaux vont se lancer dans une lutte où chacun va mettre en avant ses besoins et aspirations dans ce milieu social virtuel qu'est le cyberespace.

C'est pourquoi ces individus, catégorisés comme cybercriminels ou cyber-délinquants, vont utiliser les technologies numériques, en l'occurrence les réseaux sociaux, dans leurs interactions avec les autres utilisateurs pour avoir du profit en utilisant des méthodes qualifiées d'illégales.

Par ailleurs, c'est que Erving Goffman avance en ces termes :

> Ici les contraintes de l'institution hospitalière sont prégnantes pour réhabiliter, sous la dure loi du principe de réalité ramenée à ses exigences impitoyables, les prosaïques expédients qui forment, par la force des choses, l'essentiel de cet usage populaire de la rationalité : la débrouillardise qui investit les fins de l'institution pour en faire des moyens de réalisation de ses propres fins, la fronde calculée, la lucidité modeste, la révolte prudente, la tolérance amusée à l'égard de la prétention des savants et des puissants, vertus à demi résignées seulement de ceux qui subissent, tous ces usages modérés de l'intelligence sont le fait d'hommes apparemment démunis devant une légitimité imposée du dehors, qui luttent avec leurs seules ressources pour survivre, sauvegarder un minimum de liberté et de dignité et glisser leur volonté de bonheur dans les failles d'une organisation qui n'est pas facile pour eux. Le « mauvais esprit » des chambrés, des prisons, des internats, des fabriques, des usines de montage à la chaîne, et aussi des malades, c'est une certaine revanche de l'humanité brimée qui se défend par le refus contre l'unilatéralité des idéologies dominantes ». (Goffman, 1968)

[42] La théorie de la sélection naturelle de Charles Darwin met en avant l'idée selon laquelle les individus les plus prompts à s'adapter à leur environnement sont ceux-là qui sont les plus aptes à survivre.

Ceux-là qui sont étiquetés comme cybercriminels ou cyber-délinquants sont ceux qui se servent de la cybercriminalité pour exister. C'est-à-dire gagner leur vie. Comme le dit Goffman, « *ils font glisser leur volonté de bonheur dans les failles d'une organisation qui n'est pas facile pour eux* ». Ils ont recours aux pratiques cybercriminelles parce qu'elles leur permettent de subvenir à leurs besoins, étant donné que la structure de l'organisation sociale à laquelle ils appartiennent ne leur permet pas de s'épanouir ou ne leur en offre pas la possibilité.

Dans un contexte social où l'argent ou la richesse est de plus en plus mis en avant ou peut déterminer le statut social, il est évident que les individus pour qui l'organisation sociale n'est pas facile, pour continuer dans la logique de Goffman, vont se servir des failles et/ou des possibilités qu'offrent internet et le cyberespace. Ces actes, auxquels ces individus ont recours, rentrent dans le cadre de l'anomique. Ce qui signifie bien évidemment que les cyber-délinquants se servent des conduites socialement et/ou juridiquement répréhensibles pour avoir cette reconnaissance sociale à travers l'argent.

De plus Karl Marx s'inscrit sur cette même logique par son analyse de la société à travers la lutte des classes. Cette parcellisation de la société en deux groupes (dominants et dominés), qu'il évoque, est une des causes des inégalités sociales et économiques, dont la pauvreté est interprétée comme un des facteurs permissifs d'une « culture déviante ». La situation économique des cybercriminels fait qu'ils cherchent en la cybercriminalité dans les réseaux sociaux une façon de sortir de leur état de précarité.

Qui plus est, si l'on se réfère à l'analyse durkheimienne du suicide en utilisant le concept de défaut de régulation, on parvient à cette conclusion selon laquelle le passage à l'acte cybercriminel est une façon d'obtenir l'ascension sociale qui est synonyme d'intégration sociale. Ceci s'explique par le fait que c'est le statut social qui détermine la place de l'individu au sein de la société ou du groupe social et que ce même statut social est pour la plupart du temps déterminé par le pouvoir d'achat de l'individu. Par conséquent, les cybercriminels sont ceux qui sont caractérisés par ce défaut d'intégration que Durkheim évoque dans son argumentaire du fait de leur situation financière. Ceux-là même vont se servir des activités cybercriminelles dans les réseaux sociaux pour avoir ce pouvoir économique et par-là avoir une reconnaissance sociale.

Donc le passage à l'acte cybercriminel est une façon de matérialiser son existence, parce que le cyber-délinquant utilise le cybercrime exister et échapper à la « mort sociale ». Les activités

cybercriminelles lui permettent, à travers le profit qu'il fait, de subvenir à ses besoins mais aussi d'exister socialement.

7.1.2. La crise des valeurs

La crise des valeurs qui est évoquée ici comme cause ou facteur explicatif de la cybercriminalité dans les réseaux témoignent de ce que Emile Durkheim a appelé le dysfonctionnement social. Ce dernier évoque cet état de fait où les structures sociales et les normes qui y s'appliquent ne font plus office de régulateur du comportement social chez certains individus. Aux différents cybercrimes dans les réseaux sociaux que nous retrouvons au Sénégal, l'idée d'une crise des valeurs sociétales que promeuvent les structures sociales telles que la famille, l'école ou encore la religion est très mise en avant. Ces structures sociales peuvent être interpréter soit comme des contraintes définissant les conduites individuelles, soit comme des conditionnements incitant à la reproduction de pratiques socialement acceptées.

Dans le mesure où le processus de socialisation au sein de ces structures sociales n'est plus assuré, il est évident aussi que la reproduction de pratiques socialement acceptées ne peut l'être non plus. Il est par conséquent clair que la cybercriminalité dans les réseaux sociaux au Sénégal, dans ses différentes formes, laisse apparaitre des conduites qui ne sont pas du tout conformes au contexte social sénégalais, si l'on prend en compte les considérations sociales et religieuses qui sont évoquées comme caractéristiques de la société sénégalaise.

Le défaut de régulation issue de l'analyse durkheimienne du suicide rend compte de cet état de fait selon lequel la cybercriminalité dans les réseaux sociaux s'explique par la crise des valeurs sociales. Et qui dit valeurs morales et sociales, parle de système de régulation des comportements sociaux.

Les valeurs sociales véhiculées, à travers les structures sociales telles que la famille, l'école, les unités de socialisation de l'individu de manière générale, deviennent inopérantes ; donc ne parviennent plus à jouer leur rôle de régulateur du comportement humain, surtout dans un environnement dont les réalités ne sont pas les mêmes que le milieu social physique.

7.1.3. L'anonymat offert par internet

Le développement des technologies de l'information et de la communication est accompagné d'une diversité des moyens et techniques permettant de garantir l'anonymat dans les réseaux informatiques d'une manière générale et dans les réseaux sociaux particulièrement. En France, la Commission nationale de l'informatique et des libertés (CNIL) définit l'anonymisation comme *« un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre*

impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible » (CNIL, 2020)

Il existe plusieurs techniques permettant l'anonymisation sur les réseaux sociaux. Bien que l'objectif soit également de respecter la vie privée des personnes, l'anonymisation est aussi utilisée par les cyber-délinquants à des fins criminelles. En effet, ces outils divers et performants permettent aux cyber-délinquants d'opérer parfois en toute liberté étant donné qu'il devient difficile voire impossible dans certains cas pour les services de contrôle et de lutte contre la cybercriminalité de procéder à l'identification et à la traque des cybercriminels.

Internet, dans sa généralité, offre bien des possibilités à ses utilisateurs, en particulier quand ils utilisent les réseaux sociaux. Avec la technologie VPN (virtual private network ou réseau privé virtuel en français), qui offre aux utilisateurs d'internet en général et des réseaux sociaux en particulier la capacité de choisir ou de changer sa géolocalisation. Cette technologie est souvent utilisée quand l'utilisation d'internet est restreinte, ou simplement pour passer inaperçu.

L'utilisation de cette technologie est à la portée de tous les utilisateurs d'internet et des réseaux sociaux. Pour se faire, l'utilisateur choisit un pays parmi une liste proposée, ainsi tout le trafic issu de son appareil (smartphone, ordinateur) sera décelé comme originaire du pays choisi sur le VPN au lieu du véritable pays. Cette pratique permet aux internautes de contourner les restrictions d'internet ou de rester simplement anonyme.

A cela s'ajoute la possibilité d'anonymisation qu'offrent les réseaux sociaux. Cela consiste à les utiliser tous en étant anonyme. Même s'il existe ce qu'on appelle l'empreinte numérique, qui regroupe les traces que l'utilisateurs laisse à chaque connexion sur internet, les cybercriminels ont ce sentiment d'être anonyme dans le cyberespace. Ce qui rend les facteurs juridiques ou pénales de dissuasion inopérantes.

Cet anonymat peut favoriser chez l'utilisateur de réseaux sociaux ce qu'on appelle en psychologie sociale la désindividuation. En psychologie sociale, la théorie de la désindividuation s'explique par le fait que l'immersion de l'individu au sein d'une foule ou d'un groupe social peut entrainer une perte d'identité de soi, pour laisser finalement la place à un comportent représenté par le groupe.

Appliquée à la cybercriminalité dans les réseaux sociaux, cette théorie met en relief le fait qu'en l'absence de possibilité d'identification, favorisé par l'anonymat offert par internet, l'utilisateur

de réseaux sociaux ou le cyber-délinquant se retrouve dans une situation où la commission d'acte socialement et/ou juridiquement répréhensible lui est facilitée.

De plus, le cybercriminel est aussi dans une situation où les facteurs de dissuasion du milieu social physique ne peuvent plus s'appliquer à lui étant donné qu'il ne peut être identifié, par conséquent pas du tout condamnable socialement et/ou juridiquement.

D'ailleurs la notion de « dissolution » que Spencer et Jackson ont mis en avant qui explique que sous l'effet d'un magnétiseur la personne consciente subit une régression, s'applique à la cybercriminalité dans les réseaux sociaux, étant donné que l'anonymat offert par internet peut agir comme magnétiseur chez l'individu. Cet anonymat crée chez le cybercriminel un sentiment de désindividuation qui, étant conscient qu'il ne serait pas identifié, donc pas puni, peut se lancer dans un processus de commission d'actes cybercriminels.

D'ailleurs ces propos Niang (Lieutenant à la PNLC, homme) abonde dans ce sens en disant « *le sentiment d'anonymat sur internet pousse les gens à commettre certaines exactions. Vous pouvez commettre des crimes en masquant votre position et votre identité* ».

L'anonymat va mettre en branle les systèmes de contrôle social et structurel aux quels l'individu fait face dans le milieu social physique. Cependant même si l'appareil de contrôle social devient inopérant dans le cyberespace, il est évident que les unités de socialisation auxquelles l'individu appartient telles que la famille, le groupe social, l'école, la religion ont intégré dans le processus socialisation des valeurs sociales et morales qui devraient agir comme régulateur du comportement humain.

C'est pourquoi, se limiter à expliquer le passage de l'acte cybercriminel chez l'individu à travers des facteurs sociaux et structurelles, revient à le réduire à l'état d'agent dont le comportement relève d'une succession de contraintes sociales et structurelles. Au-delà de l'influence du déterminisme social et structurel, il est nécessaire de mettre en avant le choix individu dans le passage à l'acte cybercriminel.

D'ailleurs c'est ce que Norbert Elias explique dans sa métaphore du jeu de carte. Cette dernière met en lumière le fait que des individus disposant des mêmes cartes lors d'une partie de jeu, ne joue pas de la même manière. A travers cette métaphore de Elias, on remarque clairement l'intention, le choix de l'individu qui guide chacune de ces actions.

