Stratégie de lutte contre la cybercriminalité en Côte d'Ivoire

Strategy against cybercriminality in Côte d'Ivoire

KOFFI Hamanys Broux De Ismaël
Docteur en Sciences de la Communication
Département des Sciences de l'Information et de la Communication
Université Peleforo Gon Coulibaly, Korhogo
Laboratoire des Sciences et Technologies de l'Information et de la Communication (LASTIC)
Côte d'Ivoire
ismael.debroux@yahoo.fr

SORO Nangahouolo Oumar
Docteur en Sciences de la Communication
Département de Langues et Sciences Humaines, Yamoussoukro
Institut National Polytechnique Houphouët Boigny
Laboratoire Langue et Sciences Humaines
Côte d'Ivoire
soronangahouolooumar@yahoo.fr

Date de soumission : 03/04/2022

Date d'acceptation : 19/05/2022

Pour citer cet article :

KOFFI H. B.D. I. & SORO N. O. (2022) «Stratégie de lutte contre la cybercriminalité en Côte d'Ivoire», Revue Internationale du Chercheur «Volume 3 : Numéro 2» pp : 106 - 130

Résumé

En facilitant les activités d'information et de communication, les technologies numériques associées à l'essor d'Internet sont devenues le terrain de chasse pour une catégorie d'individus. Elles ont mis en évidence une nouvelle menace des temps nouveaux appelée cybercriminalité. En effet, depuis le début des années 2000, ce phénomène a pris de l'ampleur en Côte d'Ivoire au point qu'il impacte fortement le quotidien de tous. Le pays n'est pas épargné par ce fléau au point où l'Etat à travers le Ministère de l'Intérieur et de la Sécurité a restructuré la Police Nationale en créant la Direction de l'Informatique et des Traces Technologiques (DITT) pour répondre plus efficacement à cette problématique de sécurité. Raison pour laquelle, l'on pourrait raisonnablement chercher à comprendre comment le pays mène cette lutte.

A partir de données qualitatives et quantitatives, cette recherche ayant pour ancrage théorique l'appropriation sociale des technologies, cherche à identifier la stratégie de lutte contre la cybercriminalité en Côte d'Ivoire.

Mots clés : Cybercriminalité ; TIC ; infraction ; internet ; Côte d'Ivoire.

Abstract

By facilitating information and communication activities, digital technologies associated with the growth of the Internet have become the hunting ground for a category of individuals. They have brought to the fore a new threat of the new times called cybercrime. Indeed, since the beginning of the 2000s, this phenomenon has grown in Côte d'Ivoire to the point where it has a major impact on everyone's daily life. The country is not spared by this scourge to the point where the State, through the Ministry of the Interior and Security, has restructured the National Police by creating the Directorate of Information Technology and Traces (DITT) to respond more effectively to this security problem. For this reason, it is reasonable to try to understand how the country is conducting this fight.

Using qualitative and quantitative data, this research, which has as its theoretical anchor the social appropriation of technologies, seeks to identify the strategy for combating cybercrime in Côte d'Ivoire.

Key words : Cybercrime ; ICT ; crime ; internet ; Côte d'Ivoire.

Introduction

Depuis les années 1990, l'insertion sociale des technologies numériques et leur appropriation par les citoyens sont devenues un enjeu important pour le développement des États africains (**Bogui & Atchoua, 2016**). L'accélération de la généralisation d'utilisation des technologies de l'information et de la communication (TIC) a été l'un des plus impressionnants faits marquants (**Kossaï, 2015**). Ce développement a donné lieu à ce que l'on a appelé « révolution numérique ». En effet, les technologies du numérique n'ont pas seulement envahi de façon massive notre vie quotidienne, elles sont aussi en train de bouleverser en profondeur la sociologie de la production et de la diffusion des savoirs (**Ndoye, 2016**).

La révolution numérique peut se définir comme l'introduction progressive mais massive de la technologie numérique dans *tous* les domaines et les moments de la vie, du niveau social – économie, administration, espaces publics – au niveau individuel – équipements domestiques, activités de loisir jusqu'aux objets que l'on porte sur soi ou désormais *en* soi (**Pistoletti, 2014**). Elle désigne donc le bouleversement profond des sociétés provoqué par l'essor des techniques numériques telles que l'informatique et le développement du réseau Internet.

Le développement du Web 2.0 qui est l'Internet facile a donc transformé le paysage des médias et notre rapport à l'information. Toute information (texte, son, vidéo) peut désormais être numérisée et transmise (par courriel, par le cloud, sur les réseaux sociaux numériques) au moyen de toutes sortes d'appareils : ordinateurs, tablettes, smartphones... La numérisation a conduit à une offre considérable, quasiment infinie d'informations, avec des sources multiples. Avec sa facilité d'accès et son système décentralisé, Internet accroît les échanges entre personnes et offre d'immenses potentialités pour participer au débat public : l'interactivité au cœur du Web 2.0 est en effet au cœur de l'information numérique. Or, comme dans toute chose, tout développement induit des effets positifs et négatifs.

C'est dans ce contexte technologique que d'autres personnes vont utiliser la technologie à des fins de nuisance criminelle et sera ainsi qualifié de « cybercriminalité », la capacité de commettre des délits tout en étant caché derrière un écran et à distance ; ce qui permet l'ubiquité du délinquant dans le temps et dans l'espace. C'est de la criminalité qui se déroule dans le cyberespace à l'image de cette qui existe dans la vie physique. En 2020, le montant estimé des pertes financières par la cybercriminalité en Afrique se chiffrait à quatre milliards de dollars selon Franck Kié, consultant, fondateur de CyberObs et commissaire général du Cyber Africa

Forum. Cela témoigne du fait que le continent est plus que jamais exposé à ce phénomène des temps nouveaux.

La Côte d'Ivoire, par la faute des cybercriminels, était considérée comme un pays à haut risque…fiché par les autorités européennes…et inscrit sur la liste rouge des pays à ne plus fréquenter électroniquement (**Bogui, 2010**). En effet, entre 2000 et 2010, le pays était considéré comme une plateforme de la cybercriminalité en Afrique de l'ouest avec le phénomène des « brouteurs » du « broutage ». Aujourd'hui, le préjudice financier pour le pays est estimé en 2021 à 6 milliards de FCA (**Sahi, 2021**). Ces chiffres signifient clairement que la cybercriminalité est toujours d'actualité et que toutes les actions doivent être prises afin de freiner cette délinquance numérique. Ainsi, quelle est la stratégie de lutte contre la cybercriminalité ? Quelles sont les infractions les plus courantes ? Nous partons de l'hypothèse selon laquelle pour être efficace, la stratégie de lutte pour doit d'abord intégrer les aspects règlementaires, un renforcement de la sensibilisation, ensuite l'approfondissement des dimensions de la coopération et enfin l'accentuation de la répression des actes.

L'objectif de cette étude est d'identifier la stratégie de lutte contre la cybercriminalité.

Pour y réponde, nous allons d'abord mettre en évidence des travaux antérieurs réalisés par les chercheurs. Ensuite, il s'agira de cerner le concept de cybercriminalité à travers un éclairage conceptuel selon le point de vue de certains auteurs et institutions sans omettre l'appréhension de ce phénomène au regard des lois ivoiriennes. Après ces éléments, il reviendra de préciser la méthodologie adoptée, les méthodes de collecte des données afin d'aboutir à la présentation et à l'analyse des données. Enfin, avant de passer à la discussion des résultats, un tour d'horizon des types d'infraction des cybercriminels ivoiriens s'avère nécessaire.

