REVUE DU CENTRE DE RECHERCHE ET D'EXPERTISE EN GOUVERNANCE, RELATIONS INTERNATIONALES ET STRATEGIQUES EN AFRIQUE (RCREGRISA)

JOURNAL OF THE CENTRE FOR RESARCH AND EXPERTISE IN GOVERNANCE, INTERNATIONAL AND STRATEGIC RELATIONS IN AFRICA

LE POLITOSCOPE

N°3 Avril 2024

« Ce n'est qu'au début du crépuscule que la chouette de Minerve prend son envol »
Georg Wilhelm Friedrich HEGEL

COMITE SCIENTIFIQUE /SCIENTIFIC COMMITTEE

ABOA ABIA Alain, Professeur Titulaire en sociolinguistique, Vice-Doyen de l'UFR Langues, Littérature et Civilisations, Université Félix Houphouët-Boigny (Côte d'Ivoire).

ABOYA ENDONG Manassé, Professeur de Science Politique, Vice-Recteur chargé des enseignements, de la professionnalisation et du développement, des technologies de l'information et de la communication, Université de Yaoundé II (Cameroun).

AKONO ATANGANE Eustache, Professeur de Science Politique, Université de Yaoundé II (Cameroun).

BANGUI Thierry, Docteur en Architecture, Consultant et chercheur en développement, Bangui (République Centrafricaine).

BIPELE KEMFOUEDIO Jacques, Maître de Conférences en Droit Public, Chef de Département de Droit Public Interne, Faculté des Sciences Juridiques et Politiques, Université de Dschang (Cameroun).

CHIKOUNA Cissé, Maître de Conférences en Histoire, Université Houphouët-Boigny (Côte d'Ivoire).

DATIDJO Ismaila, Maître de Conférences d'Anthropologie, Université de Dschang (Cameroun).

DOUI-WAWAYE Augustin Jérémie, Doyen de la Faculté des Sciences Juridiques et Politiques, Université de Bangui (République Centrafricaine).

EBOGO Frank, Maître de Conférences en Science Politique, chercheur au CREPS, Université de Yaoundé II (Cameroun).

EKAMBI DIBONGUE Guillaume, Professeur de Relations Internationales, Université de Douala (Cameroun), Président du Conseil d'Administration de l'Université de Douala (Cameroun).

FANYIM Gaïus, Docteur en Science Politique, Maître de Conférences en Science Politique, Université de Douala (Cameroun).

FOLEFACK Ernest, Docteur en Droit Public, Université de Dschang (Cameroun).

JACKSON Willy, Docteur en Science Politique, Relations internationales, Université Paris Diderot-Paris 7 (France), Consultant international, Président Fondateur de Jackson International Consulting (JIC), Sarl https://www.ji-consulting.com (France).

KAMDEM Pierre, Professeur de Géographie, Université de Poitiers (France).

KAMNO Carine Gabrielle, Chargée de Cours en Science Politique, Enseignante-Chercheuse, Université de Dschang (Cameroun).

KEMIR KIYEN James, Maître de Conférences, Chef de Département de Relations Internationales et de Résolutions des Conflits, Université de Buea-Cameroun.

KOBI Joseph, Maître de Conférences en Histoire, Université de Bouaké (Côte d'Ivoire).

KOFFI-DIDIA Adjoba Marthe, Professeur de Géographie, Université Félix Houphouët-Boigny, Côte-d'Ivoire.

KOUGNIAZONDE C. Christophe, Professeur, Doyen, Docteur. Kesington Adebukonola Adebutu Faculty of Law Houdegbe North American University Benin (HNAUB), Président Exécutif Académie Alioune Blondin Beye pour la Paix (ABBAP), Cotonou (Bénin).

LOFEMBE BENKENYA BEKE, Maître de Conférences en Relations Internationales, Université de Kinshasa (République Démocratique du Congo).

MBIATEM Albert (PhD), Enseignant-Chercheur à l'Université de Buéa (Cameroun) et membre de l'African Leadership Centre, King's College London, University of London.

MANDJACK Albert, Professeur de Science Politique, Université de Douala (Cameroun).