7.1.4. La vengeance ou le règlement de compte

La vengeance est cet état de fait qu'un individu, se sentant blessé par un autre, décide de reproduire ce même sentiment de blessure voire même plus. En ce qui concerne la cybercriminalité dans les réseaux sociaux, la vengeance comme facteur explicatif de la cybercriminalité dans les réseaux sociaux, intervient comme indiqué plus haut lors qu'une relation (amicale, amoureuse, professionnelle) s'achève dans un contexte qui n'est pas du tout amical pour les individus concernés. C'est après friction, qu'intervient ce moment l'individu se sert des données à caractère personnel à sa disposition pour causer du tort à son ancien partenaire en les publiant ou lui faisant du chantage. Cette situation est désignée sous l'expression de « Revenge porn » quand des données personnelles à caractère sexuel sont utilisées.

Les technologies de l'information et de la communication (TIC) en général et les réseaux sociaux en particulier sont aujourd'hui utilisés comme outil de règlement de compte. Très souvent, ce règlement de compte est une affaire politique où les hommes politiques ou différents camps se lancent dans des guerres de décrédibilisation. Ces dernières se font pour la plupart du temps à travers des posts[43] diffamatoires ou par le biais de la divulgation d'informations relatives à des données à caractère personnel.

Ce genre d'action touche principalement les infractions cybercriminelles et sont généralement définies comme des atteintes à l'image, à la réputation. Ce qui fait qu'aujourd'hui, nous retrouvons l'utilisations des données à caractère personnel comme moyen de décrédibilisation dans le milieu politique sénégalais.

Le règlement de compte se fait aussi sous la forme d'injures sur les réseaux sociaux ou sous forme de cyber-harcèlement.

7.1.5. La pauvreté ou le chômage

L'explication de la criminalité à travers les facteurs économiques n'est pas anodine. Depuis que les sciences sociales et les autres disciplines ont commencé à s'intéresser aux phénomènes criminelles, bon nombre d'auteurs et de chercheurs ont misé leurs explications de ce phénomène sur les facteurs économiques et sociales au point de parler de facteurs criminogènes pour évoquer les conditions socioéconomiques comme influences directs sur le passage à l'acte déviant. D'ailleurs c'est constat que fait Kandé (Commissaire à la DSC, homme) en parlant la

[43] Un post est une publication sur un réseau social. Elle peut être un texte, une image, une vidéo etc.

situation de précarité quand il évoque les profils cybercriminels. Il dit en ces termes « *nous avons d'anciens étudiants en informatique au chômage* ». Ces cybercriminels qui sont animés par la pauvreté et le chômage se lancent les plus dans les activités telles l'escroquerie, la sextorsion etc. Par ailleurs, pour certains cybercrimes, la motivation des cyber-délinquants se trouvent être le gain financier. Ce qui conforte l'évocation de la pauvreté comme facteur explicatif de la cybercriminalité dans les réseaux sociaux.

7.1.6. La cybercriminalité dans les réseaux sociaux comme un rappel aux valeurs sociales pour les utilisateurs.

Analyser l'activité cybercriminelle du point de vue du cyber-délinquant donne sens à son action et par conséquent apparait la décision délibérée de celui-ci de passer à l'acte. Pour des cas de cybercriminalité dans les réseaux sociaux au Sénégal tels que la diffusion d'images pornographiques, certains cybercriminels justifient leurs actes comme étant un rappel aux valeurs sociales pour la population particulièrement les jeunes. D'ailleurs, c'est ce que cet illustre utilisateur, qui s'est autoproclamé juge, explique dans les live[44]. Pour lui, la divulgation de données à caractère personnel est « *une façon d'inciter les gens, surtout les filles, à ne pas se filmer ou d'envoyer des vidéos nues à leurs copains* ». (Tiktokeur, homme) C'est une façon pour lui d'inciter les gens à être pudiques et à se comporter selon les codes de la société. Par ailleurs, le fait de se proclamer « juge » est une façon de juger les comportements sociaux et d'en déduire ceux qui sont raccords avec son idéal social. Ce que Gresham Sykes et David Matza (Sykes & Matza, 1957) appellent des mécanismes de justification et rationalisation dont le cybercriminel fait usage afin de se dédouaner d'une culpabilité et de donner du sens à son action. Paul Cromwell et Quint Thruman définissent la neutralisation comme étant « *des mécanismes de justification et de rationalisation facilitant les comportements qui violent les normes ou contreviennent aux attitudes exprimées, permettant ainsi aux individus d'atténuer ou d'éliminer la culpabilité qui devrait en résulter et de faire face aux éventuelles accusations* » (Cromwell & Thruman, 2003). Ils poursuivent en disant que la neutralisation « *protège l'individu de l'auto-culpabilisation et du blâme des autres (…). L'individu peut rester attaché au système de valeurs de la culture dominante tout en commettant des actes criminels sans éprouver la dissonance cognitive qui serait autrement attendue »* (Cromwell & Thruman, 2003)

[44] Un Live est une transmission vidéo en direct sur les réseaux sociaux qui peuvent se faire individuellement ou avec un groupe de personnes.

Des justifications de ce cybercriminel nous relevons deux (2) techniques de neutralisation de Sykes et Matza (Sykes & Matza, 1957) que sont :

- Le déni de victime est une façon de faire porter la responsabilité de son crime à sa victime. Par ailleurs, c'est ce que fait ce cybercriminel en faisant porter la responsabilité à ses victimes en disant que « *si ces dernières ne s'étaient filmées nus, il n'aurait pas à ça* ». (tiktokeur, homme) De plus, une partie importante des internautes qui le suivent partagent sa vision en incriminant à leur tour les victimes. Ce qui conforte le cybercriminel dans la position et le dédouane de la culpabilité qui devait découler de son acte.
- L'invocation des grandes loyautés : de ses justifications, le cybercriminel évoque aussi le fait que son acte se justifie par une volonté de pousser les individus à plus de pudeur. Pour Sykes et Matza, l'invocation des grandes loyautés est le fait de présenter le comportement criminel comme servant une cause d'importance supérieure à la règle enfreinte. Ce qui est le cas avec ce cybercriminel.

Ces techniques de neutralisation sont une façon pour le cybercriminel de rationaliser son action, c'est-à-dire de lui donner du sens. Cet acte qui, selon le droit sénégalais et par extension la société sénégalaise, relève purement du criminel, se trouve être légitime du point de vue du cybercriminel parce qu'ayant du sens. Et le sens dans ce cas de figure est de pousser les individus à adopter des attitudes conformes aux normes et réalités sociales.

Cette justification du cyber-délinquant confère à la cybercriminalité dans les réseaux sociaux un caractère normal et utilitaire.

7.1.7. Les récits de vie des victimes

Les récits sont des témoignages des personnes racontant leur histoire. Recueillir des récits de vie pour notre problématique de recherche telle que la cybercriminalité dans les réseaux sociaux nous permet, à travers ces témoignages, d'avoir des éléments de réponses à nos différentes interrogations. Ces récits de vie nous permettent aussi d'avoir un aperçu sur certaines formes de cybercriminalité dans les réseaux sociaux.

7.1.7.1. Récit de vie n°1 (homme, 25ans, étudiant)

Le problème que j'ai eu sur les réseaux sociaux s'est passé sur Instagram. Un jour, en me connectant sur mon compte, j'ai reçu un message d'une fille se faisant appeler Merveille je ne sais plus comment. J'ai répondu à son message et après on a discuté. On a échangé des informations sur nos vies.

Particulièrement sur quels points ?

On a parlé de ce qu'on fait dans la vie. Elle m'a dit si je me rappelle bien qu'elle était infirmière et moi je l'ai dit que je suis commerçant. On a continué à discuter et à un moment donné elle a commencé à me draguer en me posant des questions du genre si j'étais célibataire, ma nationalité etc. Naïf que je suis, je répondais à ses avances. Elle m'a demandé si j'avais déjà eu une copine blanche et j'ai répondu non. Après elle a voulu savoir si j'aimais les filles blanches. Je l'ai dit que je ne savais pas.

Après on a commencé à s'envoyer des messages sexy et elle m'envoie son numéro et moi aussi je l'ai envoyé mon numéro. On a continué la discussion sur WhatsApp. Elle m'a appelé en vidéo et elle était complétement nu et c'est là que j'ai commis l'erreur de ma vie.

Pourquoi dites-vous cela

Parce que j'ai fait ce qu'elle voulait. Elle m'a envoyé une vidéo à la fin de l'appel vidéo en me menaçant de partager la vidéo avec mes amis d'Instagram. Il a dit qu'il allait aussi publier la vidéo sur internet. Je l'ai supplié de pas publier la vidéo. C'est là qu'il m'a avoué que c'est à un homme que je parlais. Il m'a demandé de lui envoyer 40000 francs sinon il allait publier la vidéo et j'ai commencé à avoir peur. J'ai déjà vu des vidéos de personnes partagées sur les réseaux sociaux. Je ne voulais pas que ça m'arrive. J'ai négocié avec lui jusqu'à 15000 francs et j'ai envoyé l'argent par orange money.

Pourquoi n'avez-vous pas porter plainte ?

Sincèrement tout ce que je voulais c'est préserver ma réputation. Je viens d'une famille très religieuse et si les gens étaient au courant je pourrais pas le supporter et ma famille aussi.

Que s'est-il passé après que vous lui avez envoyé l'argent ?

Il m'a laissé tranquille et j'ai bloqué son compte pour qu'il ne me contacte plus.

7.1.7.2. Récit de vie n°2 (Homme, 26 ans, chauffeur de Taxi)

J'ai perdu de l'argent sur Petonpay parce que je croyais c'était un investissement sûr et j'avais confiance à la personne qui m'a parlé de ça. C'est pourquoi je n'ai pas hésité à investir mon argent. A l'époque j'étais étudiant et j'avais mis un peu d'argent de côté grâce aux petits boulots que je faisais à côté.

Qu'est-ce qui vous a poussé à investir votre argent ?

C'est une personne de confiance qui m'a parlé de ça. Elle m'a expliqué comment ça marche, les opportunités. Elle m'a dit ce qu'elle gagne beaucoup d'argent avec ça et que je devais aussi investir. Comme je venais d'arrêter mes études et que je voulais gagner de l'argent, j'ai dit pourquoi pas. J'ai pris l'argent que j'ai mis de côté et j'ai investi.

Comment se faisait l'investissement ?

Il y avait la possibilité de payer par wave ou orange money. On avait des groupes WhatsApp et ce sont les premiers membres qui nous expliquaient comment ça se passe. Dans les groupes, ils publiaient des vidéos de personnes qui ont gagner de l'argent à grâce à ça et des rencontres qu'ils organisaient. Ça m'a motivé. On m'avait dit que c'est un investissement sur le pétrole. On devait acheter des packs pour investir. Il y'avait plusieurs packs.

Au début je gagnais de l'argent et ça m'a poussé à investir plus. La plateforme a été fermée le jour où je voulais retirer mes bénéfices.

Combien avez-vous perdu ?

Je ne sais plus exactement ça doit être dans les cinquante (50000) francs

Qu'avez-vous fait quand cela s'est produit ?

Rien du tout ! j'ai laissé comme ça

Pourquoi n'avez-vous pas porté plainte ?

Je ne sais même pas.