1. Synthèse des travaux

Plusieurs travaux scientifiques ont mis en relief la cybercriminalité en Afrique notamment en Côte d'Ivoire.

(**Bogui**, 2010), attirait l'attention à cette période. Selon ses travaux, le développement de l'usage d'Internet avait occasionné de nombreuses menaces sur le rayonnement économique du pays et son image à l'extérieur. En effet, au début de l'année 2008, les fournisseurs d'accès Internet (FAI) avaient constaté que le nombre de courriers électroniques indésirables (ou spams), dont l'objectif est d'escroquer le destinataire, avait atteint des proportions trop importantes. Ainsi, devant la prolifération de ces courriels disséminés à partir de la Côte

d'Ivoire, de nombreux pays africains ont sollicité les autorités ivoiriennes afin que des mesures soient prises pour endiguer ou à défaut maîtriser le phénomène.

Pour (**Anon N'Guessan, 2014**), le développement d'Internet a engendré de nouvelles formes de cybercriminalité en Côte d'Ivoire connu sous le nom de «broutage», l'arnaque en ligne. Ce phénomène consiste à séduire des gens sur internet et ensuite leur soutirer de l'argent. Il a atteint un niveau tel qu'il est devenu un fléau au sein de la jeunesse dans les milieux scolaire et universitaire.

(Koua & al., 2015) quant à eux, ont orienté leur travail sur les aspects psychopathologiques de la cybercriminalité en Côte d'Ivoire. Selon leur recherche, les services psychiatriques sont confrontés à la prise en charge des patients cybercriminels avec troubles mentaux. Leur étude détermine les particularités psychopathologiques et apprécie les modalités de la prise en charge psychiatrique. Comme résultats obtenus, les auteurs soutiennent que le profil psychosocial retrouvé est celui d'un jeune cyber-escroc, déscolarisé, célibataire et présentant un épisode psychotique cannabique. De plus, selon eux, l'évaluation psychopathologique a permis d'une part de retrouver une cyberaddiction avec une durée de connexion hebdomadaire minimale de 28 heures et la survenue, parfois, d'un syndrome de manque à Internet en hospitalisation psychiatrique. D'autre part, ces résultats confirment l'évolution d'une disparition des symptômes psychotiques sous traitement psychotrope ; mais, avec la persistance des activités de cyber-escroquerie sur ce fond de cyberdépendance.

(**Koné, 2015**) mettait en relief l'attitude de certains jeunes cybercriminels le jour et la nuit. Selon lui, l'essentiel de leur activité consiste à séduire des femmes occidentales. Ainsi, le jour, le brouteur est businessman et la nuit, il fait le boucan en déversant les billets de banque au son du coupé décalé[1].

L'étude de (**Bazare & al., 2017**) se penche sur le lien entre les crimes rituels et la cybercriminalité qui a court sur le territoire d'Abidjan. A travers deux communes d'Abidjan, à savoir et Abobo, leur recherche a conclu à la conclusion selon laquelle il n'y a pas un type particulier de cybercriminels qui commet les crimes rituels. Tous s'y adonnent, mais à des fins différentes : la plupart pour envoûter la cible afin d'annihiler toute volonté de résistance et de refus de la cible potentielle. Pour d'autres, les rituels mystiques les aident dans leur

[1] Le coupé-décalé est une danse apparue en 2002 en Côte d'Ivoire et dans la communauté ivoirienne vivant en France notamment dans les milieux ivoiriens de Paris (la JetSet). Il s'inscrit dans le mouvement culturel (ou le concept) plus global qu'est la Sagacité.

entendement, à échapper à la police et à la justice. Ils envoûtent d'autres acteurs du réseau afin de les impliquer tous dans leurs activités. En l'occurrence ce sont les agents de western union, cibles, agents de sécurité et autres qui se voient impliquer.

Pour (**Akadjé & al., 2017**), la cybercriminalité, connue sous la forme du «broutage», est une pratique à laquelle certains jeunes en ont fait une activité criminelle. Il s'agit d'une escroquerie qui consiste à soutirer des biens ou de l'argent à des personnes physiques ou morales par des manœuvres frauduleuses. L'escroquerie est le fait, soit par l'usage d'un faux nom ou de fausses qualités, soit par l'emploi de manœuvres frauduleuses, de persuader de l'existence de fausses entreprises, de faire naître l'espérance ou la crainte d'un succès afin de se faire remettre des fonds. Leur étude ayant pour objectif de connaître la perception des parents vis-à-vis de la pratique du « broutage » analyse la perception de ceux-ci vis-à-vis de ce fléau car la famille constitue la première cellule de socialisation et le creuset de toutes conduites sociales. A travers une enquête de terrain et par la méthode qualitative et quantitative, leur enquête révèle la perception négative des parents vis-à-vis de la pratique du «broutage» dans la grande commune d'Abidjan du nom de Yopougon. C'est la raison pour laquelle, ils estiment que pour réduire cette pratique, il est nécessaire d'impliquer et d'engager les parents dans les campagnes de sensibilisation.

Le rapport publié par (**Interpol, 2021**) sur l'«*Evaluation 2021 des cybermenaces en Afrique, principales observations d'Interpol sur la cybercriminalité en Afrique*», apporte un éclairage essentiel sur la cybercriminalité sur le continent. Fruit d'une collaboration intersectorielle, l'évaluation 2021 recense les menaces les plus importantes existant en Afrique à partir d'éléments communiqués par les pays membres de l'Organisation et de données fournies par des partenaires du secteur privé. Les cinq grandes menaces sont les suivantes :

- les escroqueries en ligne : de faux e-mails ou SMS censés provenir d'une source légitime servent à inciter des personnes à communiquer des informations financières ou à caractère personnel ;
- l'extorsion numérique : les victimes sont amenées par tromperie à partager des images sexuellement compromettantes dans le but de les faire chanter ;
- les escroqueries aux faux ordres de virement : les malfaiteurs piratent les systèmes de messagerie électronique de sociétés afin d'obtenir des informations sur leurs systèmes de paiement puis trompent des salariés pour les inciter à virer de l'argent sur un compte bancaire leur appartenant ;

- les rançongiciels : des cybermalfaiteurs bloquent les systèmes informatiques d'hôpitaux et d'institutions publiques et exigent de l'argent pour rétablir leur fonctionnement ;
- les botnets : des réseaux de machines infectées sont utilisés pour automatiser des cyberattaques à grande échelle.

2. Eclairage conceptuel : la cybercriminalité

La notion de « cybercriminalité » recouvre deux réalités qui sont d'une part, le cyberespace et d'autre part, la criminalité. Ces deux réalités méritent d'être explicitées afin de mieux appréhender la cybercriminalité.

En effet, même s'il est aussi difficile de définir le cyberespace tout comme la cybercriminalité, l'on peut dire que c'est l'espace engendré par Internet et de l'ensemble des mondes dits virtuels. Il s'agit à la fois de la totalité des éléments qui composent Internet, en partant des câbles, serveurs, routeurs jusqu'aux satellites et appareils connectés présents sur le territoire physique et politique. C'est donc une zone où gravitent les informations, les idées, les programmes et les services interconnectés où communiquent les acteurs, situés de part et d'autre du monde. Ces interconnexions donnent naissance à une étendue massive de données stockées et partagées.