MAOUNDONODJI Gilbert, Docteur en Sciences Politiques et Sociales, Université Catholique de Louvain (Belgique), Agrégé de Science Politique, Directeur Général du Centre d'Études et de Recherches sur la Gouvernance, les Industries Extractives et le Développement Durable (CERGIED), N'Djamena (Tchad).

MENGNJO TARDZENYUY Thomas, Chargé de Cours en Science Politique, Enseignant-Chercheur, Université de Bamenda (Cameroun).

MOSOH Lewis MULUH, Docteur en Science Politique, Université de Dschang (Cameroun).

MVELLE MINFENDA José Guy, Professeur de Relations Internationales, Doyen de la Faculté des Sciences Juridiques et Politiques de l'Université de Dschang (Cameroun).

NEMBOT NDEFFO Luc, Professeur d'Economie, Université de Dschang (Cameroun).

NGUEKEU NDONGMO Pierre, Maître de Conférences en Science Politique, Université de Dschang (Cameroun).

NGWE Luc, Docteur en Science Politique de l'Université Paris X Nanterre. Chercheur indépendant rattaché à différents groupes de recherches (France).

NODEM Jean Emet, Professeur de Sociologie, Université de Dschang (Cameroun).

NOUMBISSIE TCHOUAKE, Maître de Conférences en Histoire, Coordonnateur du Groupe de Recherche sur la Colonisation (GERCO), Université de Dschang.

MOUMOUNI Guillaume, Ph.D. (Peking University), Assistant-Professor, University of Abomey-Calavi, Bénin, Faculty of Law and Political Science, Department of Political Science.

NSOH NDIKUM Christopher, Professeur de Science Politique, Université de Yaoundé II (Cameroun).

NTUDA EBODE Joseph Vincent, Professeur de Relations Internationales et d'Etudes Stratégiques, Directeur du Centre d'Etudes Politiques et Stratégiques (CREPS), Université de Yaoundé II (Cameroun).

OMBALLA Magelan, Professeur de Science Politique, Université de Yaoundé II (Cameroun).

POKAM Hilaire de Prince, Docteur en Science Politique, Professeur de Relations Internationales, Université de Dschang (Cameroun).

SAHA Zacharie, Maître de Conférences en Histoire, Université de Dschang (Cameroun).

SADIO Adama, Docteur en Science Politique, Enseignant-Chercheur en Science Politique à Montpellier Bussiness School et à l'Université Catholique d'Afrique de l'Ouest et à Madiba à Dakar (Sénégal).

SALI Aliyou, Maitre de Conférences en Droit Public, Université de Dschang (Cameroun).

TSANA NGEUGANG Ramses, Docteur en Science Politique, Maître de Conférences en Science Politique, Université de Douala (Cameroun).

WANDJI KEMAJOU Axel, Docteur en Droit Public, Enseignant-Chercheur, Université de Dschang (Cameroun).

WASSOUNI François, Professeur d'Histoire, Université de Maroua (Cameroun).

Les opinions exprimées ici n'engagent que leur auteur

TABLE DES MATIERES

THE INTRICASES IN GUARANTEEING A HAVEN FOR SOCIAL MEDIA USERS IN TIMES OF SNOWBALLING CYBER CRIMINALITY IN CAMEROON

By

MBAH Valentine TEBECK
Ph.D. student, The University of Bamenda
Mbahtebeck80@gmail.com

MBIFI Richard, Ph.D.
Associate Professor, The University of Bamenda
mbifi@yahoo.com

KELESE George NSHOM, Ph.D.
Associate Professor, The University of Bamenda
gnkelese@gmail.com

Abstract : Social media crimes keep on soaring as days unfold making social media unsafe for its users, whereas communication even through the media has become a human right. Offences committed through social media hinder the enjoyment of this right. It is against this backdrop that countries the world over including Cameroon, have embarked on taking measures to guarantee a haven for social media users. A panoply of laws have been enacted in Cameroon and institutions set up to achieve this purpose but with little success. This paper sets out to uncover the intricacies of guaranteeing a haven for social media users in Cameroon. Through qualitative and quantitative research methods, the paper reveals that despite efforts deployed, there are jurisdictional and prosecution impediments that obstruct Cameroon's quest for protection of social media users. To counter these obstacles, the paper recommends amongst others, greater and more effective cooperation between the various stakeholders in the fight against social media crimes.