7.2. Les profils des cybercriminels et des victimes

Pour chaque type de cybercrimes, il est possible de mettre en évidence le profil cybercriminel ou celui des victimes ou en tout cas les plus fréquents. Cependant, il est tout à fait possible de retrouver les mêmes profils pour plusieurs cybercrimes.

7.2.1. Les profils cybercriminels

Le critère sur lequel les agents des services de lutte contre la cybercriminalité s'accordent en ce qui concerne les profils cybercriminels est l'âge. À des exceptions près, « *la plupart des cybercriminels ont un âge compris entre 17 et 35 ans voire 45 ans* » (Kandé commissaire à la DSC). Par conséquent, l'analyse faite ici est que la cybercriminalité est activité criminelle dont les principaux individus qui s'y adonnent sont des jeunes, très souvent avec des motivations différentes.

Certains, pour ne pas dire une grande partie des cybercriminels, n'ont pas une très grande maitrise de l'informatique. Parce que la plupart des activités cybercriminelles que nous retrouvons dans les réseaux sociaux ne nécessitent pas ou presque pas de connaissances en informatique. Elles relèvent plus de l'ingénierie sociale et de capacités de manipulation des sentiments humains. Les cyber-délinquants arrivent à manipuler leurs victimes au point de le faire croire tout ce qu'ils veulent en s'appuyant le manque de méfiance ou l'insouciance des utilisateurs.

Comme profil cybercriminel, nous avons aussi, toujours selon les dires de Kandé (Homme, Commissaire à la DSC), « *d'anciens étudiants en informatique au chômage* ». Ce type de profil est très souvent retrouvé pour les cas de cybercrimes nécessitant certaines compétences en informatique.

Hormis cela, il y'a aussi des cybercriminels de nationalité étrangère, qui pour la plupart sont dans l'escroquerie, l'usurpation d'identité numérique, le piratage de compte, les sextorsions[45]. Certains parmi ces cybercriminels établissent leur quartier général à l'intérieur même du pays, dans des quartiers de la région de Dakar comme Ouakam, Foire, Mbao etc.

Tandis que d'autres cybercriminels opèrent de l'extérieur du Sénégal, c'est-à-dire dans la sous-région. On les retrouve plus dans des pays comme le Nigéria, le Bénin, le Burkina Faso, la Côte d'Ivoire, le Ghana etc. Certains citoyens (jeunes) de ces pays s'adonnent fortement à l'escroquerie au point qu'elle soit dénommée escroquerie à la nigériane pour désigner l'escroquerie sur la base de sentiments amoureux ou la sextorsion. L'escroquerie au sentiment est une pratique très répandue en Côte d'Ivoire. D'ailleurs, les cybercriminels qui s'adonnent à ce type de pratique sont désigné sous le vocable de brouteur. A l'aide de faux profils, ils contactent leurs victimes en se faisant passer pour des femmes. Ces brouteurs font croire à leurs victimes qu'ils sont amoureux d'eux pour pouvoir leur soutirer de l'argent ou en les menaçant de divulguer leurs images après que leurs victimes se soient montrées nues au cours de conversations en vidéo.

En somme, nous pouvons recenser différents profils cybercriminels. Cependant, il est possible de les classer en trois catégories : les cybercriminels par accident, les cybercriminels occasionnels et les cybercriminels par choix. Pour cette classification, nous nous sommes inspiré des travaux de Cesare Lombroso en Psychologie Criminelle. Les cybercriminels par

[45] La sextorsion est une forme de cybercriminalité basée sur du chantage sous menace de divulgation de données à caractère personnel (images, vidéos et/ou enregistrements audio) de nature pornographique.

accident sont ceux n'ayant aucun motif de satisfaction personnelle avant ou au moment de passer à l'acte. Tandis que les cybercriminels occasionnels sont ceux qui passent à l'acte dans l'immédiateté, en réaction à une situation. C'est le cas de ceux dont les actions ne sont motivées que par vengeance. Par contre, les cybercriminels par choix sont ceux qui font de la cybercriminalité une activité dont les motifs peuvent être financiers, idéologiques, passionnels etc.

Tableau 19 : Récapitulatif des profils de cybercriminels et des modes opératoires

Profil des cybercriminels	Modes opératoires courants	Description
Hackers individuels locaux	Piratage de systèmes, Escroqueries en ligne, Diffusion de logiciels malveillants	Ces individus exploitent leurs compétences techniques pour accéder illégalement à des systèmes informatiques, mener des arnaques en ligne ou propager des virus.
Groupes criminels organisés étrangers	Fraude par usurpation d'identité, Chantage numérique, Escroqueries sentimentales	Des réseaux, souvent originaires d'autres pays, opèrent depuis le Sénégal pour mener des arnaques complexes, notamment en se faisant passer pour des partenaires romantiques en ligne.
Employés malveillants	Vol de données internes, Sabotage de systèmes, Fraude interne	Des employés utilisent leur accès privilégié pour dérober des informations sensibles, perturber les opérations ou commettre des fraudes au sein de leur organisation.
Hacktivistes	Défiguration de sites web, Attaques par déni de service (DDoS), Propagation de messages idéologiques	Motivés par des causes politiques ou sociales, ces individus ou groupes mènent des attaques pour promouvoir leur agenda ou protester contre des institutions.
Cybercriminels opportunistes	Phishing, Arnaques aux faux investissements, Vente de produits contrefaits en ligne	Exploitant les tendances actuelles ou les crises, ces criminels lancent des campagnes de phishing ou proposent de faux produits pour tromper les victimes.

7.2.2. Les profils de victime

La particularité de la cybercriminalité dans les réseaux sociaux est que tout le monde peut se retrouver en position de victime. Que l'on soit utilisateur de réseaux sociaux ou non, il est possible d'avoir affaire à un cybercriminel, du fait de l'adaptation des technologies de l'information et de la communication à la commission d'acte criminel. Dans certains cas de figure, le niveau de conscience et l'hygiène cyber sont ce qui distinguent les utilisateurs des réseaux sociaux et peuvent les aident à ne pas être victime de certaines formes de cybercrimes.

Comme pour les profils cybercriminels, nous avons aussi un ou des profils de victime pour chaque cybercrime ou en tout cas la ou les catégories de personnes les plus touchées. Avec sa portée internationale, la cybercriminalité est une menace à laquelle tous les utilisateurs des réseaux sociaux sont confrontés. Même si certains utilisateurs de réseaux sociaux arrivent à s'en sortir, il n'en demeure pas moins qu'un très grand nombre d'individus soit touché ou impacté.

Les infractions sur les réseaux sociaux touchent un ensemble de victimes qui peut être catégorisé en fonction du sexe, de l'âge, de la catégorie socioprofessionnelle, de l'appartenance politique etc. Cette catégorisation dépend aussi en grande partie du type d'infraction au quel nous faisons face.

Pour des cybercrimes tels que les escroqueries, il n'y a pas vraiment de profil typique de victime, parce que tous les catégories d'utilisateurs de réseaux sociaux peuvent être touchées. Par exemple dans les plateformes d'investissement comme Tesco boutique ou Petron pay, parmi les personnes escroquées, nous retrouvons des étudiants, des commerçants, des fonctionnaires de l'Etat, qu'il soit homme ou femme. Sur les réseaux sociaux comme Facebook, les cybercriminels s'appuient sur la naïveté de leurs victimes en leur faisant croire qu'elles auraient un pactole à gagner en suivant leurs instructions.

Pour ce qui est des cas de sextorsion, même si nous retrouvons de femmes parmi les victimes, la majorité est composée d'hommes et pour la plupart du temps jeunes. Les victimes hommes sont plus importes parce qu'étant plus les proies des cybercriminels étrangers qui les contactent en se faisant passer pour des femmes. Ces derniers amènent leurs victimes à se dénuder pendant des appels vidéos pour ensuite les faire chanter.

Parmi les femmes victimes de sextorsion, nous retrouvons celles en couple dans une relation à distance. Dans le but de satisfaire leurs partenaires, ces femmes envoient parfois des images d'elles dénudées à ces derniers ou font des appels vidéos avec eux. Le cybercriminel, qui par

un moyen frauduleux obtient ces données à caractère personnel, procède à chantage sous menace de divulgation auprès de sa victime.

Pour les cas de collecte et diffusion d'images pornographiques, les hommes et les femmes sont tous autant touchés. Les victimes peuvent être de tout âge. Tout de même les femmes sont plus touchées par cette sous-catégorie qui est le Revenge porn. Cela consiste à publier des images ou vidéos d'une personne par vengeance. Cela arrive le plus souvent après une rupture. La remarque fait au niveau des services de lutte contre la cybercriminalité et à travers nos observations est que les femmes étaient principalement les victimes. « *Les images compromettantes de ces personnes sont partagées par leur entourage ou elles sont partagées en cas de perte de téléphone* ». Ndour (Homme, Lieutenant à la DPJ)

Pour les cas d'usurpation d'identité numérique, les personnalités publiques sont les plus touchées. Les cybercriminels utilisent la notoriété de ces personnes pour mieux berner leurs cibles. Dans le réseau social Facebook, bon nombre des faux comptes ont été signalés. Les utilisateurs derrières ces faux comptes se font passer pour des footballeurs internationaux sénégalais ou autres. Ils rentrent en contact avec leurs cibles en leur proposant de l'aide pour ensuite leur demander des sommes substantielles, après quoi ils auront la possibilité de les envoyer des sommes plus conséquentes.

Tableau 20 : Récapitulatif des profils de victimes et des types d'attaques courantes

Profil des victimes	Types d'attaques courantes	Description
Particuliers	Escroqueries en ligne, Chantage numérique, Vol de données personnelles	Les individus sont souvent ciblés par des arnaques via e-mails ou réseaux sociaux, des menaces de divulgation d'informations sensibles ou des vols d'identité.
Entreprises	Fraude au président, Rançongiciels, Espionnage industriel	Les entreprises peuvent être victimes de fraudes impliquant des transferts de fonds illégitimes, de logiciels malveillants bloquant l'accès aux données ou de vols d'informations confidentielles.
Institutions financières	Piratage de systèmes, Fraude bancaire en ligne, Phishing ciblé	Les banques et autres institutions financières sont exposées à des attaques visant à accéder illégalement aux comptes clients ou à détourner des fonds.
Organismes gouvernementaux	Attaques DDoS, Défiguration de sites web, Vol de données sensibles	Les agences gouvernementales peuvent subir des perturbations de services en ligne, des modifications non autorisées de leurs sites ou des fuites d'informations confidentielles.
Utilisateurs de services mobiles	Escroqueries par SMS, Applications malveillantes, Fraude au paiement mobile	Les utilisateurs de téléphones mobiles sont vulnérables aux messages frauduleux, aux applications contenant des logiciels espions ou aux arnaques liées aux transactions mobiles.

Tableau 21 : Corrélation entre le niveau d'étude des enquêtés et le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux

		Niveau d'étude des enquêtés	Etre victime ou non de cybercriminalité dans les RS
Niveau d'étude des enquêtés	Corrélation de Pearson	1	-,022
	Sig. (bilatérale)		,832
	N	100	100
Etre victime ou non de cybercriminalité dans les RS	Corrélation de Pearson	-,022	1
	Sig. (bilatérale)	,832	
	N	100	100

La corrélation de Pearson entre le fait d'être victime de cybercriminalité dans les réseaux sociaux et le niveau d'étude de nos enquêtés est de -0,022. Cela indique une très faible corrélation entre le niveau d'étude des enquêtés et le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux. En outre, le fait que la valeur de la corrélation soit proche de zéro suggère qu'il n'y a pas de relation significative entre ces deux variables. De ce fait, on peut dire qu'il n'y a pas de lien significatif entre le niveau d'étude des enquêtés et le fait d'être victime de cybercriminalité dans les réseaux sociaux. D'ailleurs, les propos de M. Bakhoum (Homme, agent de la CDP) en sont une illustration. Il avance lors de l'entretien « *nous recevons de plaintes venant de plusieurs catégories de personnes, des personnalités, des cadres, des étudiants etc. Tout le monde peut être victime de cybercriminalité* ».