Dans ce sens (**Douzet, 2016**) affirme que cette notion est composée de l'infrastructure physique, du territoire géographique physique et politique et de l'espace intangible

> c'est d'abord et avant tout un espace d'information généré par l'interconnexion globale des systèmes d'information et de communication, dans lequel les données sont créées, stockées et partagées. Le terme désigne à la fois : l'infrastructure physique qui est à la source de cet environnement, à savoir les différents éléments qui composent l'internet ce réseau planétaire de réseaux informatiques comme les câbles, les serveurs, les routeurs, les satellites et tous les appareils connectés qui sont ancrés dans le territoire géographique physique et politique ; et l'espace intangible dans lequel circulent les données, l'information et les idées, l'espace où se produisent des interactions entre les individus qui sont derrière leur écran partout dans le monde à une vitesse quasi instantanée. (Douzet, 2016).

Quant à (**Joël de Rosnay, 1995**), celui-ci considère que

> le cyberspace incarne le monde virtuel qui naît des informations échangées par les hommes dans les réseaux de communication. […] Le monde d'Internet est un cyberspace. Il créé les conditions d'une nouvelle citoyenneté électronique… Mais le cyberspace est encore une jungle, bruissant de mille dangers, où l'on peut se perdre. Un Far West numérique au sein duquel pirates et escrocs évoluent à leur guise. Le cyberspace est un océan illimité, une terra incognita sur laquelle on s'aventure avec des cartes rudimentaires. (de Rosnay, 1995).

Selon cette conception, le cyberespace est un nouveau territoire virtuel calqué sur le monde réel dans lequel l'on retrouve des gens bien et des criminels de tous acabits. Après avoir explicité la notion de cyberespace, passons à celle de criminalité.

De façon générale, la criminalité est l'ensemble des actes illégaux, délictueux et criminels, commis dans un milieu donné, à une époque donnée. Cela peut couvrir un large éventail d'activités, y compris les activités terroristes et l'espionnage menés à l'aide d'Internet et le piratage illégal de systèmes informatiques, les infractions liées au contenu, le vol et la manipulation de données, et le cyberharcèlement. Le cyberespace est devenu criminogène. Il est devenu un lieu d'actes répréhensibles. Cette criminalité pourrait avoir pour synonyme la délinquance. De cette définition (**Daniel Martin & Frédéric-Paul Martin 2001**) qualifient cette infraction de « criminalité informatique » et la définissent comme

> toute action illégale dans laquelle un ordinateur est l'instrument ou l'objet du délit, tout délit dont le moyen ou le but est d'influencer la fonction de l'ordinateur, tout acte intentionnel, associé d'une manière ou d'une outre à la technique informatique, dans laquelle un ordinateur est l'instrument ou l'objet du délit, tout délit dont le moyen ou le but est d'influencer la fonction de l'ordinateur, tout acte intentionnel, associé d'une manière ou d'une outre à la technique informatique, dans laquelle une victime a subi ou aurait un préjudice et dans laquelle l'auteur a tiré ou aurait pu tirer un profit »

Ces deux notions ainsi définies, alors qu'en-est-il de la cybercriminalité ?

Cette notion recouvre aussi une variété de définitions selon les auteurs et les organisations. Selon l'Organisation des Nations Unies (ONU, 2000), la cybercriminalité est *« tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent »*, et dans une acception plus large *« tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique ».*

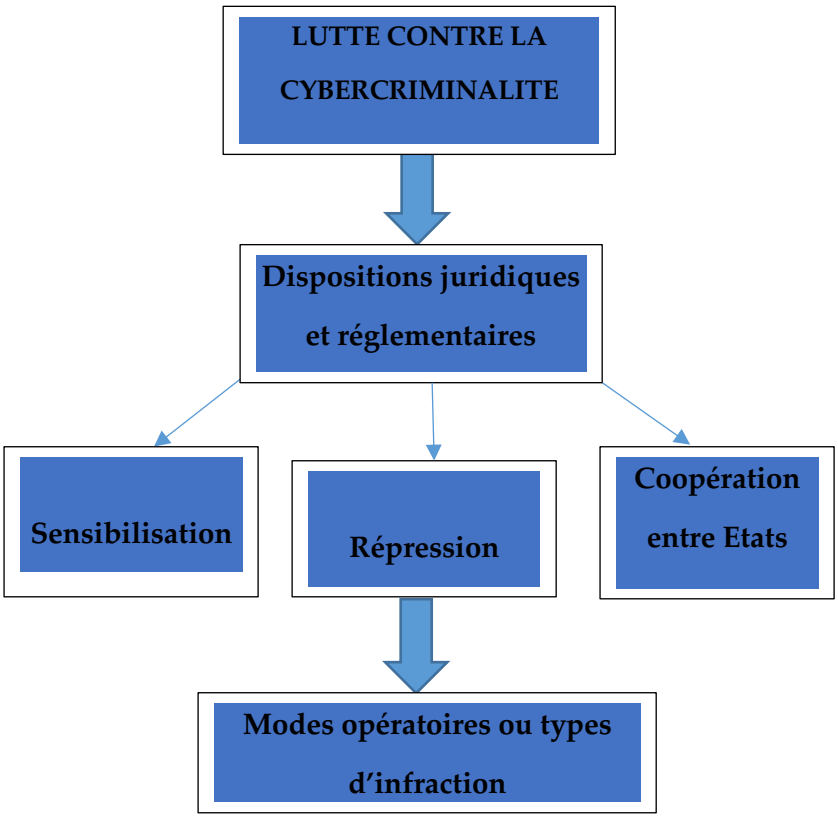
Pour (**Ghernaouti-Hélie & Dufour, 2012**),

> La cybercriminalité se définit comme toute activité criminelle réalisée au travers du cyberespace et par le réseau Internet. Par extension, elle intègre toute forme de malveillance électronique effectuée à l'aide des technologies informatique et de télécommunication (téléphonie, cartes à puces…). Qu'il s'agisse de fraude, d'escroquerie, d'extorsion, de vandalisme ou de harcèlement par exemple, les comportements malveillants ou criminels exploitent les caractéristiques d'Internet et portent préjudice aux internautes, aux organisations et à la société.

En Côte d'Ivoire, la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité la définit comme : *« l'ensemble des infractions pénales qui se commettent au moyen ou sur un réseau de télécommunication ou un système d'information ».* La cybercriminalité est donc l'ensemble des infractions traditionnelles classiques comme le vol, l'usurpation d'identité, le chantage mais commises cette fois-ci au moyen d'un système d'information, notamment internet et aussi des infractions propres aux technologies de l'information et de la

communication comme l'accès frauduleux à un système d'information. La stratégie de lutte contre ce fléau des temps nouveaux se modélise à la figure 1 comme suit : la mise en place de dispositions juridiques et réglementaires aboutit à trois étapes : sensibilisation, répression et coopération entre les Etats. Ces différentes phases aboutissent à un état des lieux des modes opératoires ou types d'infraction.

Figure 1 : Modèle conceptuel de la lutte contre la cybercriminalité en Côte d'Ivoire



Source : Auteurs

3. Méthodologie

Notre corpus repose sur un ensemble de données qualitatives et quantitatives. Si les données qualitatives s'appuient sur des impressions, opinions et avis pour recueillir des informations destinées à décrire la cybercriminalité, les données quantitatives elles, sont principalement sous forme numérique (chiffres, statistiques…). Elles concernent les chiffres et statistiques provenant de ce fléau.