KEY WORDS: **Cameroon - Cyber Criminality- social media - Haven.**

Résumé : Les délits commis sur les Réseaux sociaux ne cessent d'augmenter au fil des jours, rendant les médias sociaux peu sûrs pour leurs utilisateurs, alors que la communication, même à travers les médias, est devenue un droit de l'homme. Les infractions commises sur les Réseaux sociaux entravent la jouissance de ce droit. C'est dans ce contexte que les pays du monde entier, y compris le Cameroun, ont pris des mesures pour garantir un refuge sûr aux utilisateurs des Réseaux sociaux. Une panoplie de lois a été promulguée au Cameroun et des institutions ont été mises en place pour atteindre cet objectif, mais sans grand succès. Cet article a pour but de découvrir les subtilités de la garantie d'un refuge sûr pour les utilisateurs de Réseaux sociaux au Cameroun. Grâce à des méthodes de recherche qualitatives et quantitatives, l'article révèle qu'en dépit des efforts déployés, il existe des obstacles juridictionnels et judiciaires qui entravent la quête du Cameroun pour la protection des utilisateurs de Réseaux sociaux. Pour contrer ces obstacles, l'article recommande, entre autres, une coopération accrue et efficace entre les différentes parties prenantes dans la lutte contre les infractions liées aux Réseaux sociaux.

MOT CLES *:* **Cameroun - Cyber Criminalité - Réseaux sociaux, refuge sur.**

INTRODUCTION

The advent of the internet has brought into place a complete revolution in the traditional intercourse between humans. The traditional modes of exchange which used to be through letter writing or sending across a messenger to deliver a message in a bit to ease communication or using telegram or fax and newspapers have today been replaced by sophisticated technology which has given birth to social media. The evolution of social media has only been possible because of the human intellect and its hungriness for communication with each other, fuelled by the advancement of information communication technology. Social media is defined as an online electronic means of communication such as websites for social networking, and microblogging through which users create online communities to share information, ideas, personal messages, and other content such as videos and images[1]. This, therefore, brings to mind platforms like Facebook, YouTube, Instagram, TikTok, Likee, Linkedln, WhatsApp, Twitter, etc[2]. Thus, Social media users being content creators[3], through these channels and mediums, can create a virtual world of communication and contribute to the information and ideas available on these social networking websites[4] just with the help of a smartphone, computer and an internet connection.

With the invention and growth of this modern technology, information that generally required days or months to get to the nukes and cranes of the globe could now be gotten within a few minutes or seconds based on the speedy nature of the interconnection between computers. This phenomenon from the early 2000s witnessed a speedier and drastic transformation with the creation of mobile phones and smartphones which today permit every user to sit at the comfort of their bedside, distribute and get whatever information they want. With the proliferation of diverse actors in the dispensation of this new technology, such as mobile communication network companies, Fintec and telecommunication operators, a gateway for unlimited access of users to the social media platform has been opened due to the uncontrolled nature of users'

---

[11] Available at https://www.merriam-webster.com consulted 24/05/2022.

[2] TANTOH E. Yata and NJI E. Bafuke, "Social Media and Cybercrimes: An Appraisal of Prosecution in Cameroon", *Revue Internationale de Droit et Science Politique (R.I.D.S.P),* Vol.1, No 3, 2021, p. 3.

[3] *Ibid*.

[4] TANTOH (EY) and NJI (EB), op. cit., p. 86.

subscription and access of these networks. This is equally due to the multiplicity of outlets created by these new service providers which are virtually found scattered across the globe and the unchecked access and usage by their users. This uncontrolled access to the social media network has paved the way for some unscrupulous users such as cybercriminals, who now utilise social media as a means or tool against their victims to victimise them through threats and other means via social networks. These rampant attacks which surfaced heavily in the early 2000s, proved difficult for the government to contain and redress due to the extraterritorial nature of cybercrimes.

