Les Cahiers du CEDIMES
2024, Volume 19, Hors-série n° 2024, https://doi.org/10.69611/cahiers19-HS-27
ISSN 2110-6045

La politique de lutte contre la cybercriminalité au Cameroun : entre formalisme déclaratif et opérationnalisation poussive (2010-2020)

Georges ETOA OYONO

Université d'Ebolowa, Cameroun, georgesetoa@gmail.com

Résumé : L'évolution des Technologies de l'Information et de la Communication est un des enjeux majeurs des États en Afrique subsaharienne. En dépit de ses avantages, cette entreprise est l'objet de nombreuses déconvenues pour les économies. Qu'il s'agisse du cadre privé ou public, le phénomène des cybercrimes est préoccupant car il prend de l'ampleur et les conséquences négatives sont de plus en plus considérables et coûteuses. Le Cameroun n'a pas échappé à cette pratique néfaste. En attestent les multiples initiatives prises par le gouvernement depuis l'année 2010 pour venir à bout de cette délinquance informatique. Dans un contexte où les systèmes répressifs de la plupart des États africains se sont révélés inappropriés pour saisir ce nouveau phénomène criminel, l'objectif de cette contribution est d'évaluer les effets des mesures de lutte prises par le gouvernement camerounais pour barrer la voie à la cybercriminalité. Dans une démarche empirico-inductive, alliant l'exploitation documentaire et les entretiens, on est parvenu aux conclusions selon lesquelles, les mesures de lutte contre la cybercriminalité sont salutaires au Cameroun. Toutefois, en dehors des actions répressives contenues dans les dispositions juridiques en vigueur, le gouvernement doit intensifier, de toute urgence les efforts en question. Bien plus, un accent est à mettre sur la capacité d´application de la loi et de la justice pénale, l´éducation et la sensibilisation des populations et la coopération entre le gouvernement et les autres acteurs.

Mots clés : cybercriminalité ; cybercrimes ; opérationnalisation ; formalisme ; efficacité.

Abstract: The development of Information and Communication Technologies is one of the major challenges facing governments in sub-Saharan Africa. Despite its advantages, this enterprise is the cause of many economic setbacks. Whether in the private or public sector, the phenomenon of cybercrime is a cause for concern, as it is on the increase and the negative consequences are increasingly considerable and costly. Cameroon has not escaped this harmful practice. This is borne out by the many initiatives taken by the government since 2010 to put an end to computer crime. In a context where the repressive systems of most African states have proved inadequate to deal with this new criminal phenomenon, the aim of this contribution is to assess the effects of the measures taken by the Cameroonian government to combat cybercrime to date. Using an empirico-inductive approach, combining documentary research and interviews, we came to the conclusion that measures to combat cybercrime are beneficial in Cameroon. However, apart from the repressive measures contained in the legal provisions in force, the government urgently needs to step up the efforts in question. In addition, emphasis must be placed on law enforcement and criminal justice capacity, public education and awareness-raising, and cooperation between the government and other stakeholders.

Key words: cybercrime; operationalization; formalism; effectiveness.

1. Introduction

Le développement contemporain des Technologies de l'Information et de la Communication (TIC) constitue un enjeu majeur pour le développement économique. Cependant, il a été à l'origine de l'apparition du phénomène de la cybercriminalité dont les caractéristiques particulières ont entraîné l'inadaptation des systèmes répressifs de la plupart des États (Abella et Baziz, 2018). Depuis les années 2000 dans presque tous les pays d'Afrique subsaharienne, des lois régissent la cyber-sécurité et la cybercriminalité, ainsi que les communications électroniques.

La propagation de fausses nouvelles par voie électroniques et l'apologie de terrorisme, par tout canal visant à atteindre le plus grand public, sont sanctionnées au Cameroun de peine d'emprisonnement allant de 15 à 20 ans par la loi de 2014 portant répressions des actes de terrorisme (Loi N° 2014/028, 2014). Pourtant, le pays a bien du mal à dissuader les lanceurs de fausses nouvelles, et, bien pire, les actes de cybercriminalités prennent des proportions inattendues, passant de la piraterie de site via l'utilisation de logiciels espions, aux opérations multiformes de détournement et/ou de pillages économiques divers. La cybercriminalité est clairement devenue la nouvelle menace du XXI^{e} siècle. Face à ce danger de plus en plus grandissant, les gouvernements et Organismes se déploient par tous les moyens pour venir à bout de la menace. Des rencontres internationales et concertations diverses ont été organisées pour étudier les voies et moyens de lutte contre la cybercriminalité. L'objectif de cette contribution est d'évaluer les effets des mesures et moyens mis en place par le gouvernement camerounais pour réduire ou barrer la voie à la cybercriminalité de 2010 jusqu'à nos jours. Par cette réflexion, on se propose d'évaluer les multiples mesures de lutte formulées par le gouvernement camerounais. Depuis 2010, qu'est-ce que le gouvernement camerounais a pris comme résolutions pour barrer la voie à cette pratique en son territoire depuis sa survenue ? Peut-on dire que l'architecture sécuritaire de lutte contre la cybercriminalité du gouvernement camerounais a été efficace ? En dépit de la menace grandissante et des effets néfastes enregistrés ici et là, le gouvernement a engagé des initiatives théoriques et pratiques pour venir à bout de la cybercriminalité au Cameroun, malgré des résultats encore peu probants compte tenu de l'ampleur de la pratique. Pour traiter cette question, il a été important de convoquer le fonctionnalisme pour mieux cerner les différents maillons qui interviennent dans cette lutte contre la cybercriminalité. Ainsi, l'analyse consiste en la présentation de différentes mesures formelles déclaratives du Gouvernement camerounais (2) de l'impact desdites mesures dans la lutte contre la cybercriminalité au Cameroun (3). Dans l'analyse qui tente d'apporter des éléments de réponses à cette préoccupation, l'on ne manque pas de relever quelques aspects de ladite criminalité en terre camerounaise.