Tableau 22 : Corrélation entre le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux et le sexe des enquêtés

Corrélations

		Sexe des enquêtés	Etre victime ou non de cybercriminalité dans les RS
Sexe des enquêtés	Corrélation de Pearson	1	,162
	Sig. (bilatérale)		,107
	N	100	100
Etre victime ou non de cybercriminalité dans les RS	Corrélation de Pearson	,162	1
	Sig. (bilatérale)	,107	
	N	100	100

La corrélation de Pearson entre ces deux variables est de 0,162. Étant donné que la corrélation est positive, cela suggère une relation linéaire positive faible entre le sexe des enquêtés et le fait d'être victime ou non de cybercriminalité dans les réseaux sociaux. Cependant, cette corrélation est relativement faible, ce qui signifie que le sexe des enquêtés a une influence limitée sur le fait d'être victime de cybercriminalité dans les réseaux sociaux. Cette influence limitée est justifiée par le fait pour certains cybercrimes, on peut retrouver une plus forte probabilité d'un groupe (homme, femme) à être victime.

Chapitre 8 : La cybercriminalité dans les réseaux sociaux au Sénégal : représentations, réactions et répercussions sociales

8.1. Les représentations sociales sur la cybercriminalité dans les réseaux sociaux au Sénégal

Pour aborder les représentations sociales sur la cybercriminalité dans les réseaux sociaux, il convient d'emblée de procéder à la définition de celles-ci pour saisir ce en quoi elles consistent réellement. Les recherches sur les représentations sociales sont multiples et diverses de par les disciplines et par les auteurs. Néanmoins, nous allons nous appesantir sur quelques auteurs dont les approches mettent en évidence le sens des représentations sociales.

Pour comprendre les représentations sociales, la définition de celui qui en est considéré comme le théoricien semble idoine. Serge Moscovici définit la représentation sociale comme « *une manière d'interpréter le monde et de penser notre réalité quotidienne, une forme de connaissance sociale que la personne se construit plus ou moins consciemment à partir de ce qu'elle est, de ce qu'elle a été et de ce qu'elle projette et qui guide son comportement. Et corrélativement la représentation sociale est l'activité mentale déployée par les individus et les groupes pour fixer leurs positions par rapport à des situations, événements, objets et communications qui les concernent* » (Moscovici, 1984)

Denise Jodelet quant à elle définit la représentation sociale comme « *est une forme de connaissance socialement élaborée et partagée ayant une visée pratique et concourant à la construction d'une réalité commune à un ensemble social. Elle n'est pas le simple reflet de la réalité, mais fonctionne comme un système d'interprétation de la réalité qui organise les rapports entre les individus et leur environnement et oriente leurs pratiques* ». (Jodelet, 1997)

Ces définitions de Moscovici et Jodelet permettent de comprendre la teneur des représentations sociales. Tous les deux voient en elles des connaissances socialement partagées par le groupe social sur un objet ou une situation quelconque, qu'il interprète en fonction de leur système social de référence.

De plus Jean Claude Abric s'inscrit dans ce continuum en définissant la représentation sociale comme « *une vision fonctionnelle du monde, qui permet à l'individu ou au groupe de donner sens à ses conduites, et de comprendre la réalité, à travers son propre système de référence, donc de s'y adapter et de s'y définir une place* ». (Abric, 1997)

De toutes ces définitions, deux éléments essentiels pour comprendre les représentations sociales sur la cybercriminalité dans les réseaux sociaux ressortent.

En premier lieu, il y a cet effet de caractérisation de la représentation sociale en une vision ou connaissance socialement partagée. Cette caractérisation rend compte de l'idée que les utilisateurs des réseaux sociaux ou internautes se sont de la cybercriminalité. Autrement dit, leur appréhension de la criminalité numérique.

En second lieu, il y a la compréhension de la réalité à travers son propre système de référence. Ce qui veut dire que, contextualiser à la cybercriminalité dans les réseaux sociaux, les internautes ou utilisateurs des médiaux sociaux vont se représenter ce phénomène à travers leurs modes de penser, d'agir et de sentir. Autrement dit, l'idée qu'ils se font de la cybercriminalité dans les réseaux sociaux dépend de leur groupe social d'appartenance, dans une certaine mesure de leurs structures sociales et leur processus de socialisation.

D'ailleurs, c'est dans cette perspective que s'inscrit cette définition de Roussiau et Bonardia. Ces derniers définissent la représentation sociale en ces termes : « *une représentation sociale est une organisation d'opinions socialement construites, relativement à un objet donné, résultant de communications sociales, permettant de maîtriser l'environnement et de l'approprier en fonction d'éléments symboliques propres à son ou ses groupes d'appartenance* » (Roussiau & Bonardi, 2001)

Ce qui fait en substance des représentations sociales des opinions socialement partagées par le groupe social sur un objet ou une situation. De ce fait, pour une problématique de recherche telle que la cybercriminalité dans les réseaux sociaux, il sera question de mettre en évidence les opinions communes qui s'y rapportent.

8.1.1. Impuissance face à la cybercriminalité dans les réseaux sociaux

S'agissant des représentations sociales sur la cybercriminalité dans les réseaux sociaux, l'appréhension majeure est la dangerosité du phénomène en question. Celle-ci se justifie par les conséquences ou répercussions que la cybercriminalité peut avoir non seulement sur l'individu, mais aussi sur la société en général. Ces conséquences se manifestent sur la vie privée et publique, sur les activités économiques et sur la stabilité politique et sociale.

Bien que les représentations sociales sur la cybercriminalité dans les réseaux sociaux ne soient pas quantifiables pour mesurer leur ampleur, mais leur appréciation permet tout de même de se faire une idée de la façon dont les utilisateurs appréhendent le phénomène. A travers nos

différentes données d'enquête, la remarque faite est que les internautes voient en la cybercriminalité un fait dont ils se sentent manifestement vulnérables et dans une certaine mesure sans défense. D'ailleurs c'est que M.D.F (Femme, comptable, 40 ans) avance en ces termes : « *C'est quelque chose de très dangereux qui peut détruire des personnes. Il gagne du terrain de jour en jour et il est difficile aujourd'hui d'échapper* »

Cela se justifie par le fait qu'il est aujourd'hui difficile d'en échapper vu l'avancée fulgurante des technologies numériques et des techniques et moyens cybercriminels. De plus la cybersécurité, dans certains États comme le nôtre, est en retard par rapport à la cybercriminalité.

8.1.2. La cybercriminalité à l'image de la société sénégalaise

Au-delà de cette représentation sociale sur la cybercriminalité dans les réseaux sociaux, il y a d'autres très significatives. Etant dans un pays religieux, la cybercriminalité dans les réseaux sociaux y est vue comme le reflet d'une société en perdition. D'ailleurs c'est ce que I.D. (Homme, enseignant ; 34 ans), dit en ces termes : *« Nitt gni aduna daflène djital. Sen baneexu bakaan rek lagnuy toppu »*. C'est-à-dire « les gens ne cherchent que la satisfaction personnelle ». Autrement dit, ce qui se passe sur les réseaux sociaux est à l'image de la société sénégalaise. C'est pourquoi, la crise des valeurs sociales a été évoquée comme facteur explicatif de la cybercriminalité.

Cette représentation sociale de la cybercriminalité dans les réseaux sociaux est très prégnante en raison des considérations sur la société sénégalaise. Elle, qui était caractérisée de société ancrée sur des valeurs morales et religieuses profondes, est aujourd'hui définie comme étant en proie à des comportements antireligieux. Cette situation se traduit par la faiblesse ou l'inopérance des contrôles sociaux. Par ailleurs, A.S (Femme, commerçante, 35 ans) poursuit dans cette même perspective en disant « *aduna bi dafa yaaku, légui deef lu gnaaw ak waax lu gnaaw la nitt yi dieul. Sutura amatul niit yi dagno faté yalla motax lulène rek lagnuy deef* ». Autrement dit, « *le monde a changé. Faire du mal ou le dire est à la mode aujourd'hui. Le sens de la discrétion n'existe plus. Les gens ont oublié Dieu c'est pourquoi ils font ce qu'ils veulent* ».

Cette représentation sociale de la cybercriminalité dans les réseaux sociaux fait état d'une dégradation des valeurs sociales au sein de la société sénégalaise et par conséquent d'une reproduction de comportements déviants du milieu physique au cyberespace.

8.2. Réactions sociales ou attitudes face à la cybercriminalité

Toutes les sociétés réagissent aux faits sociaux qui s'y produisent. Les réactions de la part des individus qui composent ces sociétés ou groupes sociaux peuvent être diverses. Pour ce qui est

de la cybercriminalité dans les réseaux sociaux, les réactions sont toutes aussi diverses et multiples.

8.2.1. Les réactions des victimes de cybercriminalité dans les réseaux sociaux

Les attitudes que les utilisateurs des réseaux sociaux adoptent face à la cybercriminalité peuvent varier selon le type de cybercrimes auquel ils sont confrontés ou selon le fait qu'ils connaissent les services de lutte contre cette forme de criminalité.

Tableau 23 : Tableau croisé des réactions des victimes de cybercriminalité dans les réseaux sociaux

		Etre victime ou non de cybercriminalité dans les RS		
Effectif		Oui	Non	Total
Réactions des victimes		0	64	64
	J'ai cédé à son chantage	3	0	3
	J'ai demandé à la personne de supprimé sa publication	1	0	1
	J'ai porté plainte	10	0	10
	J'ai signalé le compte	4	0	4
	Je l'ai bloqué et j'ai signalé son compte	1	0	1
	Je l'ai menacé	1	0	1
	Je l'ai menacé de porter plainte	2	0	2
	Je n'ai rien fait	14	0	14
Total		38	62	100

Source : enquête de terrain Diouf Septembre 2023

Pour les trente-huit (38) victimes de cybercriminalité dans les réseaux sociaux de notre échantillon, les réactions ont été diverses :

Seul dix (10) victimes ont choisi de porter plainte ;

Quatorze (14) ont choisi de ne rien faire face à ces cybercrimes ;

Trois (3) victimes ont choisi de confronter les cybercriminels en les menaçant de porter plainte pour qu'ils les laissent tranquille et une autre victime a choisi de confronter le cyber-délinquant en lui demandant de supprimer sa publication.

Trois (3) victimes ont réagi en acceptant les exigences des cyber-délinquants ;

Cinq (5) victimes ont réagi en signalant et bloquant les comptes des cybercriminels.

- Pour les cas de cyber-harcèlement, la plupart des victimes essaient de confronter les cyber-délinquants en les menaçant ou en utilisant une toute autre façon de se défendre. C'est après persistance des cybercriminels, que les victimes optent pour la voie juridique en portant plainte, comme ce fut le cas pour les trois (3) victimes de cyber-harcèlement de notre échantillon et pour d'autres observées sur les réseaux sociaux.