Ces données ont été collectées de deux façons : Sur le réseau social numérique Facebook et par l'entremise de la recherche documentaire. Il s'est agi pour nous d'explorer les publications de la page Facebook de la Plateforme de Lutte Contre la Cybercriminalité (PLCC), (*plus de*

192 000 membres), du 11 juin au 26 décembre 2021. A ce sujet, il nous a fallu par moments faire des captures d'écran dans la collecte de l'information. Au niveau de la recherche documentaire, l'objectif a été de documenter la cybercriminalité durant tout le mois de décembre 2021.

Cette quête d'informations a consisté à identifier, collecter et traiter des informations en s'appuyant sur des sources fiables sur la cybercriminalité. Ces données émanent d'articles scientifiques, d'articles de presse en ligne, de thèses de Doctorat, de mémoires de recherche, de rapports de la Direction de l'Informatique et des Traces technologiques (DITT), de la PLCC, d'Interpol, de l'Union Internationale des Télécommunications (UIT) et de l'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI).

Les données ont fait l'objet d'une analyse de contenu qui consiste en un examen systématique et méthodique de documents textuels ou visuels. D'après (**Mucchielli, 1984**), *« l'analyse de contenu (d'un document ou d'une communication), c'est par des méthodes sûres, rechercher les informations qui s'y trouvent, dégager le sens ou les sens de ce qui y est présenté, formuler et classer tout ce que contient ce document ou cette communication »*.

Cette étude fonde son ancrage théorique sur l'appropriation sociale des technologies dont le précurseur est **(Michel De Certeau, 1990**). Cette théorie s'intéresse aux pratiques de la vie quotidienne des usagers. Ils ne vont pas rester passifs et dociles dans l'usage des technologies. Au contraire, à l'analyse, les usagers font preuve de créativité en raison des pratiques qui s'écartent des modes d'utilisation prescrits. Et pour lui, ces détournements d'usages sont qualifiés d'appropriation sociale des technologies. Le sens du terme appropriation est donc ici *« rendre propre à un usage, faire sien, s'attribuer la propriété, s'en rendre maître »* (**Plantard & ali., 2020**).

L'appropriation individuelle d'une technologie est le processus par lequel l'usager l'intègre à sa vie quotidienne tout en l'adaptant à sa personnalité et à ses besoins. Dans le cadre de notre travail, certaines personnes utilisent internet, la technologie ou des systèmes d'information à des fins criminelles alors que les concepteurs eux, n'avaient jamais pensé à ce type d'usage détourné ; c'est ce qui fonde l'usage de cette théorie.

4. Présentation et analyse des données

4.1. Les dispositions juridiques et réglementaires

Avant de présenter les dispositions nationales en matière de lutte contre la cybercriminalité, il convient de faire un tour d'horizon général dans la lutte contre ce phénomène. Selon (**Tano-**

Bian, 2015), le continent africain accuse un certain retard dans ce domaine : *« l'Afrique n'est pas encore dotée de système de surveillance d'internet à l'image de certains Etats comme la Chine, le Brésil ou même le Canada et l'Afrique du Sud qui se sont dotés de système de surveillance d'internet ».*

Si d'une façon générale l'Afrique accuse un retard dans la lutte contre ce phénomène cela reviendrait à dire également que ce retard est à relever au niveau des Etats. En Côte d'Ivoire, trois (3) principaux textes régissent le principal outil théorique de lutte contre la cybercriminalité.

Le premier texte est la loi n°2013-450 du 19 juin 2013 relative aux transactions électroniques qui fixe le cadre juridique de la protection des données à caractère personnel et de la lutte contre la cybercriminalité. Ainsi, il :

- fixe le régime juridique applicable à tout traitement de données à caractère personnel, notamment la déclaration et l'autorisation (Art 5 à 13);
- précise les principes fondamentaux du traitement des données (les principes de légitimité, de finalité, de sécurité et confidentialité, de proportionnalité et de transparence…) ;
- reconnaît plusieurs droits à la personne dont les données sont traitées (le droit à l'information, le droit d'accès, le droit d'opposition, le droit de rectification ou de suppression) ;
- prévoit des sanctions pénales à l'encontre du Responsable du traitement qui violerait ces dispositions (Art 14 à 25).

Le deuxième texte est la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité. Elle fait la part belle aux atteintes aux systèmes informatiques, aux atteintes aux systèmes de cryptologie et aux atteintes aux systèmes automatisés des données (STAD). Elle traite :

- les atteintes à la confidentialité (l'accès frauduleux et le maintien frauduleux dans un système informatique) ;
- les atteintes à l'intégrité (altération des systèmes, qui consiste dans l'action ou la tentative, soit de fausser le fonctionnement du système, soit d'en entraver le fonctionnement) ;
- les atteintes à la disponibilité des systèmes informatiques (d'introduire ou de tenter d'introduire des données dans un système informatique de manière frauduleuse

Le troisième texte est la loi n°2013-546 du 30 Juillet 2013, relative aux transactions électroniques. Elle :

- met à la charge du commerçant une obligation d'information de sa clientèle sur son identification ;
- prescrit des règles sur la publicité par voie électronique (précisions, identification de la publicité et de la personne pour le compte de qui elle est faite) ;
- exige un consentement préalable avant toute prospection directe par envoi de message au moyen d'un automate d'appel ou d'un short message service (SMS) ;
- le non-respect de ces obligations est sanctionné par une peine d'emprisonnement de 1 à 5 ans et d'une amende de 1 à 10 millions FCFA ;
- reconnait la valeur juridique de la signature électronique et du message électronique dès lors qu'ils assurent avec certitude l'identification des signataires et l'Authentification du message ;
- consacre la confidentialité des échanges par le chiffrement des messages.

Selon le juriste (**Désiré Alléchi, 2021**)

> *Au regard de l'évolution des méfaits constatés dans le domaine du numérique en Côte-d'Ivoire, les autorités étatiques décident de durcir le ton en entamant un processus de modification de certains articles de la loi ivoirienne en matière de cybercriminalité. Le Conseil des Ministres du mercredi 08 septembre 2021 a adopté le projet de loi modifiant les articles 17, 33, 58, 60, 62 et 66 de la loi ivoirienne précitée au motif que : « ce dispositif s'avère peu dissuasif, compte tenu de la criminalité cybernétique qui persiste et devient multiforme ».*

Concrètement, cette modification consiste à doubler le quantum des peines encourues par les auteurs de ces types d'infractions. Ces articles sont relatifs à la pornographie infantile (17), aux atteintes à la propriété intellectuelle (33), à la détention…partage par le biais d'un système d'informations à caractère racial (58), aux injures ou invectives proférées par le biais des systèmes d'information (60), aux faits de nature à troubler l'ordre public ou la vie humaine (62), aux menaces de porter atteinte à des biens ou à des personnes par le biais d'un système d'information (66).