2. La cybercriminalité et analyse des différentes mesures formelles déclaratives du Gouvernement camerounais.

Depuis qu'elle a fait son apparition, dans les années 1980, la cybercriminalité est considérée comme un danger phare[1] pour les économies des États. Malgré la perception variée en fonction des États, cette pratique fait l'objet de mesures appropriées par de nombreux États, le Cameroun en particulier. Cette section se propose de faire une clarification dudit concept (2.1.) et par la suite d'examiner les différentes mesures formelles déclaratives déployées par le Gouvernement camerounais (2.2.).

[1] La pratique a fait de nombreux dégâts et pertes importantes auprès des civils et organismes sur le plan économique.

2.1. La cybercriminalité : un concept polysémique aux origines récentes

Le terme même de cybercriminalité ne se prête pas à une définition simple et est considéré comme une série d´actes ou de comportements plutôt que comme un acte unique. Vu le caractère multiforme de la pratique, nous sommes d'avis qu'il n'existe pas de définition universelle de la cybercriminalité qui soit consacrée, si bien que chaque Etat l'a défini selon ses propres critères.

Compte tenu de cela, on propose une perception plurielle de certains chercheurs et organismes. Ainsi, David Wall déclare que « *le terme cybercriminalité ne signifie plus qu'un acte illicite qui est d'une façon ou d'une autre relatif à l'ordinateur »* (Wall, 2001).

Le Professeur André Lucas considère la cybercriminalité comme *« la seule démarche acceptable qui consiste à réserver l'acception de fraude informatique aux hypothèses dans lesquelles la technique informatique est au cœur de l'agissement incriminable » tout en sachant fort bien qu'il est parfois difficile d'isoler le « noyau dur » de la « périphérie »* (Lucas, 1987).

Selon l'O.N.U. la Cybercriminalité doit recouvrir *« tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent »* et, dans une acception plus large, *« tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique »* (Abella et Baziz, 2018).

Dans l'usage courant, la cybercriminalité sert à désigner toutes les formes d'attaques réalisées au moyen de réseaux informatiques ou de systèmes d'information, où les ayant pour cible. En d'autres termes la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet (Abella et Baziz, 2018).

La définition Camerounaise que propose l'ANTIC de la cybercriminalité s'inspire de la Loi N°2010/012 du 21 décembre 2010 relative à la cyber sécurité et à la cybercriminalité au Cameroun. Cette définition est beaucoup plus pratique. Elle fait de la cybercriminalité une activité qui consiste à utiliser les systèmes et réseaux informatiques en général et l'Internet en particulier pour poser des actes criminels ou proscrits par la loi.

La cybercriminalité peut alors se définir comme toute action illégale dont l'objet est de perpétrer des infractions pénales sur ou au moyen d'un système informatique interconnecté à un réseau de télécommunication. Elle vise soit des infractions spécifiques à Internet, pour lesquelles les technologies de l'information et de la communication sont l'objet même du délit, soit des infractions de droit commun pour lesquelles Internet est le moyen de développer des infractions préexistantes (Quemener et Ferry, 2009).

Pour ce qui est de l'origine exacte de la cybercriminalité, à savoir la toute première date à laquelle un individu a commis un méfait sur un réseau informatique, il est très difficile voire impossible de l'identifier. Ce qu'il est possible de connaître, c'est le moment où la première attaque majeure sur un réseau informatique a eu lieu, puis de partir de ce point de référence pour voir l'évolution de la cybercriminalité. Les éléments de réponses à cette évolution sont perceptibles dans les travaux de master en Science de Gestion de Abella Aini et Baziz Samira (2018). Pour ces chercheurs, la cybercriminalité s'est développée entre 1980 et 1988. La première date se réfère à la création d'internet qui fait suite à la séparation d'Arpanet entre un réseau militaire et un réseau civil. La seconde date renvoie au premier outil de piratage connu et complètement automatisé. Elle correspond au premier incident informatique de type « *Malware* » occasionné par un ver Internet qui a infecté en quelques jours plus de 6000 serveurs Unix sur un parc d'environ de 60 000 reliés au réseau Internet de l'époque, soit un taux d'infection de 10% (Abella et Baziz, 2018). Plus communément appelé « *ver Morris* » ou « *ver de Morris* » du nom de son concepteur, ce vers informatique est le premier d'une longue série, à l'origine d'une nouvelle course en avant, celle du piratage informatique. Les recherches sur la cybercriminalité vont dans le même sens et confirment que la pratique criminelle s'est développée dans les années 1980.

Devenu un véritable fléau dès la fin du XXe siècle, le piratage informatique n'est plus un mythe, ou une chimère à laquelle certains ne voulaient ou ne semblaient pas croire. Aucun continent n'en est épargné. Pour faire face à cette sorte de nébuleuse, le gouvernement camerounais a pris certaines mesures formelles que nous examinons dans la partie qui suit.

2.2. Les différentes mesures formelles déployées par le gouvernement camerounais

La vitesse à laquelle les nouvelles technologies de l'information et des communications se développent a pour conséquence qu'il devient très difficile de discerner les directions qu'elles emprunteront dans les années, voire les mois à venir (Fortin et Gagnon, 2013). Ainsi, devenu un véritable fléau dès la fin du XXe siècle, le piratage informatique ou cybercriminalité n'est plus un mythe, ou une chimère à laquelle certains ne voulaient ou ne semblaient pas croire, comme certains organismes ou grandes entreprises. Les pirates informatiques n'en finissent plus de faire parler d'eux. D'après L'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC), la quantification des effets de la cybercriminalité au Cameroun est devenue de nos jours un exercice difficile à réaliser et ce, par rapport aux nombres inestimables d'infractions et de pertes qu'elle entraine. Il est néanmoins avéré que cette pratique fait des dégâts importants. C'est pour tenter d'enrayer le phénomène que le gouvernement Camerounais a pris diverses mesures depuis 2010. Parmi celles-ci on a les mesures juridiques ou coercitives et les mesures préventives.