This modern form of crime commission has proven to be more complex than the traditional modes of crime, wherein in most cases, the commission of the crime is physical or involves the physical presence of the offender or physical proximity[5] of the offender to offence. There is hardly any physical connection between the offender and the crime and even when there is a slight connection, there could be an aberration during criminal investigations caused by factors such as identity theft or cloning of IP protocol. This makes prosecution difficult since in most cases, it is difficult to identify who exactly the offender is. Where there is a possibility to uncover who the offender is, his physical presence within the competent jurisdiction of trial may be impossible. Other factors include differences in Penal norms between the offender's country and the victim's country, coupled with sovereign issues, especially when it is a state-sponsored cyber-attack[6].

Cameroon has in the last two decades put in place rigid institutional and legal mechanisms to abate and mitigate the nuance and damage that could be caused via social media outlets by cybercriminals and others. It is thus, in this reflection and response that the National Agency for Information and Technology (ANTIC) was created in 2002 by Decree n^{o} 2002/092 of 8th April 2002 and was able to register an official number of

[5] The physical doctrine proximity requires that the overt act required for an attempt must be proximate to the completed crime, or directly tending toward the completion of the crime, or must amount to the commencement of the consummation, available in Ellen Kreitzberg Criminal Law Book Resource 7.1.13, Notes and Questions- *United States v. Mandujano* Available at https://opencasebook.org. consulted 1/3/2024. Equally see G. Roger Jarjoura & Ruth A. Triplett., 1997, "Delinquency and Class: A test of the Proximity Principle", *Justice Quarterly,* Vol. 14, Issue 4, pp 763-792. Published online 18 August 2006.

[6] See the Stuxnet worm, which targeted Iran's nuclear program. The 2017 WannaCry ransomeware attack, linked to North Korea available at https://www.drishtiias.com. Consulted 28/2/2024.

12,800 cyber-attacks in Cameroon as of 2017[7]. These cyber-attacks revealed by ANTIC caused a loss of close to 4 billion FCFA due to scamming (financial fraud through the internet) ; 3.7 billion FCFA were reported to have been lost through skimming (fraud via bank credit cards)[8] On the legal perspective, there has been the adoption of Law n° 2010/13 of 21 December 2010 governing Electronic Communication in Cameroon[9]. Law n° 2010/012 of 21 December 2010 relating to Cyber Security and Cyber Criminality in Cameroon, Law n° 2010/021 of 21 December 2010 governing Electronic Commerce in Cameroon, Law n° 2011/012 of 6 May 2011 on Consumer Protection, and Law n° 2023/009 of 25 July 2023 to institute the Charter on the Child Online Protection in Cameroon.

To these, should be added the government strategy for the progress of the digital economy, amongst which one of the pillars which is digital governance aims to promote digital trust by strengthening the fight against cybercrime. This has been enabled through actions, such as the establishment of two cyber security laboratories at the Directorate of the Judicial Police for the General Delegation for National Security and the establishment of the surveillance networks of the Cameroon cyberspace within the competent administration responsible for public security. A national campaign was equally launched to identify subscribers of the telephone network in 2016 by setting up digital platforms for identifying subscribers and monitoring the electronic communication traffic as a response to Government efforts to curb cyber criminality.

However, the implementation of this legal panacea seems almost like a white elephant project at the instance of the existing institutions in the domain; the rate of such crimes has persisted as years unfold. This is evident, as statistics from the leading institution in the fight against cybercrimes ANTIC, have revealed a persistent occurrence of cybercrimes within the last decades. Statistics on the amplitude of cybercrime in Cameroon indicate that local banks lost a colossal sum of over 3 billion CFA in recent years, with close to 1200 cases of identity theft recorded with over 800 cases of scam as of 2019[10]. A 2023 report further revealed that Cameroon had in the past 13 years lost billion CFA to cyber scamming

[7] Annual report of ANTIC 2017.
[8] An exposé by Mme Minette Libom Li Likeng the minister of Post and Telecommunications (MINPOSTEL) at the Governor's conference which held in Yaoundé on the 26 July 2017, Crtv News 7:30 Broadcast.
[9] Amended and supplemented by Law n° 2015/006 of 20 April 2015.
[10] Cybercrime a threat to Cameroon's nascent digital economy, Available antic.cm https://www.antic,cm. consulted 25/2/2024.