Le juriste explique que la modification de ces différents articles est la preuve manifeste du dépassement des sanctions prévues par la loi en ces termes :

> *La modification d'un texte juridique devrait selon notre raisonnement dans le cadre de cet article, être la résultante soit du caractère désuet du texte soit du caractère non dissuasif des sanctions prévues par ce texte. Dans la première situation, c'est le cas de figure où le texte en question n'arrive plus à coller avec la réalité. C'est-à-dire que le texte fait référence à des*

> *faits qui ne sont plus actuels. Quant à la deuxième situation, il est question du cas de figure où malgré l'existence de textes actuels réprimant le fait incriminé et le prononcé de sanctions après jugement des personnes qui se rendent coupables de ces faits, l'on ne cesse de constater la commission des mêmes infractions (idem).*

Dans l'élan de la lutte contre la cybercriminalité, il a été créé à la Police nationale, la Direction de l'Informatique et des Traces Technologiques (DITT) par le Ministère de l'Intérieur et de la Sécurité afin de renforcer la lutte contre la cybercriminalité. Ainsi, l'on a assisté à la naissance le 02 Septembre 2011 de la Plateforme de Lutte Contre la Cybercriminalité (PLCC) et la mise en place du CI-CERT (Côte d'Ivoire Computer Emergency Response Team). Cette plateforme est le fruit d'un accord entre la Direction Générale de la Police Nationale de Côte d'Ivoire et l'ARTCI. Les compétences opérationnelles et techniques de la PLCC dans le domaine de la cybercriminalité, recouvrent les infractions spécifiques liées aux nouvelles technologies et celles dont la commission est facilitée par l'usage de ces mêmes technologies. Pour répondre aux nouveaux enjeux de la lutte contre la cybercriminalité, les services chargés de l'application de la loi doivent adopter une nouvelle approche en matière d'échange d'informations de police, capable de soutenir le rythme rapide des développements des enquêtes sur la cybercriminalité et de l'informatique légale.

4.2. La sensibilisation

Dans les prérogatives qui lui sont dévolues, la PLCC dans sa stratégie de lutte contre la cybercriminalité organise de façon permanente la sensibilisation des acteurs dans le cyberespace. L'exploration de la page Facebook de cet instrument de lutte révèle que des campagnes de sensibilisation sont régulièrement menées.

Sensibiliser, c'est conscientiser, de rendre sensible, réceptif, attentif à quelque chose pour lequel on ne manifestait pas d'intérêt auparavant. La sensibilisation est donc l'action qui consiste à rendre une personne ou un groupe de personnes réceptifs à quelque chose qui peut être un problème dans une communauté, un comportement à adopter vis à vis d'une situation donnée.

La PLCC attire toujours l'attention des internautes sur une variété de sujets.

Les figures 2, 3, 4 et 5 illustrent clairement ces campagnes. A la figure 2, la PLCC donne des conseils pour ne pas être victime de cyberescroquerie lors de la navigation.

Figure n°2 : Comment éviter la cyberescroquerie ?

Capture n°1

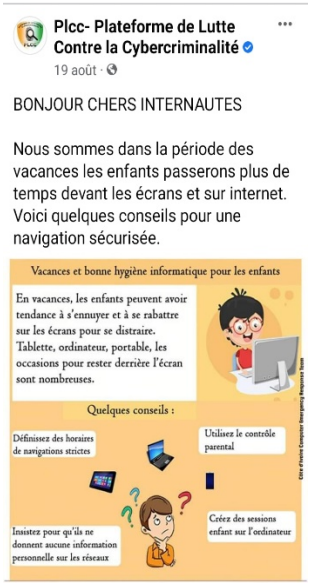
Figure n°3

Faire son shopping en ligne

Capture n°2

Figure n°4

Attention aux écrans !



Capture n°3

Figure n°5

Attention au cyberharcèlement

Capture n°4

Source : Auteurs

Si la figure 3 sensibilise à la sécurité des achats en ligne, les 4 et 5 font la part belle à la protection des enfants dans le cyberespace. Les enfants plus que tous, doivent faire l'objet d'un traitement préventif parce qu'ils sont beaucoup plus fragiles. C'est pourquoi, la PLCC attire l'attention des parents parce qu'ils peuvent être victimes de cyberharcèlement.

En collaboration avec la PLCC, certains organismes à l'image de la Jeune Chambre Internationale (JCI) sensibilisent la jeunesse dans plusieurs communes de Côte d'Ivoire. Ainsi, ces deux structures ont organisé une campagne de sensibilisation à l'intention des jeunes pour un meilleur usage de l'internet et des nouvelles technologies de l'information. Cette cérémonie s'est tenue dans le hall du centre commercial Cosmos de Yopougon avait pour objectif principal de faire prendre conscience à cette frange de la population des risques encourus sur la toile (en tant que potentiels victimes) ou sur le plan pénal en tant que cyber délinquants.

Dans même élan, l'opérateur de téléphonie mobile, MTN Côte d'Ivoire et ses partenaires, avec l'appui de la PLCC et de la Police scientifique, ont organisé à l'intention des élèves des élèves du lycée moderne de la commune d'Abobo, la campagne « Protection des enfants en ligne ». Elle portait sur les dangers auxquels les jeunes sont confrontés et a attiré leur attention sur le comportement à adopter sur Internet. Ce type de campagne a été organisé avec les mêmes acteurs au collège moderne du Plateau pour un bon usage d'internet mais cette fois-ci avec la participation du Fonds des Nations unies pour l'enfance (Unicef).

A Korhogo, c'est le bureau de l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO) en collaboration avec le ministère de la Communication, des Médias et de la Francophonie et la PLCC qui ont organisé la caravane de sensibilisation contre les fake news et la cybercriminalité dénommée « Education aux médias et à l'information », (Emi Tour). Cette campagne de sensibilisation visait à développer l'esprit critique des jeunes universitaires contre les fake news et la cybercriminalité. Il ressort que l'objectif spécifique est de faire un usage responsable des réseaux sociaux numériques, d'en percevoir les richesses autant que les limites et les dangers. Cette campagne de sensibilisation porte en général sur un total de 25 000 élèves et étudiants par an.

4.3. La coopération entre Etats

La cybercriminalité constitue l'une des formes de criminalité transnationale qui connaît le développement le plus rapidement dans les pays. Elle est un phénomène qui s'affranchit des frontières physiques. En conséquence, les services chargés de l'application de la loi doivent surmonter les défis des enquêtes transfrontalières, les différences entre les systèmes juridiques et la disparité des capacités.

L'Afrique en général est confrontée à ce défi parce que les menaces ne peuvent être pleinement prises en charge que par le développement d'une solide culture de la cybercriminalité, la

création de capacités d'intervention robustes et l'adoption de politiques nationales appropriées et efficaces. Compte tenu de la complexité et des dimensions multiples de ce phénomène, la protection et la prévention contre les activités criminelles dans le cyberespace à travers le monde nécessite la coopération et la coordination de toutes les parties concernées aussi bien à l'intérieur et entre les pays. Étant donné l'importance du secteur des TIC et son impact direct et positif sur le développement social et économique des pays Africains, il existe un besoin urgent de développer une approche globale et une stratégie cohérente en matière de cyber sécurité au niveau continental pour promouvoir la paix et la sécurité dans la société de l'information.

En ce qui concerne la Côte d'Ivoire, la lutte contre la cybercriminalité nécessite un accroissement de la coopération entre le pays et le reste des pays africains d'une part et entre les pays d'Afrique et les Etats industrialisés d'autre part. En ce sens, la PLCC intensifie désormais sa coopération avec les services de sécurité des Etats étrangers parce que toutes les plaintes contre ces délinquants ne sont pas toutes localisées en Côte d'Ivoire. Dans une région africaine où le banditisme informatique est en plein essor, la lutte contre ce fléau commande des procédures particulières et une synergie d'action plus accrue, tant des partenaires nationaux, sous régionaux qu'internationaux.