Pour ce qui est des premières mesures qui tournent autour de multiples dispositions juridiques, on a la promulgation de la loi N°2010/012 du 21 décembre 2010 relative à la cyber sécurité et à la cybercriminalité au Cameroun, qui est la première initiative forte pour barrer la voie à la pratique. Restant sur le même plan, il y a aussi la loi N°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun, modifiée et complétée par la loi N°2015/006 du 20 avril 2015 qui stipule respectivement en ses articles 55 (1) et 69 (6) que :

- Les opérateurs et exploitants des réseaux de communications électroniques ouverts au public ainsi que les fournisseurs de services sont tenus, au moment de toute souscription, de procéder à l'identification des abonnés et des terminaux. Ils tiennent à jour des listes d'abonnés ;
- Sont passibles d'une pénalité de 200 000 000 (deux cent millions) à 500 000 000 (cinq cent millions) de francs, les opérateurs de réseaux de communications électroniques et exploitants de services de communications électroniques qui violent les dispositions de l'article 55 relatives à l'identification des abonnés (Loi N° 2010/013, 2010).

Par ailleurs, le décret N°2015/3759 du 03 septembre 2015 fixe les modalités d'identification des abonnés et des équipements terminaux de communications électroniques. Cette campagne d'identification des abonnés des réseaux téléphoniques commencée en 2016 précise, entre autres, le nombre de puces par opérateur pour les personnes physiques et morales et interdit la commercialisation des cartes SIM pré-activées dans les rues.

Outre ces multiples dispositions juridiques prises par le gouvernement camerounais, il y a également les nombreux textes d'application de la loi N°2010/012 du 21 décembre 2010 relative à la cyber sécurité et à la cybercriminalité au Cameroun (Entretien, 2022).

Dans ces mesures formelles prises par le gouvernement camerounais pour venir à bout de la cybercriminalité, nous avons aussi les mesures préventives. Parmi celles-ci, nous pouvons également citer la stratégie de développement de l'économie numérique du Cameroun qui prévoit tout un axe sur le renforcement de la confiance numérique ainsi que la politique nationale de sécurité des réseaux et des systèmes d'information qui a été élaboré en 2017(Entretien, 2022).

Il importe de relever que la mise en pratique d'un esprit de collaboration est nécessaire entre divers Organes nationaux pour implémenter ces multiples mesures formulées par le gouvernement camerounais, et par ricochet, asseoir un climat de lutte efficace contre la cybercriminalité. En outre, il convient de relever qu'une stratégie efficace pour lutter contre la cybercriminalité et les activités malveillantes dans le cyberespace nécessite une approche multipartite où les rôles et les

responsabilités des organismes et institutions gouvernementaux et les autres partenaires potentiels doivent être définis au plus haut niveau. Ainsi, bien que l'ANTIC soit reconnu comme le principal acteur de lutte contre la cybercriminalité[1], plusieurs autres acteurs participent sous l'impulsion du gouvernement et de manière spécifique dans la lutte contre la cybercriminalité au Cameroun. Chacune de ces structures gouvernementales détient une base de données qui lui permet de suivre les opérations des cybers opérateurs et cybers crimes en particulier, d'analyser les données par la suite. Il s'agit par exemple :

- Du Ministère des Postes et Télécommunications du Cameroun, (MINPOSTEL) qui élabore et met en œuvre la politique de sécurité des communications électroniques et des systèmes d'information en tenant compte de l'évolution technologique et des priorités du Gouvernement dans le domaine ;
- De L'Agence de Régulation des Télécommunications (ART) qui collabore avec l'ANTIC dans la mise en œuvre de ses missions ;
- Des services de sécurité (SED, DGSN, DGRE, INTERPOL) qui mènent des investigations numériques, éventuellement en collaboration avec l'ANTIC ;
- Du MINJUSTICE qui, à travers ses tribunaux, jugent les infractions liées aux crimes cybernétiques et prononcent des sanctions à l'encontre des contrevenants (Entretien, 2022).

C'est dans ce sens que, convoquant le fonctionnalisme, on ambitionne de bien cerner le rôle dévolu à chacun de ces organes appelé à intervenir dans la lutte contre cette pratique dont les dégâts ne sont plus un doute. En effet, il s'agit de montrer que bien que louant les initiatives de création ou de mise sur pieds d'organismes pour mieux lutter contre la cybercriminalité, il est nécessaire de créer un organisme supranational pour coordonner les actions des institutions existantes et déjà en œuvre pour mieux résoudre le problème de cybercriminalité.

On n'a pas la prétention de remettre en cause les initiatives existantes, mais il est question de suggérer une approche de rendement desdites structures. En effet, il serait louable d'organiser la lutte contre la cybercriminalité au Cameroun dans un esprit de collaboration en mettant sur pied un organisme aux pouvoirs plus spécifiques que ceux de L'ANTIC. Jusqu'à nos jours, en dépit du rôle central peu connu ou dont les résultats sont peu perceptibles, cet organisme occupe pourtant une place particulière dans cette lutte au Cameroun, eut égard aux multiples missions dévolues à cette Institution.

Dans le décret N° 2019/150 du 22 mars 2019, en son article 5, les missions de l'ANTIC sont clairement présentées et tournent autour de la veille technologique et de l'émission des alertes et recommandations en matière de sécurité des réseaux de communications électroniques et de certification. Afin d'assurer cette fonction à elle assignée, l'ANTIC a mis en place un *Computer Incident Response Team* (CIRT). Ce dernier a une mission préventive et réactive. À titre préventif, le CIRT est chargé :

- D'analyser, de suivre et de réaliser la cartographie des niveaux de risques afférents à la sécurité des infrastructures critiques du cyberespace national ;
- De concevoir et de produire les bulletins et les alertes de sécurité sur les vulnérabilités et les actions palliatives des attaques cybercriminelles ;
- D'administrer, de développer et maintenir les outils collaboratifs du CIRT (plateforme collaborative, portail web, etc…) ;
- De sensibiliser toutes les couches sociales sur la cybercriminalité à travers les différents canaux de communication ;
- De réaliser la veille informationnelle pour le compte de l'État ;
- De collecter et de suivre les statistiques afférentes à la cybercriminalité ;
- D'élaborer les référentiels et les politiques de sécurité ;

[1]L'ANTIC a été créé par décret n°2002/092 du 08 avril 2002 par le Chef de l'Etat, Son Excellence Monsieur Paul Biya. Cette structure est chargée de la régulation, du contrôle et du suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques.