- Pour les cybercrimes qui touchent aux mœurs, la plupart les utilisateurs de réseaux sociaux, qui en sont victimes, se sentent sans défense. Ils sont animés par un sentiment d'impuissance et de peur. Cela se justifie par le regard et l'intransigeance de la société sénégalaise sur les questions de réputation. Étant donné la réputation et les étiquettes sont des choses sur lesquelles notre société s'appesantit pour des choses comme le mariage ou même le respect et la considération qui est accordé à l'individu au sein de la société. Une fois dans cette position, les victimes de ces formes de cybercriminalité se mettent à obéir et à respecter les exigences des cyber-délinquants et la raison est qu'elles ont peur que leur réputation soit entachée. Elles vont aussi même jusqu'à ne pas porter plainte par peur que l'affaire s'ébruite ou qu'elles soient jugées.

  D'ailleurs cette remarque a été faite au niveau des différents services de lutte contre la cybercriminalité au Sénégal. D'après les estimations de Kandé (Homme, Commissaire à la DSC), « *40 à 60% des victimes de cybercriminalité ne portent pas plainte à cause des menaces de divulgation* ». Il poursuit en disant « *la plupart des victimes préfèrent se soumettre aux exigences des cyber-délinquants parce qu'elles se sentent impuissantes ou ont peur que leurs réputations soient entachées* ». Cependant, il est clair que le fait les internautes ne connaissent pas les services spécialisés dans la cybersécurité et la lutte contre la cybercriminalité et leurs missions est en soi un facteur qui explique le fait que les victimes ne choisissent pas la procédure juridico-

institutionnelle. C'est la crainte de n'avoir aucun recours à part suivre les instructions ou de demander la clémence des cybercriminels, pousse les victimes à ne pas porter plainte.

Certaines victimes choisissent la voie juridique en allant vers les services de lutte, qui, au-delà de la poursuite des cybercriminels, procèdent au retrait des contenus illicites sur les réseaux sociaux.

8.2.2 Les réactions des services étatiques

Au-delà des réactions des particuliers, nous avons la réaction des autorités étatiques qui, face à certaines cybercrimes sur les réseaux sociaux, adoptent un certain nombre de mesures.

8.2.2.1. La restriction d'internet et/ou des réseaux sociaux

Face à des cybercrimes comme les incitations à la violence et/ou à la haine, la diffusion de fausses nouvelles, les autorités réagissent à travers une restriction d'internet ou des certains réseaux sociaux sur l'étendue du territoire national. D'ailleurs, ces restrictions ont été observables au cours de ces dernières années. A travers le Ministère de la communication, des télécommunications et du numérique, l'Etat du Sénégal a déjà procédé à la restriction de l'internet mobile au motif de diffusion de fausses nouvelles ou d'incitation à la violence ou à la haine.

Image 11 : Suspension de l'internet mobile au Sénégal

REPUBLIQUE DU SENEGAL

Un Peuple - Un But - Une Foi

Ministère de la Communication, des Télécommunications et de l'Economie Numérique

LE MINISTRE

COMMUNIQUE

OBJET : suspension temporaire de l'internet des données mobiles

Le Ministre de la Communication, des Télécommunications et de l'Economie numérique informe le public qu'en raison de la diffusion de messages haineux et subversifs relayés sur les réseaux sociaux dans un contexte de menace de trouble à l'ordre public, l'internet des données mobiles est suspendu temporairement sur certaines plages horaires à partir du lundi 31 juillet 2023.

Les opérateurs de téléphonie sont tenus de se conformer aux réquisitions notifiées.

Fait à Dakar, le 31 juillet 2023

Le Ministre

Me Moussa Bocar THIAM

REPUBLIQUE DU SENEGAL
Un Peuple - Un But - Une Foi

Ministère de la Communication,
des Télécommunications et du Numérique

Dakar, le 13 février 2024

LE MINISTRE

COMMUNIQUE

OBJET : Suspension provisoire de l'Internet des données mobiles

Le Ministre de la Communication, des Télécommunications et du Numérique informe le public qu'en raison de la diffusion sur les réseaux sociaux de plusieurs messages haineux et subversifs qui ont déjà provoqués des manifestations violentes avec des décès et des dégâts matériels importants, l'internet des données mobiles est suspendu ce mardi 13 février 2024 selon certaines plages horaires.

Les opérateurs de téléphonie sont tenus de se conformer aux réquisitions notifiées.

Ces restrictions de l'internet mobile sont intervenues durant des périodes de tensions politiques et sociales allant de Mars 2021 à Février 2024. Pour les autorités gouvernementales, elles sont justifiées par un besoin d'ordre et de stabilité sociale.

8.2.2.2. Le retrait de contenus illicites

Le contenu illicite est soit une vidéo, un audio, un article ou une image qui porte atteinte à la dignité humaine, incité à la haine, ou qui porte atteinte à la vie privée d'une personne. Il peut s'agir également de contenus relatifs aux données à caractère personnel mise en ligne sans le consentement de la victime.

Le retrait de contenus illicites est très souvent l'étape qui suit après que la victime de cybercriminalité dans les réseaux sociaux ait porté plainte auprès des services compétents. Après l'étude de la plainte, les services comme la division spéciale de cybersécurité (DSC) ou

la plateforme numérique de lutte contre la cybercriminalité (PNLC) ou encore la commission de protection des données personnelles (CDP) somment le mis en cause de retirer le contenu. Mais dans le cas de figure où le mis en cause n'est pas identifié ou n'est pas disposé à retirer le contenu, ces services en charge de la cybercriminalité au Sénégal envoie une requête à la plateforme concernée pour que le contenu puisse être supprimé ou rendu inaccessible.

Tableau 24 : Retrait des contenus illicites effectués par la division spéciale de cybersécurité (DSC) de 2020 et 2022.

Année	Blocage réseaux sociaux (facebook, instagram, youtube, autres)	Blocage site internet (sites pornographiques, e-commerce, actu et piratage IPTV)	Total
2020	09	47	56
2021	07	40	47
2022	10	50	60
Total	26	137	163

De 2020 à 2022 la division spéciale de la cybersécurité (DSC) a effectué un nombre important de retrait de contenu illicites à la demande de victimes de cybercriminalité dans les réseaux sociaux ou à travers de signalements de citoyens sénégalais ; soit un total de 163. De 2020 à 2021, la DSC a procédé aux blocages de cent trois (103) sites internet et réseaux sociaux, soit un taux d'évolution de -16,07%. Cette baisse notable indique que le nombre de blocages de réseaux sociaux a diminué en 2021 par rapport à 2020. Cependant, la tendance s'est inversée entre 2021 et 2022, où le nombre de blocage de réseaux sociaux et de sites internet est de cent sept (107) ; soit un taux d'évolution de 27,66%. Ce taux d'évolution rend compte de l'importante augmentation des blocages effectuées par la division spéciale de cybersécurité (DSC). Le retrait des contenus illicites permet aux victimes de sortir de l'affront dans lequel elles sont.

8.2.2.3. Les peines

Dans les différentes lois que le Sénégal a adopté dans le cadre de la réglementation du cyberespace et de la lutte contre la cybercriminalité, il y est fait mention de peines à infliger aux cybercriminels pour chaque type de cyber-infractions. Ces peines vont de la privation de

liberté (emprisonnement) aux amendes. Ces peines constituent des formes de réactions à la cybercriminalité.

- Peines privatives de liberté : elles se caractérisent en des emprisonnements d'individus jugés coupables de cybercriminalité.
- Peines pécuniaires : elles se manifestent sous forme d'amendes infligés à la personne reconnue coupable de cybercriminalité
- Peines complémentaires : elles se constituent en grande partie de coupure d'accès au site ayant servi à la commission de l'acte cybercriminel

8.3. Les répercussions de la cybercriminalité dans les réseaux sociaux

Internet et les réseaux sociaux, qui plus est avec la cybercriminalité, ont fait qu'il est difficile de nos jours de parler de vie privée. La criminalité numérique dans ses formes a des répercussions considérables sur la vie privée et sociale. D'ailleurs les propos de Solange Ghernaouti s'inscrivent dans cette même perspective. Elle dit en ces termes *« la criminalité, qu'elle soit organisée ou non, s'est largement appropriée les technologies de l'informatique, induisant des conséquences préjudiciables tant pour les individus, les organisations que pour les États* » (Ghernaouti-Hélie, 2009). Elle poursuit dans son ouvrage *La cybercriminalité : le visible et l'invisible* à travers un passage dans lequel elle explique les effets de la cybercriminalité. Elle fait le portrait de ces effets en ces termes « *citoyens détroussés, enfants en dangers, entreprises ruinées, États menacés, les cybercriminels étendent leur emprise en même temps qu'internet se développe. Nous ne les voyons pas, nous ne nous en méfions pas et c'est leur force* » (Ghernaouti-Hélie, 2009)

8.3.1. Sur la vie privée

La cybercriminalité dans les réseaux sociaux, sous ses différentes formes au Sénégal, présente son lot d'impacts sur l'individu, en l'occurrence sa vie privée. L'essence de l'activité cybercriminelle est les données à caractère personnel. Ce qui implique inéluctablement que leur utilisation à des fins criminelles présente des répercussions sur la vie privée des victimes de cybercriminalité dans les réseaux sociaux.

Dans la société sénégalaise où l'image et la réputation sont au centre des considérations sociales, être victime de cybercriminalité dans les réseaux sociaux présentent bon nombre de conséquences surtout quand le cybercrime en question attrait à l'image de la personne. Les cybercrimes sur les affaires de mœurs ont plus de répercussions sur la vie privée parce que comme souligné tantôt elle implique l'image et la réputation de la personne. D'ailleurs c'est ce

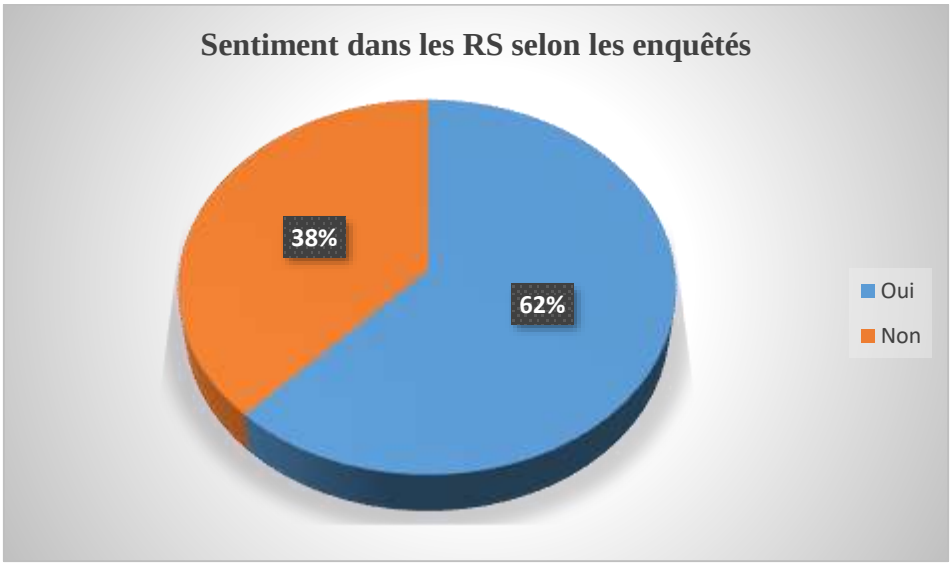
qu'avance T.A.C. (Homme, informaticien, 29 ans) en ces termes « *la cybercriminalité diminue la confiance des uns par rapport aux autres et oblige certains même à quitter internet du fait de la divulgation des données personnelles, de l'humiliation, d'usurpation d'identité etc.* »

Par ailleurs, il est difficile aujourd'hui de parler de vie privée quand les données personnelles sont collectées à l'insu des utilisateurs. De ce fait, ces derniers font l'objet de prospection directe de la part de toutes sortes d'entreprises. Cette dernière implique très souvent une collecte ou un traitement illégale de données personnelles comme les numéros de téléphones. La prospection directe suppose la proposition de services non sollicités par appels téléphoniques ou messages. Au-delà de la violation de la confidentialité, le cyber-harcèlement et la cyber-intimidation sont des facettes de la cybercriminalité dans les réseaux sociaux qui ont très souvent des conséquences d'ordre psychologique sur les victimes de ce type de cybercrime. Traditionnellement, le harcèlement était restreint à des espaces comme l'école ou les groupes de quartier. Ce qui faisait de l'espace familial un endroit sûr ; un refuge pour les victimes de harcèlement. Cependant, il est, de nos jours, difficile pour les victimes trouver leurs cocons étant donné que le harcèlement pénètre l'espace familial à travers les réseaux sociaux.