L'importance de la coopération entre les Etats a amené Aristide Ouattara, expert en cybercriminalité d'affirmer :

> *La collaboration internationale est très importante. Parce que vous pouvez être attaqué en Côte d'Ivoire par un hackeur basé en Corée du Nord. Donc il faut mettre en place des systèmes de surveillance internationaux. Alors on va avoir des partenariats à plusieurs niveaux. Dans la défense, on va avoir des spécialistes de l'armement. On parle aussi beaucoup d'objets connectés (Source : Deutsche Welle, la radio internationale allemande).*

Les organisations criminelles privilégient de plus en plus Internet pour faciliter leurs activités et réaliser des bénéfices maxima en un minimum de temps. La criminalité de très haute technologie comme le piratage informatique, les attaques par logiciel malveillant, et l'extorsion DDoS, représente une menace réelle pour la sécurité des gouvernements, des entreprises, et des particuliers. Elle présente, en outre, d'importants défis pour les services chargés de l'application de la loi, car de nombreux pays ne disposent pas encore de la connaissance ou des compétences techniques nécessaires pour y faire face. L'utilisation accrue de la technologie pour commettre les infractions comme les vols, la fraude et même le terrorisme ajoute une nouvelle dimension à ces activités criminelles « traditionnelles ». Cette coopération a amené le pays a ratifié la Convention de Budapest sur la criminalité en mars 2019. Cette ratification permet aujourd'hui

à la Côte d'Ivoire de bénéficier d'une collaboration internationale dans sa lutte contre la cybercriminalité.

> *La Convention de Budapest sur la cybercriminalité répond à la forte volonté des Etats de mettre en œuvre une politique pénale commune destinée à protéger les populations contre la criminalité dans le cyberespace. Cet instrument juridique vise à harmoniser les législations nationales pénales tout en fournissant les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions commises au moyen d'un système informatique. L'adhésion de la Côte d'Ivoire à la Convention de Budapest témoigne de sa forte implication dans la lutte contre la cybercriminalité et de son attachement à la coopération internationale en matière de cybersécurité. (Source : Business France, Communiqué du Conseil des Ministres).*

Selon (**Pereira, 2016**), la Convention de Budapest met en évidence neuf types d'infractions[2] : l'accès illégal aux systèmes et données informatiques, tel que le piratage ; l'interception illégale ; l'atteinte à l'intégrité des données ; l'atteinte à l'intégrité des systèmes (virus, spam et déni de service) ; le marché noir de la production ou la vente de moyens de commettre les infractions (infractions d'abus de dispositif) ; la fraude informatique ; la falsification informatique ; les infractions se rapportant à la pornographie enfantine ; les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes. Des sommets, des colloques, des forums sont organisés en partenariat avec le Conseil de l'Europe, l'Union européenne, Interpol, le Département de la Justice des Etats-Unis, le Gouvernement britannique, le Secrétariat du Commonwealth, l'Office des Nations unies contre les drogues et le crime (UNODC). La France singulièrement et d'autres pays accompagnent des pays africains. Cet accompagnement se traduit au plan de la formation des policiers et de dons d'équipements. Au Bénin par exemple, un laboratoire financé par Paris permet de remonter à des preuves cachées au sein d'un ordinateur ou d'un téléphone mobile perquisitionné. La Côte d'Ivoire dispose pour sa part d'un centre de surveillance du cyberespace en temps réel.

Par ailleurs, en fonction des enquêtes liées aux plaintes qui sont déposées, la PLCC coopère et collabore également avec plusieurs Etats afin de résoudre les affaires. Les pays ont le devoir de créer une bonne capacité de réaction et de collaboration. Dans ce sens, plusieurs rencontres sous régionales sont organisées afin d'échanger des informations, des expériences et des stratégies dans la lutte dont le dernier projet en date : Ocwar-C (Réponse ouest-africaine à la cybersécurité et à la lutte contre la cybercriminalité). Ce projet visant à financer les stratégies de lutte contre la cybercriminalité est financé par l'Union européenne plus de 5 milliards de FCFA et mis en

[2] La convention relative à la lutte contre la cybercriminalité s'étend au-delà des seuls États membres du Conseil de l'Europe. 55 pays l'ont adoptée dont le Canada (2015), l'Australie (2013), les États-Unis (2007) et le Japon (2012).

œuvre par Expertise France[3]. D'une durée de 48 mois, du 1er février 2019 au 31 janvier 2023, concerne les pays tels que le Bénin, le Cap-Vert, la Côte d'Ivoire, le Burkina Faso, la Gambie, le Ghana, le Togo, la Guinée, le Sénégal, le Liberia, la Guinée-Bissau, le Mali, le Niger, le Nigéria, la Mauritanie et la Sierra-Leone.

4.4. La répression

La répression est l'acte de réprimer. Réprimer c'est punir, c'est sévir contre. Après les textes juridiques et réglementaires, la sensibilisation, la coopération entre Etats, la PLCC dans sa stratégie de lutte contre la cybercriminalité n'hésite pas à sanctionner et à sévir contre les auteurs de délinquance numérique.

Selon le premier responsable de cette structure, la PLCC traite en moyenne 4 500 à 5 000 plaintes par an contre 150 en 2011 et 50% d'entre elles sont généralement résolues. Il suffit de parcourir sa page Facebook pour s'en convaincre. Ainsi, depuis le mois de juin 2021, plusieurs individus indélicats ont été mis aux arrêts après enquêtes. Nous allons parcourir ces cas depuis le mois de juin 2020.

Le 26 octobre 2021, les investigations menées par la PLCC avec l'appui du Laboratoire de Criminalistique Numérique (LCN), ont permis de remonter à KVA. Interpellé puis conduit dans les locaux de la PLCC, il reconnaitra être l'utilisateur du compte Facebook Patri Axan et l'auteur des menaces de harcèlement et menace de publication d'images à caractère sexuel à l'encontre de dame AYI.

Le 07 octobre 2021, un individu aux initiales de DM a été conduit devant le parquet pour usurpation frauduleuse d'éléments d'identification de personne physique, menaces de publication d'images à caractère sexuel, escroquerie par le biais d'un système d'information et homicide involontaire.

Le 25 août 2021, la PLCC avec l'appui du LCN a appréhendé l'indélicat SBH et conduit devant le parquet pour menace de publication d'image à caractère sexuel sur internet suivie de tentative d'escroquerie.

Le 20 août 2021, les investigations menées par la PLCC avec l'appui du LCN, ont permis de remonter à l'individu KI, ex-employé de celui ayant pour initiales DC. Il a été conduit devant

[3] Expertise France est l'agence publique française de conception et de mise en œuvre de projets internationaux de coopération technique.

le Parquet d'Abidjan pour utilisation frauduleuse d'éléments d'identification de personne physique et escroquerie.

Le 16 août 2021, après les investigations de la PLCC, MA a été conduit devant le Parquet d'Abidjan pour utilisation frauduleuse d'éléments d'identification de personne physique, atteinte à la dignité, escroquerie et tentative d'escroquerie.

Le 13 août 2021, les enquêtes menées par la PLCC avec l'appui du LCN ont permis d'appréhender ZBA et ZBE. Ils ont été conduits devant le parquet pour utilisation frauduleuse d'éléments d'identification de personne physique, d'atteinte à la dignité humaine suivie d'escroquerie.

Le 11 août 2021, EMA a été conduit devant le Parquet d'Abidjan pour utilisation frauduleuse d'éléments d'identification de personne physique, de publication d'images à caractère sexuel suivie de tentative d'escroquerie.