- D'exploiter et d'administrer le Centre d'Appel ou « Call Center » (Site officiel ANTIC).

À titre réactif, le CIRT se doit :

- De traiter les incidents survenus dans le cyberespace national ;
- De collecter et d'analyser les preuves numériques lors des investigations ;
- D'assurer la formation du Personnel des Administrations publiques sur la pratique ;
- De déployer les dispositifs de sécurité dans les infrastructures critiques ;
- De réaliser les scans de vulnérabilité périodiques des sites web et des systèmes d'information des Administrations publiques et des Établissements privés sensibles (Départements Ministériels, Établissements Publics, Banques) ;
- D'organiser les « cyberdrills » (Site officiel ANTIC).

Par ailleurs, la loi relative à la cyber sécurité et à la cybercriminalité prévoit certaines dispositions techniques qui en grande partie sont de la compétence de l'ANTIC. Ainsi, ce texte institue à l'ANTIC d'assurer, pour le compte de l'État, la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques ainsi qu'une redevance à laquelle sont assujettis les autorités de certification accréditées, les auditeurs de sécurité, les éditeurs de logiciels de sécurité et les autres prestataires de sécurité agréés[1].

Dans l'ensemble, en l'état théorique et formel des mesures prise pour faire faire face à la cybercriminalité, on peut dire que le gouvernement camerounais dispose d'un chapelet très intéressant de réponses techniques au phénomène.

Toutefois, en raison du caractère transfrontalier et international de la cybercriminalité, les législations nationales ne peuvent pas être rédigées de manière isolée et les gouvernements doivent chercher à harmoniser les législations nationales, les règlements, les normes et lignes directrices sur les questions de cyber sécurité afin de contribuer à la création de cadres régionaux et internationaux efficaces pour lutter contre la cybercriminalité[2].

En dépit de ces multiples mesures formelles prises par le gouvernement camerounais depuis 2010, l'on est en droit de questionner leur efficacité dans la lutte contre la cybercriminalité onze ans après. Quelle lecture peut-on faire de l'opérationnalisation et l'efficacité desdites mesures dans la lutte contre cette pratique en terre camerounaise ?

3. L'opérationnalisation desdites mesures dans la lutte contre la cybercriminalité au Cameroun

L'opérationnalisation des mesures suppose ici l'implémentation ou la mise en pratique des multiples dispositions prises par le gouvernement camerounais. Cette seconde partie examine l'aspect pratique de la lutte contre la cybercriminalité au Cameroun. Il s'agit de relever quelques actions concrètes de cette lutte (3.1.) et, par ricochet, montrer les limites relatives à cette opérationnalisation (3.2.).

[1]Cf Article 5 du décret N° 2019/150 du 22 mars 2019 portant organisation et fonctionnement de l'ANTIC. En dehors de cette mission, il s'y ajoute, toujours dans ce décret, certaines obligations spécifiques : - aux opérateurs de réseaux et aux fournisseurs de services de communications électroniques, fournisseurs d'accès, de services et des contenus d'installer des mécanismes de surveillance de trafic des donnés de leur réseau et de conserver les données de connexion de trafic pendant une période de dix (10) ans ; - aux fournisseurs de contenus des réseaux de communication électroniques et systèmes d'information de mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs ; - aux réseaux de communications électroniques et systèmes d'information de se soumettre de manière obligatoire et périodique à un audit de leurs systèmes de sécurité par l'organe de régulation ; - Enfin, aux opérateurs du secteur de la communication de fournir aux utilisateurs un certain nombre d'informations relatives à la sécurité.

[2] L'Union africaine, « Une approche globale sur la cyber sécurité et la cybercriminalité en Afrique » en page 9, in: https://au.int/sites/default/files/newsevents/workingdocuments/31357-wddoc_on_cybersecurity_extra_ord_session_stc_cict_bamako_sept_2016_fr.pdf, consulté en ligne le 02 mai 2023.

3.1. Un aperçu de quelques actions de pratiques de cybercriminalité et les actions concrètes de lutte.

Les actes de cybercriminalités ne sont plus tabous sur le sol camerounais (3.1.1), pour y remédier, le gouvernement camerounais s'est montré actif à travers certaines actions (3.1.2.)

3.1.1. Un aperçu de quelques actions de pratiques de cybercriminalité

Au cours de la dernière décennie, le continent africain a connu une évolution dans l'acquisition, l'adaptation et la mise en place des infrastructures nécessaires aux nouvelles technologies de l'information et de la communication (TIC). Ceci s'est manifesté rapidement, passant d'un débit moyen à un accès croissant et largement répandu d'internet à haut débits. De moins de 5% en 2007, la pénétration d'internet a atteint 28% en 2015 (Union Africaine, 2016). Il est clair que l'internet, les réseaux mobiles, les informations connexes et les technologies de communication (TIC) sont devenues des outils indispensables pour les gouvernements, les entreprises, la société civile et les individus à travers le monde. S'il est vrai que ces technologies ont favorisé un développement économique considérable, ont augmenté la libre circulation des informations et ont contribué à des gains réels sur le plan du rendement, de l'efficacité, de la productivité et la créativité à travers l'Afrique, ils sont la proie d'une catégorie d'usagers mal intentionnés et parfois criminels. L'usage de plus en plus récurrent de l'exploitation réseaux consiste à pratiquer des actes criminels : escroquerie, vol, piraterie, accès illégal aux comptes d'autrui, vol d'informations, etc. Le Cameroun n'est pas en reste au nombre des pays victimes.