and 80% of cybercrimes as of 2021 were linked to scamming.[11] In furtherance, an estimated 6,000 incidents of identity theft were reported as of 2021 wherein cybercriminals usurp the identities of high-profile state dignitaries and state institutions, of which 4,000 had been closed down thanks to a collaboration between ANTIC and Facebook[12]. The persistence of these crimes could equally be spotted from the rampant rise in cases of hate speech[13], defamation[14], cyberbullying[15], cyberstalking, child pornography[16], and obscene publications[17] on social media platforms such as Facebook and Tik Tok, etc.

It is in this reflection, that Cyber security experts hold that many people continue to buckle under cyber-attacks and online scams in Cameroon because they manipulate ICT gadgets and access internet services with very limited knowledge about the plethora of danger underneath. Ignorance therefore is certainly one of the factors that make cyber users more susceptible to cybercrime[18], coupled with other factors such as jurisdictional impediments. This persistence in the occurrence of such crimes puts to question the efforts by the government to salvage this nightmare social media users have got to deal with daily. Through qualitative and quantitative research methods, this paper sets out to uncover the intricacies of guaranteeing a haven for social media users in Cameroon. On that note, it would be worthy to identify and discuss those hurdles that shield the accomplishment of the herculean task of mitigating and eradicating cybercrime within the Cameroonian Society. These hurdles are classified under jurisdictional and prosecution impediments.

---

[11] Comments by TIMOTHY Shing on a report made by the DG of Antic during his opening speech a three-day seminar by Antic in Limber Cameroon to raise the awareness of magistrates and judicial police officers of the region on cyber security and cybercrimes, readings of the Guardian Post, 7 August 2023, 08:47 AM consulted 20/12/2023.

[12] See ANTIC report for 2021.

[13] Section 241-1 of the penal code (Law n° 2019/020 of December 24, 2019 to amend and supplement some provisions of Law n° 2016/7 of July 12, 2016 relating to the Penal Code).

[14] See section 305 of the Cameroon Penal Code.

[15] See *Affaire Mirabelle Lingum c/ Julien Bapes Bapes, Actu Cameroun,* available at actucameroun.com. consulted 24/2/2024.

[16] Section 342 of the Cameroon Penal Code.

[17] See section 265 of the Penal Code.

[18] ANTIC report presented in a seminar to raise awareness of the population Dja et Lobo Division of the South Region of Cameroon on cybersecurity and cybercrimes in Sangmelima 27th February 2019. Equally available at Antic.cm https://www.antic.cm consulted 29/02/2024.

I - JURISDICTIONAL IMPEDIMENTS TO GUARANTEEING A SAFE HAVE TO SOCIAL MEDIA USERS IN CAMEROON

Jurisdiction in criminal law entails two things: the area of competence of the court (territorial jurisdiction) and the matters the court is empowered to hear and determine (subject matter jurisdiction). Keeping subject matter jurisdiction aside, a major impediment in social media crimes is determining the place of commission which equally determines the place of prosecution. Jurisdiction impediments therefore have to do with determining the jurisdiction of the court, identification of the offender and issues relating to extradition of the offender since he may be in a country different from that of the victim.

A - Difficulty determining jurisdiction in social media offences

From time immemorial, jurisdiction has always proven to be a barrier to the effective prosecution of crimes. The question of jurisdiction appears to be even more fundamental and grievous in the domain of private international law or conflict of laws. This is so because the choice of jurisdiction determines the choice of the applicable law. Hence, what may be considered a breach of law in one jurisdiction may not constitute a breach in another jurisdiction. This, therefore, frustrates the process of investigating cybercrimes especially where the offender and the victim are in different jurisdictions with opposing laws as to the subject of the crime. This is a preeminent barrier to the investigation and prosecution of cybercrimes due to the principle of state sovereignty. Most of the time, the person committing the crime is located out of the country or the legal jurisdiction of the court and the agency involved in the investigation or the prosecutor seeking to charge the cybercriminal[19].