Le 2 août 2021, la PLCC a mis la main sur les sieurs CPB puis SS. Ceux-ci ont été interpellés puis conduits dans les locaux de la PLCC et poursuivis par le Parquet d'Abidjan pour fraude et complicité de fraude à l'examen du Baccalauréat session 2021 au moyen d'un système d'information.

Le 28 juillet 2021, OAJ a été interpellé par la PLCC et poursuivi par la justice ivoirienne pour utilisation frauduleuse d'éléments d'identification de personne physique (usurpation d'identité) suivie d'escroquerie.

La liste des cas de répression pour l'année 2021 est longue. L'essentiel ici est de montrer que tous les individus reconnus coupables d'infraction dans le cyberespace où à partir d'outils numériques sont effectivement appréhendés, jugés et sanctionnés par les peines prévues par la loi. La PLCC est au contact des citoyens victimes d'actes de cybercriminalité et de crime technologique. Elle reçoit des plaintes, enquête et fait des interpellations.

5. Les modes opératoires ou les types d'infraction

La PLCC reçoit chaque année entre 4 500 et 5 000 plaintes par an. Les modes opératoires sont divers. Toutefois, pour l'année 2020-2021 en Côte d'Ivoire, cinq (5) grands modes opératoires ont été identifiés en termes d'infraction. Il s'agit de :

- l'atteinte à la dignité humaine ;
- la fraude sur les transactions électroniques ;
- l'utilisation frauduleuse d'éléments d'identification ;

- l'atteinte à l'image et à l'honneur ;
- l'escroquerie sur Internet.

En effet, la PLCC a reçu près de 1200 plaintes sur 5000, soit 24% concernant l'atteinte à la dignité humaine. Les atteintes à la personne désignent toutes les formes d'infractions qui ont pour motivation ou pour effet de porter atteinte à l'intégrité physique ou psychologique d'autrui. Cette infraction concerne les menaces de tous genres, les menaces d'images, les menaces de publication à caractère sexuel ou les publications d'image à caractère sexuel.

Le deuxième type concerne la fraude sur les transactions électroniques, la PLCC a traité 1000 cas sur 5000 soit 20% des plaintes. Cette infraction est relative aux arnaques et vols de tous genres sur les transferts d'argent par mobile money. Le troisième type est l'utilisation frauduleuse d'éléments d'identification. Elle a fait l'objet de 900 plaintes soit 18% et concerne la duplication de comptes des réseaux sociaux numériques Facebook, Instagram ou Twitter…

L'atteinte à l'image et à l'honneur se classe en quatrième position avec 500 plaintes, soit 10 % du volume des plaintes. Il s'agit des injures, des diffamations, les harcèlements. L'on a en cinquième position, l'escroquerie sur Internet dont entres autres, les faux achats, fausses ventes en ligne, les fausses bourses d'étude, les promesses d'emploi autour de 400 plaintes par an. Ces 5 grandes catégories forment la typologie des infractions en Côte d'Ivoire durant l'année 2021.

Les préjudices financiers se situent dans les accès frauduleux aux systèmes d'information qui se chiffrent à deux (2) milliards de franc CFA sur un ensemble de six (6) milliards de franc CFA pour l'ensemble des préjudices financiers.

6. Discussion

La cybercriminalité progresse dans un monde où les TIC sont omniprésentes et régissent notre quotidien. La lutte contre ce fléau est mondiale car la menace se développe et nécessite une réponse continentale. Pour ce faire, l'Afrique, si elle veut tirer tous les bénéfices de l'économie numérique doit impérativement mettre tous les atouts de son côté dans cette grande société de l'information.

Pour la Côte d'Ivoire comme pour la plupart des pays africains, les « indices » électroniques susceptibles d'identifier les auteurs d'actes de cybercriminalité sont souvent détenus par des entités privées comme les fournisseurs d'accès à Internet ou les compagnies de téléphonie mobile. Même si l'on remarque une avancée dans la coopération au sein des différentes institutions, il existe néanmoins encore des blocages au niveau de ces structures qui sont

incapables de ressortir l'identité d'un individu derrière une adresse IP. Mieux pour le pays et ses habitants, les préjudices sont en termes d'image de marque comme le souligne (**Bogui, 2010**) pour qui la cybercriminalité pose un problème d'image du pays et des citoyens ivoiriens à l'extérieur qui ne cesse de se dégrader. Or, selon (**Boukarnaoui & Attouche, 2021**), les spécialistes de l'image de marque d'une nation estiment qu'un pays est un ensemble soumis à la perception du reste du monde. Cette vision appelée sous le terme de «Nation Branding» (NB) a vu le jour par Simon Anholt en 1996 et a considéré l'image de marque d'une nation comme un moyen pour les pays d'améliorer leur réputation internationale. C'est donc dire combien de fois l'image d'un pays est un facteur important de retombées économiques.

Au cours des années 2000, la cybercriminalité était connue sous le nom de «broutage». Elle était devenue une véritable gangrène pour la jeunesse dans les milieux scolaire et universitaire (**Anon N'guessan, 2014**).

Selon cet auteur, cette pratique qui commence généralement par des petites arnaques, débouche parfois à des pratiques mystiques appelées «zamou». En effet, pour atteindre leurs objectifs, les «brouteurs» s'attachent souvent les services de mystiques pour envoûter leurs victimes afin que celles-ci cèdent le plus facilement aux mensonges et autres stratagèmes mis en œuvre par le cyberescroc, pour soutirer le maximum d'argent. Au final, l'on peut identifier plusieurs causes de la cybercriminalité dont la crise de l'école, les problèmes financiers, l'absence d'autorité parentale, l'appât du gain facile, le chômage des jeunes et l'accessibilité d'internet et des terminaux mobiles et l'anonymat que garantit les technologies mobiles dans un monde de plus en plus connecté.

Dans cet ordre d'idée (**Bazare & al., 2017**) soutiennent que dans la pratique, les actes du «zamou» peuvent être commis dans le cadre de trafics d'organes ou de d'événements politiques tels que (les campagnes électorales, nominations, remaniements ministériels, promotion…), ou à des fins d'impunité (comme échapper aux mailles de la justice), ou simplement pour arnaquer, «brouter» (envoûter la cible afin de la contraindre à remettre la somme demandée). L'objectif de toutes ces formes de «zamou» serait de pactiser avec une entité mystique à travers (du sang humain, une partie du corps, des secrétions humaines, etc.…). C'est donc dire combien de fois les jeunes sont prêts à tout pour le gain facile. La jeunesse ne veut plus étudier pour avoir des diplômes et espérer obtenir un emploi pour gagner de l'argent. L'on est en droit de s'interroger sur la mentalité de la jeunesse africaine quand on sait que le développement d'un pays repose sur celle-ci. En effet, si les jeunes qui sont sensés faire avancer leur pays s'adonnent à ce genre

de pratiques inutiles, alors il sera difficile aux pays africains de pouvoir progresser en vue de concurrencer les autres nations du monde. C'est pourquoi il serait plutôt intéressant de développer l'ingéniosité de cette frange de la population leur appropriation de la technologie à de meilleurs fins en vue de contribuer à la promotion de leur génie créateur et à l'essor réel de la révolution numérique dans les pays en développement.