Un des modes dont se servent les cybers crimes de plus en plus au Cameroun est l'escroquerie sur les réseaux. Des informations reçus de cette recherche, il apparaît que deux stratagèmes ont été plusieurs fois utilisés. Tout d'abord, il est arrivé que, pratiquement au même moment, plusieurs abonnés à la téléphonie mobile reçoivent sur leur téléphone portable des messages leur annonçant explicitement ou leur faisant croire qu'ils avaient gagné tantôt de l'argent, tantôt un crédit de communication, tantôt un voyage en Europe avec leur famille, et les invitant, pour les formalités y afférentes, à appeler à un numéro de téléphone qui était clairement indiqué. À chaque fois, au bout du fil, le répondant confirmait le gain et entretenait de très longues conversations téléphoniques avec les victimes, qui devaient plus tard se rendre compte que l'annonce était mensongère (Entretien, 2022).

Ensuite, le second stratagème consiste à appeler un abonné très tard la nuit, pour lui annoncer qu'un des siens qu'on nomme très clairement est victime d'un accident de la circulation et se trouve aux services d'urgence (parfois qu'il en est mort) et de demander un transfert immédiat de crédit de communication pour permettre à l'informateur de donner plus de détails sur l'accident (Entretien, 2022).

Le mode opératoire desdits criminels consiste généralement à se servir des bases de données informatiques. Il peut s'agir de celles des opérateurs de téléphonies qu'ils pénètrent par effraction ou en interférant toute autre base de données d'un service public ou privé. Une fois les informations en leur possession, ils peuvent opérer en toute aisance.

Les fonctionnaires avides de nomination sont aussi assez régulièrement escroqués par des appelants qui leur signalent que leur dossier de nomination à tel poste est en bonne voie, mais qu'il faudrait fournir un pot-de-vin pour un heureux aboutissement (Entretien, 2022). Dans ce cas, la quête des informations se fait généralement par curiosité en ayant effectué un passage dans une des Institutions compétentes, ou par une fuite quelconque de l'information parfois due à un manque de professionnalisme des agents en service dans l'organisme traitant d'un éventuel dossier en question. Parfois aussi, la fuite d'informations peut être issue des causeries entre agents dans un cadre inapproprié (restaurant, débit de boisson, lieu public, etc..).

Sur un tout autre plan, les actes de cybercriminalités peuvent être visibles dans les cas d'escroquerie réseaux, chantage et publication d'images intimes et/ou privées. Les comptes des

personnalités membres du gouvernement connaissent le plus grand nombre de piratage des cybers crimes, où des actions d'extorsion de fonds et fausses promesses et arnaques sont opérées.

Entre 2015 et 2017, l'Agence nationale des technologies de l'information et la communication (ANTIC) a recensé plus de 300 cas d'attaques cybernétiques. Cela concerne les piratages informatiques de sites gouvernementaux (*Web defacement*, infection par des programmes malveillants, saturation de serveurs, attaques de type force brute), le *scamming*, la fraude à la carte bancaire et à la Simbox. Nul n'échappe aux hackers. En 2015, le site de la présidence de la République a connu un piratage informatique. Plus tard, en date du 24 juin 2020, c'était au tour du site d'Elections Cameroon de subir des telles malveillances ; des hackers ont pris possession de la plateforme. Au niveau de l'accueil, c'est une photo de l'opposant Maurice Kamto qu'on y retrouve, le poing serré comme pour crier victoire. L'image est accompagnée du message : « *La vérité doit toujours prévaloir. C'est juste une question de temps »* (Bihina, 2020).

Par ailleurs, les Banques camerounaises sont fréquemment victimes de ces informaticiens d'un autre genre et préfèrent ne point faire de bruits sur cette réalité. Des attaques perpétrées contre la Société camerounaise des banques et le crédit communautaire d'Afrique, entre 2016 et 2019, a généré des pertes de plus de 924 millions de Francs Cfa. La publication des résultats des enquêtes menées pourrait faire grimper le bilan (Bihina, 2020).

Les informations tirées du site Internet de l'ANTIC font état de plusieurs autres exemples tout aussi parlants concernant les administrations camerounaises qui ont accusé plus de 14 milliards de FCFA de manque à gagner en 2014 du fait de la cybercriminalité. En 2012, la compagnie aérienne nationale Camair-Co a perdu 2 millions FCFA en vente de billets ; Ecobank s'est fait hacker 43 comptes en 24 heures avec 3 milliards de Francs Cfa, l'opérateur Mobile Télécommunications Networks (MTN) a perdu un 1,8 milliard d'envoi de crédits. Toujours selon l'ANTIC, les fraudes à la carte bancaire ont induit des pertes de plus 3,7 milliards de FCFA ; des sommes tout autant élevées, mais non précisées, ont été enregistrées à la suite de fraude à la Simbox. S'agissant des arnaques sur Internet, l'Agence estime à 4 milliards de FCFA les pertes induites (Bihina, 2020).

D'autres statistiques importantes, livrées par la Ministre des Postes et Télécommunications, viennent confirmer l'ampleur du phénomène de cybercriminalité dans notre pays. Ainsi, il appert à titre d'exemple que, pour l'année 2018, 3 388 cas d'usurpation d'identités ont été constatés. En 2019, 2050 plaintes relatives au scamming et au phishing dont environ 5 milliards FCFA de perte financière, ainsi que près de 6 milliards de pertes relatives aux fraudes bancaires, et 11 617 vulnérabilités ont été détectés sur les sites web des administrations publiques (Minpostel, 2023).

Face à ces actes criminels, le gouvernement camerounais n'est pas resté amorphe. Nos investigations ont permis de découvrir quelques actions d'éclats de cette lutte contre la cybercriminalité.