De plus, en un clic, la réputation d'une personne peut être ternie avec le concept de e-réputation qui est l'image que l'utilisateur se construit dans le cyberespace, qui, à bien des égards, peut avoir une incidence sur les considérations dans l'espace social physique. Parce que les images de certains utilisateurs se retrouvent sur des sites de prostitution en ligne sans même qu'ils ne soient au courant. D'ailleurs Niang (Homme, Lieutenant à la PNLC) le souligne en ces termes « *les photos de beaucoup de filles se retrouvent à leur insu sur sites ou pages de prostitution en ligne pour attirer des hommes* ». La réputation des utilisateurs est d'autant plus ternie quand des contenus illicites les concernant se retrouvent sur les réseaux sociaux à plus forte raison dans une société sénégalaise aussi conservatrice. Ce qui ruine des mariages ou projets de mariages voire même des carrières professionnelles.

La cybercriminalité dans les réseaux sociaux a aussi des répercussions sur la vie des couples. Ces propos de Kassé (Sous-Lieutenant à la PNLC) la présente comme une cause de divorce. Il dit en ces termes « *des couples se séparent à l'issu de fuite de vidéos sur internet* ».

Graphique 22 : Répartition de l'échantillon en fonction du sentiment de sécurité dans les réseaux sociaux



Source : enquête de terrain Diouf Septembre 2023

8.3.2. Sur la vie sociale

Comme sur la vie privée, la cybercriminalité dans les réseaux sociaux a son lot de répercussions sur la vie sociale en générale. Ces répercussions concernent l'économie numérique, la stabilité sociale et politique etc.

8.3.2.1. La cybercriminalité dans les réseaux sociaux : une menace au développement de l'économie numérique

Les formes de cybercriminalité telles que les escroqueries en ligne sont une très grande menace pour l'économie particulièrement dans un contexte où celle se numérise. Le commerce en ligne ou e-commerce facilite non seulement les transactions commerciales mais il permet aussi d'impliquer un nombre important d'acteurs dans ce secteur. Cependant, la menace cybercriminelle vient perturber ceci en installant un climat d'insécurité et de méfiance. Ce qui, inévitablement, joue sur la performance et le développement du commerce numérique. C'est pourquoi, il est clair que la cybercriminalité dans toutes ses facettes représente un frein à la réalisation de la vision déclinée dans la stratégie nationale de cybersécurité « en 2020 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous ». Elle l'est par conséquent pour le développement de l'économie numérique et de la digitalisation des administrations.

8.3.2.2. La cybercriminalité dans les réseaux sociaux : une menace à la stabilité sociale

Les réseaux sociaux sont en quelque sorte des espaces de promotion des libertés d'expression et d'information. Aujourd'hui, il est difficile pour les États et gouvernements de maitriser celles-ci sans porter atteinte aux libertés de leurs citoyens.

Les réseaux sociaux ne sont plus de simples plateformes communautaires mais des zones d'expression libre qui permettent aux masses silencieuses d'user d'un de leurs droits les plus fondamentaux : celui de s'exprimer librement. Cependant, cette liberté d'expression de l'utilisateur de réseaux sociaux atteint un niveau socialement et/ou juridiquement illégal en se transformant en de la diffusion des messages haineux, raciaux ou diffamatoires ou encore incitant à la violence.

Les cybercrimes tels que les atteintes à l'État menacent directement la stabilité sociale, parce que celles-ci se manifestent sous forme d'incitation à la haine, à la violence, de terrorisme etc. Les répercussions de ces cybercrimes se manifestent à travers une escalade de la violence comme le notifient les services de lutte contre la cybercriminalité au Sénégal durant la période de Mars 2021 à février 2024. Cette période fut marquée par une instabilité sociopolitique durant laquelle plusieurs individus ont été arrêtés ou ont été sous le coup de mandat d'arrêt pour des faits de d'incitation à la violence ou de troubles à l'ordre publique. Durant cette période, les réseaux sociaux ont été les espaces d'expressions de vagues de mécontentement de la part des utilisateurs de réseaux sociaux sur et en dehors du territoire sénégalais. Cette période a été marqué par la publication sur médias sociaux des bavures et forfaitures des autorités étatiques et des forces de défense et de sécurité. Ce qui a valu, entre Mars 2021 à Février 2024, plusieurs ordonnances de coupure de l'internet mobile par le ministère sénégalais de la communication, des télécommunications et de l'économie numérique.

En somme, sous ses différentes formes, la cybercriminalité dans les réseaux sociaux a eu des incidences négatives et ce à plusieurs échelles. D'abord, elle affecte directement l'individu, c'est-à-dire sur sa vie privée. Ensuite, elle affecte les activités transactionnelles telles que le commerce en ligne. En fin, la cybercriminalité dans les réseaux sociaux atteint un niveau où ses répercussions se mesurent à grande échelle. Elle devient source d'instabilité politique et sociale.

8.3. Les recommandations

La partie recommandation regroupe des réponses sociétales et sociologiques envisageables dans le cadre de la lutte contre la cybercriminalité. Ces dernières sont à plusieurs niveaux : les

particuliers, les gouvernements et les institutions spécialisées, les chercheurs, les entreprises etc.

8.3.1. Les réponses sociétales

- Sensibilisation du public : Organiser des campagnes de sensibilisation pour informer le public des risques en ligne, des arnaques courantes et des mesures de prévention, notamment pour les populations les plus vulnérables (jeunes, personnes âgées, entreprises locales).
- Éducation numérique : Intégrer l'éducation à la cybersécurité dans les programmes scolaires et universitaires pour former les jeunes aux bonnes pratiques de sécurité en ligne, et encourager le développement de compétences en cybersécurité.
- Formation des professionnels : Offrir des formations spécifiques aux professionnels dans les domaines de la finance, de la santé, des télécommunications, et de l'administration publique pour renforcer leur vigilance et leur préparation face aux cybermenaces.
- Renforcement des infrastructures de sécurité : Collaborer avec les entreprises technologiques et les opérateurs de télécommunications pour sécuriser les réseaux, protéger les données personnelles et mettre en place des protocoles de détection et de réponse aux cyberattaques.
- Appui à la recherche et à l'innovation : Soutenir les initiatives locales de recherche en cybersécurité et développer des solutions technologiques adaptées aux besoins et aux particularités du Sénégal pour une réponse plus ciblée aux cybermenaces.
- Engagement communautaire : Encourager la formation de groupes de cybervigilance communautaires qui peuvent signaler les arnaques et incidents suspects, et collaborer avec les autorités pour protéger les citoyens.
- Coopération internationale : Renforcer la collaboration avec des organisations internationales et d'autres pays pour partager des informations, des technologies et des expertises en matière de lutte contre la cybercriminalité.
- Renforcement du cadre législatif : Adapter et mettre en œuvre des lois strictes sur la cybercriminalité, assurant des peines dissuasives et une meilleure protection des victimes.

8.3.2. Les réponses sociologiques

- Études de comportement en ligne : Mener des recherches sociologiques sur les comportements numériques des citoyens pour comprendre les pratiques à risque et identifier les groupes les plus vulnérables à la cybercriminalité. Cela peut aider à mieux cibler les campagnes de prévention.
- Renforcement de la cohésion sociale : Promouvoir des initiatives communautaires et des valeurs de solidarité pour renforcer la vigilance collective. Les communautés unies et informées peuvent mieux résister aux manipulations et escroqueries en ligne.
- Influence des normes sociales : Créer et promouvoir des normes de sécurité numérique dans la société, encourageant les comportements de prudence en ligne et la vérification des informations. Par exemple, normaliser le partage des pratiques de sécurité de base, comme l'authentification à deux facteurs.
- Rôle des leaders d'opinion : Impliquer des figures publiques, des influenceurs et des leaders communautaires pour diffuser des messages de prévention et sensibiliser leurs audiences aux dangers de la cybercriminalité.
- Intégration de la cybersécurité dans les discours culturels : Utiliser les médias et la culture populaire (comme la musique, les émissions de télévision, les séries locales) pour aborder les enjeux de cybersécurité de manière accessible, en sensibilisant par des exemples et des histoires proches de la réalité des citoyens.
- Études sur les motivations des cybercriminels : Analyser les raisons qui poussent certains individus à se tourner vers la cybercriminalité, qu'il s'agisse de motivations économiques, sociales, ou d'un manque de perspectives d'avenir. Cette compréhension peut aider à élaborer des programmes de réinsertion et de sensibilisation.

CONCLUSION GENERALE

Dans son ouvrage *Sociologie des réseaux sociaux,* Pierre Merklé met en avant l'approche d'une étude des réseaux sociaux à travers « *les relations entre les individus et les régularités qu'elles présentent pour les décrire, rendre compte de leur formation et de leur transformation, analyser leurs effets sur les comportements individuels.* » (Merklé, 2011)

Ce qui, par ailleurs, a inscrit ce présent mémoire sur la cybercriminalité dans les réseaux sociaux dans une perspective d'étude des usages illégaux des technologies de l'information et de la communication telles que les réseaux sociaux. Cette étude suppose une description des tendances de la cybercriminalité dans les réseaux sociaux au Sénégal et à leurs compréhensions.

Ainsi, sur une volonté d'apporter une plus-value à la recherche sur la cybercriminalité en général et spécifiquement celle concernant les réseaux sociaux, cette recherche, sur la base d'une triangulation méthodologique, a permis de faire une mise au point de la situation sur la cybercriminalité au Sénégal. Cette mise au point s'est matérialisée par un état des lieux sur le cadre juridique et institutionnel sénégalais en matière de cybersécurité et de lutte contre la cybercriminalité. Ce cadre s'est renforcé par l'élaboration de politiques de cybersécurité telles que la stratégie nationale de cybersécurité (SNC2022) et d'un cadre de coopération tant national qu'international. Cependant, force est de constater que, même si les mobilisations en termes de cybersécurité et lutte contre la cybercriminalité sont impressionnantes, celles-ci présentent des limites considérables. Les recherches sur notre problématique ont montré une carence ou absence de programme de sensibilisation au niveau national et une coopération internationale qui fait défaut du fait du caractère transnational de la cybercriminalité et de territorialité des infractions cybercriminelles. Autrement dit, le principe de la double incrimination doit être de mise pour que des poursuites judiciaires puissent avoir lieu.