Conclusion

Dans un contexte marqué par l'évolution constante des technologies numériques avec l'essor d'Internet, la cybercriminalité figure parmi les formes de criminalité transnationale qui progressent le plus rapidement. En Côte d'Ivoire, l'on pourrait affirmer qu'il existe une stratégie de lutte contre la cybercriminalité. Elle repose d'une part sur la création de la Plateforme de Lutte Contre la Cybercriminalité. D'autre part, elle réside aussi sur un arsenal juridique et réglementaire renforcé en 2021 pour être à jour de l'évolution de ce fléau, sur la sensibilisation des jeunes élèves et étudiants (ils sont majoritaires dans le cyberespace ivoirien), la coopération entre les Etats pour une synergie d'actions pour être plus efficace, et une campagne de répression. Au nombre des typologies d'infraction, cinq (5) grandes catégories sont identifiées à savoir l'atteinte à la dignité humaine ; la fraude sur les transactions électroniques ; l'utilisation frauduleuse d'éléments d'identification ; l'atteinte à l'image et à l'honneur et l'escroquerie sur Internet. La lutte contre la cybercriminalité est une activité complexe et de longue haleine. Elle nécessite non seulement de la clairvoyance dans le cyberespace mais aussi la participation de tous les cybercitoyens. La cybercriminalité laisse entrevoir d'importants enjeux sécuritaires, économiques et éducationnels dans les pays en développement. Alors que le pays renoue avec la croissance et que les investisseurs affûtent leurs arguments pour saisir au bond les opportunités d'affaires ; ce n'est pas le moment de laisser des individus cachés derrière des écrans d'ordinateurs, saboter les efforts accomplis. C'est la raison pour laquelle il est urgent pour le gouvernement ivoirien d'envisager une réponse technologique et juridique appropriée face à l'évolution constante de ce fléau tel que constaté depuis des années.

BIBLIOGRAPHIE

- Akadje A. M., Zady C., & Wilfried A. J. (2017). Parents Et ‘‘Broutage’’ À Abidjan. *European Scientific Journal, ESJ*, *13*(5), 285. https://doi.org/10.19044/esj.2017.v13n5p285.
- Allechi Désiré (2021), « Opportunité de réviser certains articles de la loi ivoirienne relative à la cybercriminalité », sur https://www.village-justice.com/articles/opportunite-revision-des-articles-loi-ivoirienne-no2013-451-relative-lutte,40610.html
- Anon N. (2014), la pratique de la cybercriminalité en milieux scolaire et universitaire de Côte d’Ivoire. Cas des élèves et étudiants du district d’Abidjan, *European Scientific Journal*, 31.
- Bazare R. N., Ladji, B., & Kadidja, D. (2017). Cybercriminalité ou "Broutage" et Crimes Rituels à Abidjan: Logiques des Acteurs et Réponses au Phénomène Cas des Communes de Yopougon et d’Abobo. *European Scientific Journal, ESJ*, *13*(23), 104. https://doi.org/10.19044/esj.2017.v13n23p104.
- Bogui M. J.-J. (2010). La cybercriminalité, menace pour le développement : Les escroqueries Internet en Côte d'Ivoire. *Afrique contemporaine*, 234, 155-170. https://doi.org/10.3917/afco.234.0155, consulté le 26 décembre 2021.
- Bogui M. J.-J. & Atchoua N. J. (2016). La régulation des usages des TIC en Côte d’Ivoire : entre identification et craintes de profilage des populations, tic&société [en ligne], Vol. 10, N° 1 | 1er semestre 2016, Online since 30 May 2019, connection on 26 December 2021. URL : http://journals.openedition.org/ticetsociete/1983 ; DOI : sur URL : https://doi.org/10.4000/ticetsociete.1983, consulté le 24 décembre 2021.
- Boukarnaoui H. & Attouche H. (2021) « L'image de marque nationale «nation branding» : une piste pour améliorer la réputation des pays», *Revue Internationale du Chercheur* «Volume 2: Numéro 3» pp: 1598 -1616.
- De Rosnay J. (1995) ; L’homme symbiotique. Regards sur le troisième millénaire, Seuil, Paris.
- Douzet F. (2016). Le cyberespace, un enjeu majeur de géopolitique, in *La revue des médias*, sur URL *: https://larevuedesmedias.ina.fr/le-cyberespace-un-enjeu-majeur-de-geopolitique,* consulté le 24 décembre 2021.

- Ghernaouti-H. S. & Dufour A. (2012). Cybercriminalité et cybersécurité. Dans : Solange Ghernaouti-Hélie (D) éd., *Internet* (pp. 94-108). Paris cedex 14: Presses Universitaires de France.
- Interpol (2021), Evaluation 2021 des cybermenaces en Afrique, principales observations d'Interpol sur la cybercriminalité en Afrique.
- Koné Yaya, « Le travail mondialisé du jour et le travaillement local la nuit », *Journal des anthropologues* [En ligne], 142-143 | 2015, mis en ligne le 15 octobre 2017, consulté le 19 avril 2022. URL : http:// journals.openedition.org/jda/6327 ; DOI : 10.4000/jda.6327 ;
- Kossaï M. (2013). Les Technologies de L'Information et des Communications (TIC), le capital humain, les changements organisationnels et la performance des PME manufacturières. Economies et finances, Thèse de Doctorat, Université Paris Dauphine Paris IX, 2013. Français. ffNNT : 2013PA090035ff. fftel-01124114f
- Koua A.M., Traore B.S., Konan K.P., Ahounon I., Djo F.D.B., Aka R.A., Kouadio R.A. & Yeo-T. Y.J.M. (2015). Cinq vignettes cliniques sur la cybercriminalité juvénile en Côte d'Ivoire : profil psychopathologique. *L'Information psychiatrique* ; 91 : 847-52 doi:10.1684/ipe.2015.1419.
- Martin D. & Martin F.-P. (2001). Cybercrime : menace, vulnérabilités et repostes, Presses universitaires de France, coll, criminalité internationale, Paris.
- Mucchielli R. (1984). L'analyse de contenu de documents et communications, 5e Edition ESF.
- N'Guessan A. (2014), La pratique de la cybercriminalité en milieux scolaire et universitaire de Côte d'Ivoire. Cas des élèves et étudiants du district d'Abidjan. *European Scientific Journal, ESJ*, *10*(31). https://doi.org/10.19044/esj.2014.v10n31p%p, consulté le 26 décembre 2021.
- Ndoye B. (2016). La révolution du numérique : enjeux culturels et épistémiques, pp. 7-18, in *CODESRIA*, *Les sciences sociales au Sénégal* : Mise à l'épreuve et nouvelles perspectives.
- ONU. (2000). Dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, Vienne.

- Pereira B. (2016). La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité. *Revue internationale de droit économique*, XXX, 387-409, sur URLhttps://doi.org/10.3917/ride.303.0387, consulté le 26 décembre 2021.
- Pistoletti P. (2014). Révolution numérique : genèse et enjeux, in revue *Sources.*
- Plantard P., Le Boucher C. & Perret D. (2020). Les enseignants et le numérique : modèles pédagogiques vs modèles d'appropriation des technologies numériques ? in *Bulletin de Veille n°1*.
- Sahi E. (2021). Cybercriminalité : les victimes perdent 6 milliards de FCFA en 2021**,** in *Afrique-sur7.ci* sur **https://www.afrique-sur7.ci/483677-cybercriminalite-cote-divoire-en-2021**
- Tano-B. A. J.-A. (2015). La répression de la cybercriminalité dans les Etats de l'Union européenne et de l'Afrique de l'Ouest. Droit. Thèse de Doctorat, Université Sorbonne Paris Cité, Français. ffNNT : 2015USPCB067ff. fftel-01249586f