3.1.2. Les actions concrètes de lutte

Face à la recrudescence des actes de cybercriminalités, l'Union africaine n'est pas restée amorphe. L'Organisation supra africaine a cherché à encourager une approche continentale pour lutter contre la cybercriminalité par le biais de la Convention sur la cybersécurité et la protection des données à caractère personnel dite Convention de Malabo (Institute for Security Studies, 2019). L'UA soutient que « la législation nationale ne peut être rédigée de manière isolée et les gouvernements nationaux doivent chercher à harmoniser les législations, les réglementations, les normes et les directives nationales sur les questions de cybersécurité » (Union Africaine, 2016). Cette recommandation suivie par le gouvernement camerounais a porté des fruits, suite aux mesures fortes prises dans un esprit de collaboration entre différents organismes impliqué dans cette lutte. Dans cette croisade contre la cybercriminalité, le gouvernement par l'intermédiaire du ministre des Postes et Télécommunications, Minette Libom Li Likeng, rappelle dans une interview la campagne d'envergure nationale que le pays mène pour la promotion de la culture de la cyber-sécurité et la

sensibilisation à l'usage responsable des réseaux sociaux (Eco Matin, 2020). La sensibilisation et la répression, souligne-t-elle, sont au cœur des stratégies nationales mises en œuvre pour lutter contre la cybercriminalité.

La propension de la cybercriminalité à l'intérieur des frontières nationales a ainsi contraint le gouvernement à former une unité de la police judiciaire spécialisée dans le domaine. À Yaoundé, cette brigade est logée au sein de la direction régionale de la police judiciaire. Ses actions ont permis de tracer la piste de quelques 600 cybercriminels entre Douala, Bamenda, Buea, Kumba, et Yaoundé (Entretien, 2022).

Pour faire face à l'impératif de la cybersécurité, le gouvernement camerounais a développé un certain nombre d'applications visant à automatiser les procédures dans le cadre de la politique de mise en place de la gouvernance électronique. Il s'agit notamment de Sigipes, Sydonia, Depmi, E-Guce, etc. Ces applications n'échappent cependant pas aux menaces cybernétiques au vu des défaillances encore observées dans l'implémentation de systèmes de protection (Entretien, 2022).

En dehors de l'usage des TIC à des fins de menace, de propagande, des attaques ciblées contre des hautes personnalités de la République et les fausses nouvelles, c'est beaucoup plus dans l'escroquerie par réseaux et dans les cas d'usurpation d'identité des personnalités, devenus de plus en plus légion, que les actions de lutte des personnels formés ont été salutaires.

Ainsi, en juin 2020, trois personnes qui utilisaient l'identité de Samuel Eto'o Fils, l'ancien sociétaire du FC Barcelone pour commettre des dégâts sur Internet avaient été arrêtées à Foumban, dans la région de l'Ouest. Le scénario de l'arnaque utilisé par les quatre suspects reprenait un *modus operandi* déjà utilisé par d'autres escrocs sur le web.

Dans la capitale économique camerounaise, nous rapporte le quotidien à capitaux publics *Cameroon tribune*, en date du 24 février 2021, quatre individus interpelés par les éléments des forces de l'ordre, sont accusés d'avoir usurpé l'identité de l'ancien international camerounais, Samuel Eto'o pour procéder à l'escroquerie dans les réseaux sociaux. Même si les montants volés n'ont pas été dévoilés à la presse, la Division régionale de la Police judiciaire (DRPJ) du Littoral, informe dans les colonnes de *Cameroon Tribune* que le quatuor aurait soustrait de l'argent à plusieurs victimes (Mbala, 2021).

Depuis plusieurs années se multiplient ainsi les tentatives d'arnaque sur la toile. De supposées jeunes femmes ou jeunes hommes, signale *Cameroon Tribune,* se font passer pour certaines personnalités et tentent de séduire les internautes pour leur extorquer de l'argent. Ces malfrats ont, après information, collaboration et exploitation des données, ont été mis aux arrêts par les forces de polices de la capitale économique.

Le cas le plus récent de la prouesse des éléments de la DGSN dans la lutte contre la cybercriminalité remonte à la date du 11 mai 2021. En effet, le nommé Eyafa Jacques Calvin, détenu à la prison centrale de Kondengui, s'est longtemps déployé dans le mode d'usurpation d'identité. Ce détenu s'est illustré au mois de mai 2021, en se faisant passer pour Samuel Mvondo Ayolo, directeur du cabinet civil de la présidence de la République du Cameroun. Des informations livrées par l'officier de police judiciaire, Vincent de Paul Meva, après exploitation de son répertoire téléphonique, il ressort que sieur Eyafa Jacques Calvin, qui n'en est pas à son premier forfait, a tenté d'escroquer le président du Niger en se faisant passer pour Samuel Mvondo Ayolo. L'exploitation de son téléphone a permis de découvrir qu'il a fait plusieurs victimes dans les chancelleries, les Organisations non gouvernementales, celles rattachées au Système des Nations-Unies et la Banque mondiale. Des hommes d'affaires se comptent également parmi ses victimes (Etoundi, 2021). Au moment de son arrestation, le présumé attendait un virement de 300 000 euros soit 195 millions de Fcfa d'une Ong américaines (Etoundi, 2021).

Outre les actions d'éclats accomplis par les services de la DGSN et de la Gendarmerie nationale, l'Agence nationale des technologies de l'information et de la communication (ANTIC), signale la poursuite de multiples enquêtes pour mettre hors d'état de nuire les cybercriminels, dans un contexte où l'usurpation d'identité des personnalités est l'une des arnaques les plus récurrentes au Cameroun. Pour plus d'efficacité de cette action eu égard à la non maitrise des méandres de

l'informatique, le gouvernement a été contraint de procéder à la formation des agents de la police, de la gendarmerie, des Magistrats et autres agents publics. Ceci a permis d'obtenir des résultats satisfaisants, souligne cet OPJ (Entretien, 2022).