The principle of State sovereignty empowers each nation to make laws that are binding on all persons within its national territory[20]. This principle attributes exclusive right to the State to exercise complete authority and power over its geographical territory. For instance, the recent cyber-attacks of May 7, 2021, on the US colonial pipeline[21], medical infrastructures, and transport systems are difficult to investigate because the hackers are alleged to be based in Russia. Russia opposes the Budapest

[19] TANTOH E. Yata and NJI E. Bafuke, "Social media and cybercrimes: an appraisal of prosecution in Cameroon" Revue Internationale de Droit et Science Politique R.I.D.S.P, *Vol. 1, N°3* www.revueridsp.com. 2021, p.876.
[20] See Section 7 of the Cameroon Penal Code.
[21] US National Cybersecurity – Cyber for National Security by Booz Allen. Available at https://www.boozallen.com. Consulted 1/3/2024.

Convention on cybercrime for which the United States is a signatory stating that adoption would violate Russian Sovereignty and has usually refused to cooperate in law enforcement investigations relating to cybercrime[22]. It, therefore, makes it difficult for mutual assistance and cooperation on the trans-border investigation of cyber-related crimes between the two States.

A country's jurisdiction is often constrained by physical boundaries. Its concern is to detect and prosecute crimes that occur within the area of its sovereignty[23]. As such, with states making laws on the same matter from different jurisdictions, conflict of laws is unavoidable or bound to arise especially when it has to do with the criminalisation of offenses, which is a matter reserved to sovereigns. This does not ipso facto hinder Parallel investigations[24]. However, parallel investigations that lack the proper coordination may hinder effective cooperation and increase the risks associated with conflicts of jurisdiction and/or occurrence of ne bis in idem situations, not to mention the waste of resources resulting from the duplication of work. Owing to the greater potential for problematic situations, a judicial response can be hindered and there may be difficulties in asserting criminal jurisdiction. Uncoordinated investigations may result in different law enforcement authorities investigating the same targets and one investigation may cause negative consequences for the other. International cooperation can solve these problems by de-conflicting the targets of the parallel investigations, with the result that the judiciary will be more inclined to pursue cooperation as well.[25] However, the decision of a foreign court may be recognised but will be unenforceable due to conflicting views with foreign penal norms or public policy or where it is a state-sponsored cybercrime there will be a strong resentment for a foreign jurisdiction clause or solicitation.

In a nutshell, cybercrime jurisdiction could equally be established by other factors, such as the nationality of the offender (principle of nationality; active personality principle), the nationality of the victim (principle of nationality; passive personality principle), and the impacts of the State (protective principle) as long as "a 'sufficient connection' or

[22] Available at https://consultations.justice.govt, retrieve on the 01/09/2021.
[23]MCDOUGALL Robert, "Challenges in the Age of Cyberspace", Paper delivered at the Fifth Annual Judicial Seminar on Commercial Litigation, Hong Kong, 2016, p. 13.
[24] Parallel or joint or contemporaneous investigation means investigating facts which constitute criminal offences in the involved jurisdictions at the same time.
[25] The European Union Agency for Criminal Justice across borders (EUROJUST), 2020, op, cit, p. 4.

'genuine link' [can be shown] between the … [cybercrime] and the State exercising jurisdiction"[26]. In the United States of America for example, the courts have the right to hear and adjudicate on any case of cyber criminality that is aimed at materializing in the United States of America as was in the case of *DPP v. Ramon Olorunwa Abbas* (popularly known as Hushpuppi)[27]. The accused Ramon was arrested in Dubai and extradited to the USA where he was judged and sentenced to a jail term by the US courts for a crime he committed in Dubai whose effect was on the USA. The accused Ramon had been arrested in the UAE back in 2020 alongside 11 of his associates over allegation bordering on hacking, impersonation, scamming, banking fraud and identity theft. His extradition to the United States had followed after the UEA police detailed his arrest in a special operation dubbed 'Fox Hunt 2', where he was accused of defrauding 1.9 million victims to the tune of N168 billion. In 2021, a Federal Bureau Investigation (FBI) special agent, Andrew Innocent, alleged that the Hushpuppi contracted the service of Abba Kyar, Deputy Commissioner of the Police (DCP) after a "Co-conspirator," Chibuzo Vincent, allegedly threatened to expose the alleged 1.1-million-dollar fraud committed against a businessman. Innocent, who said he obtained voice calls and WhatsApp conversations between Kyari and Hushpuppi, had also alleged that the latter paid the officer N8million or 20,600 dollars for the arrest and detention of Vincent.