Étant parti de l'hypothèse principale selon laquelle les causes la cybercriminalité dans les réseaux sociaux sont de l'ordre des conditions socioéconomiques de l'individu et de l'anonymat qui lui est offert par internet, il nous a été donné de remarquer, à la suite de l'analyse des données de terrain, que les facteurs évoqués ne suffisaient pas à elles seules pour expliquer cette criminalité. En plus de celles-ci qui s'imposent à l'individu s'ajoute le choix rationnel de l'individu de passer à l'acte. Il convient par-là de prendre en compte les justificatifs que ces individus considérés comme cybercriminels utilisent pour donner du sens à leurs actions. Il en est de même pour notre première hypothèse secondaire dans laquelle la cybercriminalité dans les réseaux sociaux se manifestait sous forme d'escroqueries et d'atteintes à l'image et à la vie

privée. Cependant, les données ont révélé que la cybercriminalité dans les réseaux sociaux en revêt d'autres, regroupées en des atteintes à l'État, à l'extrémisme et au terrorisme. Ce qui infirme notre hypothèse parce que celle-ci est incomplète. Ces infractions cybercriminelles ont été évoquées à partir de 2021 du fait des perturbations sociopolitiques auxquelles le Sénégal a été confronté. Celles-ci sont essentiellement des incitations à la violence et de la xénophobie.

De plus, ce travail de recherche a permis de relever les différentes considérations sur la cybercriminalité dans les réseaux que nous abordions à travers notre deuxième hypothèse secondaire. Ainsi, les exactions commises à travers les réseaux sociaux sont aujourd'hui problématiques pour la société sénégalaise au point que celle-ci se représente la cybercriminalité comme une criminalité à laquelle elle se trouve sans défense et impuissante. De plus, il est noté que la cybercriminalité dans les réseaux sociaux est à l'image de cette même société dont la dégradation des certaines valeurs sociales est perceptible de par les comportements sur les technologies de réseautage.

En outre, les données révèlent également que même si certaines victimes en acceptant les exigences des cybercriminels et de ne pas porter plainte par peur que l'affaire s'ébruite et qu'elles soient jugées, il existe d'autres catégories de victimes qui réagissent à la cybercriminalité en portant plainte ou en confrontant les cyber-délinquants de sorte à les obliger à les laisser tranquille. Ce qui infirme notre quatrième hypothèse secondaire parce que celle-ci est incomplète.

En effet, la cybercriminalité dans les réseaux sociaux, sous ses différentes formes, a d'énormes incidences non seulement sur la vie privée des victimes, mais aussi sur la vie sociale de manière générale. Cette criminalité a révoqué l'idée même de vie privée parce qu'une grande partie de ses manifestations ont trait à la réputation des victimes. De plus, la cybercriminalité dans les réseaux sociaux, sous les formes d'incitation à la violence et/ou à la haine, menace l'ordre et l'équilibre sociopolitique comme ce fut le cas durant la période allant de Mars 2021 à Février 2024. Les données sur les conséquences de la cybercriminalité dans les réseaux sociaux infirment aussi notre troisième hypothèse secondaire parce que ces dernières ne se limitent à la menace de la stabilité politique et sociale.

En définitive, la cybercriminalité dans les réseaux sociaux au Sénégal est une problématique dont la portée est très difficile à saisir. Cette difficulté réside dans le fait que les chiffres sont loin de refléter la réalité étant donné que 40 à 60 % des cybercrimes ne sont pas rapportés. De plus, centraliser les données permettrait d'en avoir une idée un peu plus précise. Ce qui n'est

pas encore le cas. A cela s'ajoute des politiques publiques et mesures de cybersécurité et de lutte contre la cybercriminalité n'étant accès que sur les aspects techniques et juridiques. Puisque cette approche n'est pas des plus inclusives en termes de politiques de cybersécurité et de lutte contre la cybercriminalité, il serait de ce fait judicieux d'en adopter une qui soit un peu plus holistique afin de prendre en compte l'aspect humain qui permettrait d'inclure la formation et la sensibilisation des acteurs dans ces politiques, d'autant plus que l'atout majeur des cybercriminels dans les réseaux sociaux est l'ingénierie sociale.

Eu égard aux éléments de réponses de la recherche, l'acte cybercriminel ne peut être considéré comme la résultante des conditions économiques et sociales ou des dysfonctionnements structurels et sociaux. En effet, ces conditions extérieures à l'individu prennent sens que quand ils sont associés au sens que ce dernier donne à son action. Ce qui fait que nos modèles théoriques, pris isolément, n'expliquent pas avec suffisance l'activité cybercriminelle.

En raison de la singularité de cette étude qui n'aborde la cybercriminalité qu'uniquement dans les réseaux sociaux, il serait enrichissant d'aborder cette thématique dans sa globalité au Sénégal et d'en saisir les dynamiques et les enjeux.

Bibliographie

Abric, J.-C. (1997). *Pratiques sociales et représentations* (éd. 2e). Paris: PUF.

ACID. (2022). *The Geography of BEC : The Global Reach of the World's Top Cyber Threat.*

ANSD. (2019). *Situation économique et sociale régionale.* Dakar.

ANSD. (2020-2021). *Situation Economique et Sociale de la région de Dakar.* Dakar.

ANSD. (2023). *Rapport préliminaire RGPH-5.*

Bardin, L. (1977). *L'Analyse de contenu.* Paris: PUF.

Becker, H. (1985). *Outsiders.* Paris: Métaillé.

Benbouzid, B., & Ventre, D. (2016). Hackers malveillants, cybervictimations, traces du web et reconfigurations du policing. (D. l. réseaux, Éd.) *Pour une sociologie du crime en ligne*(197-198), pp. 9-30.

Breton, D. L. (2004). *L'interactionnisme symbolique.* Paris: PUF.

Burger, S. (2020). Phishing attacks in Africa diversify, target small companies. *Creamer Media*, 1.

Burgess, R., & Akers, R. (1996). Une théorie différentielle d'association-renforcement du comportement criminel. *Problèmes sociaux, 14*(2), 128-147. Consulté le 03 10, 2023, sur https://doi.org/10.2307/798612

Chawki, M. (2006, Juillet). Essai sur la notion de cybercriminalité. 5.

CHEDS. (2022, Mai). CYBERSECURITE AU SENEGAL. *Magazine du centre des hautes études de défense et de cybersécurité*, p. 8.

Chelin, R. (2021). Afrique : nouvel eldorado d'arnaques aux crypto-arnaques et du blanchiment d'argent. *ISS Today*, 2.

CNIL. (2020, Mai 19). *Commission nationale de l'informatique et des libertés*. Consulté le Janvier 28, 2024, sur cnil.fr: https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

(2001). *Convention sur la cybercriminalité.* Budapest.

Corbin, C. (2020, 10 16). Consulté le 08 29, 2022, sur united nations office on drugs and crime: unodc.org

Cornish, D., & Clarke, R. (1987). comprendre le déplacement de la criminalitité : une application de la théorie du choix rationnel. *Criminologie, 25*(4), 933-948. Consulté le 03 11, 2023, sur https://doi.org/10.1111/j.1745-9125.1987.tb00826.x

Cromwell, P., & Thruman, Q. (2003, Décembre). The devil made me do it : use of neutralizations by shoplifters. *Deviant Behavior, 24*(6), 535-550.

Cusson, M. (1992). Déviance. Dans R. Boudon, *Traité de socilogie* (pp. 389-422). Paris: PUF.

DataReportal, Meltwater, & WeAreSocial. (2024). *Numérique 2024 : Sénégal.*

Diakhaté, O. (2013, 09 05). *SENEPLUS*. Consulté le Août 2023, sur SENEPLUS: https://www.seneplus.com/article/l%E2%80%99escroc-de-selbe-ndom-tombe

Dufour, A., & Ghernaouti-Hélie, S. (2019). *De l'ordinateur à la société de l'information.* ePagine.

Durkheim. (1897). *Le Suicide.* Paris: Presses universitaires de France & Félix Alcan.

Durkheim, E. (1893). *De la division du travail social.* Paris: P.U.F.

Durkheim, E. (1895). *Les Régles de la Méthode Sociologique.* Paris: P.U.F.

Elias, N. (1987). *La Société des indivindus.* Paris: Pocket.

Ferri, E. (1893). *La socilogie criminelle.* Paris : Dalloz.

Ghernaouti-Hélie, S. (2009). *La cybercriminalité: le visible et l'invisible.* Paris: Presses Polytechniques et Universitaires Romandes.

Gibson, W. (1984). *Neuromancien.* New York: Ace Books.

Goffman, E. (1968). Asiles. 21. Paris: Minuit.

Grawitz, M. (1996). *Méthodes en sciences sociales.* Paris: Dalloz.

Hirschi, T. (2002). *Causes of delinquency.* New York: Routledge.

Intepol. (2021). *Evaluation des cybermenaces en Afrique.*

Jaishankar, K. (2008). Space transition theory. Dans F. Schmalleger, & M. Pittaro, *Crimes of the Internet* (pp. 283-301). Pearson.

Jodelet, D. (1997). *Les représentations sociales.* Paris: PUF.

Kaluszynski, M. (2005). Quand est née la criminologie ? ou la criminologie avant les Archives... (Criminocorpus, Éd.) *Histoire de la criminologie. Autour des Archives d'anthropologie criminelle 1886-1914*, p. 6.

Kaspersky. (2022, Décembre 7). Chiffre de l'année : Les cybercriminels s'attaquent aux internautes avec 400 000 nouveaux fichiers malveillants par jour: c'est 5% de plus qu'en 2021. Consulté le Mars 14, 2023, sur https://www.kaspersky.fr/about/press-releases/2022_chiffre-de-lannee-les-cybercriminels-sattaquent-aux-internautes-avec-400-000-nouveaux-fichiers-malveillants-par-jour-cest-5-de-plus-quen-2021

Knowbe4. (2019). *African Cybersecurity Research Report.*

Lacassagne, A. (1913). *Des transformations du droit pénal et les progès de la médecine légalede 1810 à1913.*

Lebert, M.-F. (1999). Thèse. *De l'imprimé à l'internet*. Paris: 00h00.

Martin, D. (1997). *La criminalité informatique.* Paris: PUF.

Mead, G. H. (1963). *L'esprit, le soi et la société.* Paris: PUF.

Merklé, P. (2004). *La sociologie des réseaux sociaux.* Paris: La Découverte.

Merton, R. (1953). *Éléménts de théorie et de méthode sociologique.* Paris: Free Press.

Meynaud, H. Y., & Duclos, D. (2007). De l'échantillonnage à la remise du produit. *Les sondages d'opinion*, pp. 49-63.

Ministère de la communication, d. t. (2017). *Stratégie nationale de cybersécurité du Sénégal (SNC2022).* Dakar.

Ministère de l'intérieur français. (s.d.). *Ministère de l'intérieur et des outre-mer*. Consulté le Mars 03, 2023, sur Ministère de l'intérieur et des outre-mer: https://www.interieur.gouv.fr/

Moscovici, S. (1984). *Représentations sociales : Essais de psychologie sociale.* New York: NYU Press.

Niang, L. M., Otonkala, L. K., Kpeto, S. M., & Yaffa, S. K. (2022). La criminalité dans les réseaux sociaux : bilan, enjeux et .

Parsons, T. (1951). *Le Système Social.* Free Press Paperback.