Au plus fort de la crise dans les régions du Nord-Ouest et du Sud-Ouest, le Gouvernement camerounais a pratiqué la plus longue censure d'internet jamais enregistrée dans le monde en privant ces deux régions de connectivité pendant trois mois, entre janvier et avril 2017. Cette suppression provisoire de 94 jours a permis au gouvernement de freiner les activités de déstabilisation de certains membres de ces corporations d'activistes extrémistes, mus par des velléités sécessionnistes qui en ont profité pour diffuser des messages de haine et inciter à la perpétration d'actes de violence et à des exactions de toutes sortes (Eco Matin, 2020).

Une autre illustration des plus marquantes du point d'honneur que met le gouvernement camerounais à combattre ces tares et/ou actes de délinquance informatiques est la sortie du président de l'Assemblée nationale le 10 novembre 2016, lors de l'ouverture de la session parlementaire, qui avait qualifié les internautes de « félons du cyberespace » et les médias sociaux qui encouragent ces pratiques de « terroristes » (Eco Matin, 2020).

Dans l'ensemble, les actions ci-dessus démontrent clairement que le gouvernement camerounais s'est activé depuis 2010 dans la lutte contre la cybercriminalité. L'on peut d'une certaine manière saluer ces quelques initiatives concrètes ayant porté quelques fruits. Toutefois, nous restons de l'avis du Professeur Abdoullah Cisse, qui pense que très peu de réponses techniques et concrètes ont été apportées par le gouvernement camerounais au phénomène de la cybercriminalité.

3.2. Les limites relatives à cette opérationnalisation

Des réponses techniques pouvant aider l'administration à venir à bout de la cybercriminalité, on apprend de nos entretiens avec des responsables techniques du MINPOSTEL qu'il a été proposé l'installation d'un serveur de surveillance des domaines de la zone « .cm » à l'Agence Nationale des TIC et l'identification des abonnés au téléphone et des terminaux (Entretien, 2022).

Si l'on peut se réjouir du succès de la campagne d'identification des abonnés au téléphone, initiative lancée par le gouvernement à l'endroit des opérateurs de téléphonie, beaucoup reste encore à faire. Comme les pays Africains ont de plus en plus accès à Internet haut débit, les questions liées à la cybersécurité et à la cybercriminalité se posent et il est nécessaire de veiller à ce que les citoyens, les gouvernements et les entreprises soient protégés. C'est pourquoi nous pensons, dans le contexte camerounais, à une amélioration ou un renforcement des mesures de prévention des pratiques de cybercriminalité.

La cybercriminalité à n'en point ignorer est devenue l'une des formes de délinquance qui connaît actuellement la croissance la plus forte. De plus en plus de malfaiteurs exploitent la rapidité, la fonctionnalité des technologies modernes, ainsi que l'anonymat qu'elles permettent, pour commettre des infractions sur le réseau Internet. Ainsi, ces cybercriminels ont recours à plusieurs techniques qui reposent généralement sur le facteur humain et que l'on nomme l'ingénierie sociale (Quemener et Ferry, 2009). Il s'agit ici de l'art de soutirer des informations à quelqu'un par la ruse (*Ibid.*) Pour lutter contre ce caractère planétaire que revêt la cybercriminalité, aux mesures et sanctions prévues dans les multiples dispositions juridiques, le gouvernement camerounais doit adjoindre des stratégies préventives en cybercriminalité : les campagnes de prévention afin de rejoindre le plus de personnes possibles, les campagnes sociétales implantées à grande échelle utilisent divers moyens pour communiquer leurs messages à la population : des affiches posées dans des lieux publics, des messages télévisés ou diffusés à la radio ou des vidéo annonces placées dans des sites Internet (Bertrand *et al*., 2006).

Ces campagnes de prévention sociétale peuvent s'avérer très coûteuses et certains chercheurs s'interrogent sur leur efficacité et les bénéfices réels que la population en retire (rapport coût-bénéfice). En effet, les résultats des effets des campagnes de prévention universelle,

notamment en santé publique, révèlent que celles-ci sont souvent très coûteuses et n'obtiennent pas tous les effets escomptés (Bertrand *et al*., 2006).

Une campagne implantée à un seul moment (*one-off campaign*) ne sera pas aussi efficace que si les organisateurs prévoient différentes phases de rappel qui reprennent ou adressent le même message en insistant sur l'importance du problème. De plus, la façon de transmettre le message constitue aussi un facteur de succès déterminant qui doit être pris en considération.

En contrepartie, d'autres études ont montré que les campagnes de prévention universelle (tous domaines confondus) donnent parfois des résultats positifs pour le public ciblé lorsque certaines conditions sont rencontrées (Bauman, *et alt*., 2001). Par exemple, un des ingrédients clés du succès de ces campagnes de prévention est d'instaurer une phase de maintien ou de rappel à moyen et à plus long terme (Mitchell, *et al.,* 1992). La population a besoin que le message soit réitéré afin de rappeler à leur mémoire les risques ainsi que les comportements préventifs à adopter. À l'instar des spots audio de sensibilisation prononcé par le Président Paul Biya contre la pandémie au Covid19 diffusé chaque jour aux éditions du journal d'information radio, on propose qu'il en soit autant pour la sensibilisation contre les actes de cyber criminalité.

Cette opération de campagne de sensibilisation doit tenir compte d'un esprit public. Il est question de ne pas formuler des messages sans tenir compte de la qualité du public. Ainsi, comme le relève la chercheure Axelle Drack, il a été démontré que le contenu du message et la stratégie employée pour le transmettre doivent être adaptés aux besoins et aux caractéristiques du public cible (Drack, 2020). Par exemple, un message s'adressant à des intervenants formés (par exemple des professionnels de l'éducation) pourra comporter plus de contenu technique ou des allusions à leurs réalités de travail alors qu'un message s'adressant à des parents issus de différents milieux pourra miser davantage sur leurs expériences de vie à la maison (Drack, 2020).