B - Problem of Identification of offenders

One of the greatest impediments against global efforts towards abating the whirlwind of cybercrimes remains the anonymous nature of the identity of cybercriminals. There is no hard and fast rule for identifying who is doing what and where a user of the Internet is situated at any point in time; the global information system is free and there is no prerequisite that needs to be fulfilled before a user can log in to connect from anywhere and with anyone across the globe than mere acquisition of internet data. Thus, the unfettered freedom of information and communication enables cybercriminals to hide their identity using different telecommunication

[26] See Module 3 on Legal Frameworks and Human Rights, Epping and Gloria, 2004, cited in the United Nations Office on Drugs and Crime, ,2013, p.184-185 I. 95 UNODC, The Doha Declaration: Promoting a Culture of Lawfulness, 2019, www.unodc.org>cybercrime.
[27] Trial date July 27,2021 see Sahara Reporters, New York.

gadgets to make it impossible to trace the online Internet Protocol (IP) address of any user[28].

Moreover, if one were to trace the IP address of a cybercriminal to a particular location, the next hurdle cannot be scaled as the identity of a cybercriminal is undisclosed to the owner or operator of the internet service provider[29]. Several telecommunications gadgets are used to shield the identity of internet users and communications are often routed in many servers which further compounds the possibility of cybercriminals being traced. In effect, if the identities of criminals are incapable of being traced, how can prosecution take effect so that the laws enacted do address cybercrimes work effectively?

The point being emphasized here is that, in so far as the identities of cybercriminals remain elusive, no law however well-crafted or intended, can work because the law does not work in a vacuum. In other words, cybercrime laws were principally enacted to apprehend and prosecute cybercriminals and if they are not identifiable, any law put in place will not achieve the intended purpose. It should be quickly added that the campaign in some quarters to end anonymity in the use of the internet by the mandatory introduction of identification as a prerequisite has been ferociously opposed by human rights activists on the grounds of violation of privacy rights[30]. With that development, cybercriminals appear to have been offered latitude to continue to operate unhindered and by so doing, the challenge of anonymity continues to render cybercrime laws nugatory.

Anonymity enables individuals to engage in activities without revealing themselves and/or their actions to others[31]. There are several anonymization techniques that cybercriminals use. One such technique is the use of proxy servers. A proxy server is an intermediary server, which is used to connect a client (i.e., a computer) with a server that the client is

---

[28] AJAYI, E. F. G, "Challenges to enforcement of cyber-crimes laws and policy", *Journal of Internet and Information Systems, Vol. 6(1),*2016, p. 4 at http://www.academicjournals.org/JIIS (accessed on the 17th of July 2022).

[29] TANTOH (E-Y) and NJI (B-E) op, cit, p. 887.

[30] The most prominent argument against ID verification is that online anonymity is necessary in some parts of the world in particular those who live in oppressive regimes who make their oppressors wrongs known to the rest of the world through their anonymous social platforms. Oppressive regimes may imprison (worse) user for speaking out online. Requiring ID verification, could significantly deter whistle-blowers from speaking out. By Aiden P. 2021, Social Media ID Verification & the Right Privacy/Anonymity available at LinkedIn. Aidan P. consulted 2/2/2023.

[31] HELEN M. Mary, Cyber criminology, Oxford University Press, ISBN: 9780190278441 1st Edition, 2016, pp. 1-448.

requesting resources from[32]. Anonymiser or anonymous proxy servers are used to hide the user's identity. This is done by making their IP address hidden while substituting it with a different IP address. Most often the Cameroon IP addressed might be masked and changed with that of another country. To this, there exist legitimate reasons for which some individuals will want to remain anonymous online and maintain the protection for anonymity online. For example, anonymity facilitates the free flow of information and communication without fear of repercussions for expressing undesirable or unpopular thoughts[33] especially, in cases of oppressive regimes. This makes difficult and complex the possibility and procedure of identifying and mapping out the cybercriminals.