Pinatel, J. (1987). *Le phénomème criminel.* Paris: MA Editions.

Rose, P., & Lamère, J.-M. (1996). *Menaces sur l'autoroute de l'information.* Paris : L'Harmattan .

Roussiau, N., & Bonardi, c. (2001). *Les représentations sociales : états des lieux et perspectives.* Belgique: Margada.

Schmalleger, F., & Pittaro, M. (2008). *Crimes of the Internet.* Pearson.

Ségur, P., & Périé-Frey, S. (2023, 12 4). Cybercriminalité, ordre public, économique et déstabilisation de l'Etat. *Internet et la démocratie numérique*, p. 5.

Shaw, C., & Mckay, H. (1942). *Juvenile Delinquancy and urban areas.* Chicago: University of Chicago Press.

(2017). *Stratégie nationale de cybersécurité du Sénégal* .

Sutherland, E., & Cressey, D. (1966). *Principes de criminologie.* Paris: Cujas.

Sykes, G., & Matza, D. (1957, Décembre). Techniques of neutralization : a theory of delinquency. *American Sociological Review, 22*(6), 664-670.

Tine, B. (2004). *La toxicomanie à Thiès : étude sociologique d'une forme de déviance au Sénégal.*

Touré, P. A. (2010). La cyberstratégie de répression de la cybercriminalité au Sénégal : présentation de la loi n° 2008-11 du 25 janvier 200 8, portant sur la cybercriminalité. *Conférence sur la coopération contre la cybercriminalité,,* (p. 1). Strasbourg.

Touré, P. A. (2014). *Le traitement de la cybercriminalité devant le juge.* Paris: L'Harmattan.

UIT. (2009). *Comprendre la cybercriminalité: Guide pour les pays en développement.* Genève.

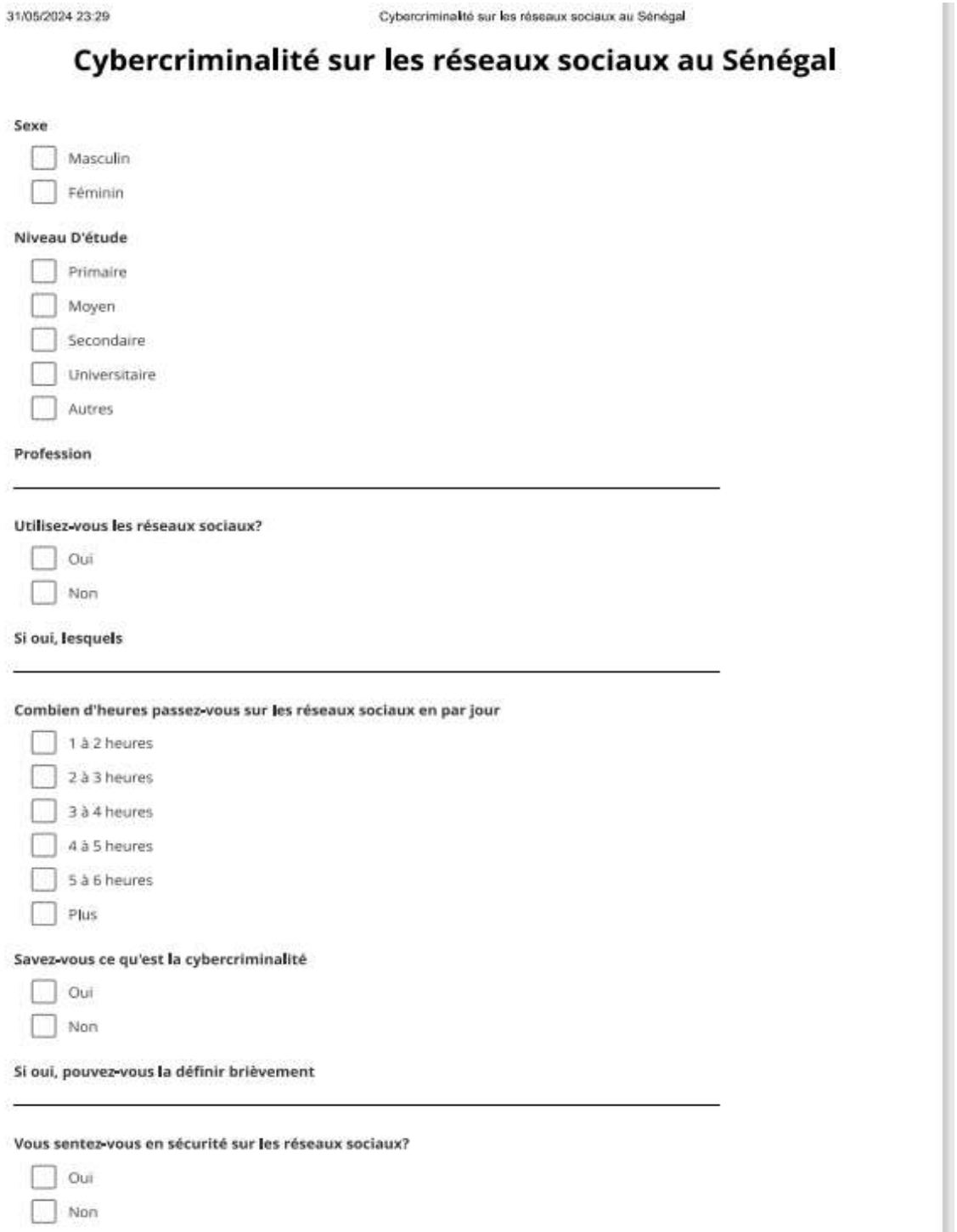
UNICEF. (2021, Octobre). Définitions des normes sociales et des concepts connexes. *UNICEF*, 1.

Wall, D. (2007). *Cybercrime : the transformation of crime information Age.* Politique.

ANNEXES

Annexe 1 : Questionnaire pour les utilisateurs des réseaux sociaux

Bonjour, je me nomme Cheikh Sidath Mbagnick Diouf, étudiant en master 2 de sociologie à l'université Assane Seck de Ziguinchor. Dans le cadre de la rédaction de mon mémoire sur la cybercriminalité dans les réseaux sociaux au Sénégal, je souhaite vous soumettre un questionnaire de recherche qui aborde différents aspects de cette thématique.



31/05/2024 23:29 Cybercriminalité sur les réseaux sociaux au Sénégal

Cybercriminalité sur les réseaux sociaux au Sénégal

Sexe

- ☐ Masculin
- ☐ Féminin

Niveau D'étude

- ☐ Primaire
- ☐ Moyen
- ☐ Secondaire
- ☐ Universitaire
- ☐ Autres

Profession

_____

Utilisez-vous les réseaux sociaux?

- ☐ Oui
- ☐ Non

Si oui, lesquels

_____

Combien d'heures passez-vous sur les réseaux sociaux en par jour

- ☐ 1 à 2 heures
- ☐ 2 à 3 heures
- ☐ 3 à 4 heures
- ☐ 4 à 5 heures
- ☐ 5 à 6 heures
- ☐ Plus

Savez-vous ce qu'est la cybercriminalité

- ☐ Oui
- ☐ Non

Si oui, pouvez-vous la définir brièvement

_____

Vous sentez-vous en sécurité sur les réseaux sociaux?

- ☐ Oui
- ☐ Non

Avez-vous une fois été victime de cybercriminalité sur les réseaux sociaux?

- [ ] Oui
- [ ] Non

Si oui, quel genre de cybercrime?

_____

Pouvez-vous nous dire comment cela s'est produit?

_____

A travers quel réseau social s'est-il produit

- [ ] Instagram
- [ ] Twitter
- [ ] Facebook
- [ ] Snapchat
- [ ] Tiktok
- [ ] Youtube
- [ ] Autres

Qu'avez-vous fait quand cela s'est produit?

_____

Selon vous, pourquoi certaines victimes ne portent pas plaintes?

_____

Selon vous, quels sont les causes de la cybercriminalité sur les réseaux sociaux au Sénégal?

_____

Quels sont les cybercrimes que vous connaissez?

_____

Savez-vous ce qu'est la cybersécurité?

- [ ] Oui
- [ ] Non

Avez-vous des notions en cybersécurité?

- [ ] Oui
- [ ] Non

Avez-vous connaissance de politiques de sensibilisation sur la cybercriminalité sur les réseaux sociaux

- [ ] Oui
- [ ] Non

Si oui, lesquelles

_____

Connaissez vous des services de lutte contre la cybercriminalité au Sénégal?

- ◯ Oui
- ◯ Non

Si oui, lesquels?

_____

Appliquez-vous les mesures de sécurité qui vous sont suggérer lors de l'installation ou la mise à jour des applications?

- ☐ Oui
- ☐ Non

Utilisez-vous des applications de sécurité sur vos appareils?

- ☐ Oui
- ☐ Non

Si oui, lesquelles

_____

Quelles mesures adoptez-vous pour éviter d'être victime de cybercriminalité?

_____

Les mesures étatiques de lutte contre la cybercriminalité sont-ils efficaces?

- ◯ Oui
- ◯ Non

Selon vous, qu'est ce qui doit être fait pour améliorer la sécurité des personnes sur internet?

_____

Annexe 2 : Grille d'observation

Critères d'observation	Description
Typologie des cybercrimes	Nature du cybercrime et la finalité, les profils de victimes, les modes opératoires
Réactions sociales	Attitudes et mesures prises par les victimes, les utilisateurs de manière générale
Représentations sociales	perceptions sur la cybercriminalité, les cybercriminels et les victimes
Répercussions sociales	les dommages causées par les cybercrimes dans les réseaux sociaux sur les victimes et la société dans son ensemble

Annexe 3 : Guide d'entretien pour les agents des services de cybersécurité et de lutte contre la cybercriminalité

1. **Identification**

Sexe

Age

Fonction

Grade

Niveau d'étude

2. **Rôles et missions**

Structuration de l'institution

Ses rôles

Ses missions

Son Efficacité dans la lutte contre la cybercriminalité

3. **Situation de la cybercriminalité au Sénégal**

Dispositifs politiques, techniques et législatifs

Coopération

Efficacité des dispositifs et de la coopération

4. **Les facteurs explicatifs de la cybercriminalité dans les réseaux sociaux au Sénégal**

Les causes techniques ou technologiques

Les causes sociales

5. **Les formes de cybercrimes dans les réseaux sociaux au Sénégal**

Les catégories de cybercrimes

Les techniques de passage à l'acte

6. **Le profilage des victimes et des cybercriminels**

Les profils de victimes

Les profils de cybercriminels

7. **Les réactions face à la cybercriminalité**

Procédures d'enquêtes et de mise en accusation

Les sanctions

8. **Les conséquences de la cybercriminalité dans les réseaux sociaux au Sénégal**

Conséquences sur la vie privée de l'individu

Conséquences sur l'économie numérique

Conséquences sur la vie publique

Annexe 4 : Guide d'entretien pour les utilisateurs des réseaux sociaux au Sénégal

1. **Identification**

Prénom et nom

Age

Sexe

Situation matrimoniale

Niveau d’étude

2. **Les facteurs explicatifs de la cybercriminalité dans les réseaux sociaux**
3. **Les formes de la cybercriminalité dans les réseaux sociaux au Sénégal**
4. **Les réactions sociales**
5. **Les représentations sociales**
6. **Les conséquences de la cybercriminalité dans les réseaux sociaux au Sénégal**

Sur la vie privée

Sur l’économie numérique

Sur la vie publique

Tables des matières