4. Conclusion

« La cybercriminalité est un phénomène qui n'épargne aucun Etat, aucune institution, aucun individu. Le Cameroun n'en est pas épargné et subit les conséquences désastreuses de ce fléau, tant sur les biens que sur les individus », a déclaré Mme la ministre au cours du point de presse qu'elle a donné ce mercredi 12 août 2020 dans la salle de conférence de son département ministériel. Au vu des développements réalisés, il n'est point de doute des efforts que mène le gouvernement camerounais à propos de cette pratique néfaste. Malgré les formes variées que peut prendre la pratique et qui sont à l'origine de l'efficacité réduite de l'action répressive du gouvernement, il serait souhaitable que soit accentué certaines mesures visant à réduire ou barrer la route à la pratique. En dehors des actions répressives contenues dans les dispositions juridiques en vigueur, le gouvernement camerounais doit en outre intensifier, en toute urgence, les efforts visant à lutter efficacement contre toutes sortes d'activités criminelles dans le cyberespace. Outre la facilitation au partage de l'information entre le public et le privé et favoriser la coopération entre les services chargés de l'application de la loi et les fournisseurs de services Internet (ISP), l'évaluation régulière de l'efficacité des législations en vigueur et la stratégie de lutte contre la cybercriminalité doivent être une priorité constante des décideurs camerounais. Sur un autre plan, les bonnes pratiques en matière de prévention de la cybercriminalité incluent un leadership efficace, le développement de la capacité d´application de la loi et de justice pénale, l´éducation et la sensibilisation, le développement d´une solide base de connaissance, et la coopération entre le gouvernement, les communautés, le secteur privé et au niveau international. La connaissance du phénomène de cybercriminalité à la base et la prise à bras le corps de cette lutte par le gouvernement peuvent générer des résultats plus palpables.

Bibliographie

1. Abella Aini et Baziz Samira., « La cybercriminalité dans le secteur Bancaire Cas : Banques de la wilaya de Tizi-Ouzou », Mémoire de fin d'études en vue de l'obtention du diplôme de master en Science de Gestion, Université Mouloud Mammeri de Tizi-Ouzou, 2017/2018.
2. Bauman, A. E., Bellew, B., Owen, N., & Vita, P. (2001). « Impact of an Australian mass media campaign targeting physical activity in 1998 » in *American Journal of Preventive Medicine*, 21(1), 41-47.
3. Bihina Fred, « Cameroun – Cybercriminalité : La page Facebook d'ELECAM piratée ! » juin 2020, in http://www.cameroon-info.net/article/cameroun-cybercriminalite-la-page-facebook-delecam-piratee-375741.html, consulté le 11 mai 2023.
4. Boos Romain (2016)., « La lutte contre la cybercriminalité au regard de l'action des États », Thèse de doctorat en Droit privé et Sciences criminelles, Université de Lorraine, 2016.
5. Cameron Coutu (2019)., « La prévention de la cybercriminalité : résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière », Mémoire présenté à la Faculté des études supérieures et postdoctorales en vue de l'obtention du grade de Maîtrise ès sciences (M.Sc) en criminologie, Université de Montréal.
6. Drack Axelle (2020)., « 6 étapes pour définir une stratégie de communication redoutable », in https://www.appvizer.fr/magazine/communication/communication/strategie-de-communication, consulté le18 mai 2023.
7. EcoMatin, « Cybercriminalité : la réponse du gouvernement au scanner » septembre 2020, in https://ecomatin.net/cybercriminalite-la-reponse-du-gouvernement-au-scanner/ consulté le 16 mai 2023.
8. Fortin Francis (s/s la Dir) (2013)., *Cybercriminalité, entre inconduite et crime organisé,* Presses internationales Polytechnique et Sûreté du Québec, 388p.
9. Ghernaouti-Hélie Solange (2009), *La cybercriminalité : le visible et l'invisible,* Collection le savoir suisse, 123p.
10. Institute for Security Studies, Karen Allen « Is Africa cybercrime savvy? » (2019) (accessible en anglais sur : https://issafrica.org/iss-today/is-africa-cybercrime-savvy).
11. Kaspersky Eugene (2009), « *Cybercriminalité, une guerre perdue ?* », documentation française, article n°6 sécurité globale, défis de la cybercriminalité, hiver 2008-2009 ; France ; 181p.
12. *Loi* n°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun.
13. *Loi* n° 2014/028 du 23 décembre 2014 portant répressions des actes de terrorisme.
14. Lucas André (1987)., *Le Droit de l'Informatique*, Paris, éd PUF, n° 413.p
15. Mitchell E. A., Aley P., Eastwood J.., « The national cot death prevention program in New Zealand », juin 1992 *in https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1753-6405.1992.tb00045.x*, consulté le14 mai 2023.
16. Parker Donn B (1985)., *Combattre la Criminalité Informatique*, Paris, OROS.
17. Pansier Frédéric-Jérôme et Jez Emmanuel (2000)., *La criminalité sur internet*, Paris, PUF.
18. Perrin Stéphanie (2005)., « "Cybercriminalité". Enjeux de mots : regards multiculturels sur les sociétés de l'information », C & F Éditions, 5 novembre.
19. Quemener Myriam, Ferry Joël (2009)., *Cybercriminalité, défi mondial*, Economica, 2e éd., cité par Romain Boos. « La lutte contre la cybercriminalité au regard de l'action des États ». Thèse de doctorat en Droit privé et Sciences criminelles, Université de Lorraine, 2016. https://tel.archives-ouvertes.fr/
20. Union africaine, « Convention sur la sécurité cybernétique et la protection des données à caractère personnel », article 3(g) (2014) (accessible sur : https://au.int/fr/treaties/african-union-conventioncyber-security-and-personal-data-protection).
21. Union africaine, « Une approche globale sur la cybersécurité et la cybercriminalité en Afrique » en page 9 (accessible sur : https://au.int/sites/default/files/newsevents/workingdocuments/31357-wddoc_on_cybersecurity_extra_ord_session_stc_cict_bamako_sept_2016_fr.pdf).
22. Wall David (2001)., *Crime and the Internet*, ed Routledge, (N.Y).