In addition, even where the identity of the user is known, most often investigation has revealed that the account or identity being used by these cybercriminals, appears to be the account(s) of neutral persons or in some cases, deceased persons that have been hacked and these criminals use them to defraud others through an identity theft. This phenomenon is very rampant with users of Facebook.

C) - Challenges relating to extradition of identified offenders

Extradition refers to the removal of a person from a requested state to a requesting state for criminal prosecution or punishment[34]. Extradition has also been defined as the surrender by one state to another of a person accused of committing an offense in the latter[35]. A casual glance at the definition of extradition as above would ordinarily raise the hope that if a person is alleged to have committed a computer crime in one jurisdiction and escapes to another country, all that needs to be done by the country where the cybercriminal is domiciled is to expeditiously return the said criminal to the requesting country, to face trial. However, in practice, this is not so because of the principle of state independence and sovereignty earlier mentioned. Under international law, except in countries of the European Union, no instrument imposes on sovereign states an obligation to automatically return cybercriminals except if there is an extradition treaty between the requesting and requested states. In effect, countries where cybercriminals are resident, for different reasons more often refuse

[32] HELEN M. Marie, Forth International conference on Mobile Adaptability and Rapidly Assembled Structures11-13 June 2014 Ostend, Belgium, p. 294.
[33] HELEN (M-M), Cyber criminology, op, cit.
[34] Available at https://www.law.cornell.edu consulted 20/9/2022.
[35] BEDI (D.S), "Law and Practice of Extradition within the Commonwealth Countries", Journal of the Indian Law Institute, Vol.19, No 4, 1977, pp. 419-437.

to extradite the criminals and this presents an insurmountable challenge to the enforcement of cybercrime laws across the globe[36].

To address the lacuna created as a result of the lack of mandatory provisions of international law to extradite criminals, extradition treaties fill the void. Criminals may be extradited where there is a treaty, but even at that, there may be many exceptions to extradition processes. In Cameroon, the basis for extradition is the preamble of the constitution[37] and the conditions for extradition are regulated in article 642-645 of the Criminal Procedure Code[38]. However, extradition is not permissible if that could be prejudicial to the rights of defense of the accused person, or if the request was based on political, religious or racial reasons, or based on the nationality of the person concerned. It is worth noting that as of date, Cameroon has concluded three bilateral treaties on mutual legal assistance with Mali, the Democratic Republic of Congo and France[39], which is in line with article 46 of its constitution. But then it will be important to state that Cameroon has not yet agreed on the transfer of sentenced persons or enabled any specific legislation on the transfer of criminal proceedings[40].

One of the biggest hurdles to the extradition of criminals to requesting states is the unruly legal issue called jurisdiction. Jurisdiction is often invoked by countries to deny extradition especially if the requesting states have jurisdiction to try criminals and if the cybercrime was state-sponsored or was aimed at benefiting the state wherein the crime originated from[41]. For example, on February 16, special counsel Robert S. Mueller III unsealed a 38-page indictment charging 13 Russian nationals and three entities principally with conspiring against the United States to infiltrate the 2016 election through a sophisticated and complex scheme that included the use of stolen identities of American citizens to surreptitiously influence and infiltrate social media sites as Facebook, Instagram and Twitter. Although each United States intelligence agency had definitively stated, without equivocation, that Russia meddled in the 2016 presidential election, those agencies were constrained to explain how Russia did so with any detail because of legal restrictions on classified

---

[36] HERBERT Atuheire, *The Challenges in Investigating and Prosecuting Computer Crimes. A Reflection on Online Fraud in Uganda,* Bachelor Degree Research Report, School of Law, Kampala International University, 2017, p. 17.
[37] See article 65 of Law No 96/06 of 18 Dember 1996 on the Cameroon Constitution.
[38] Law n° 2005/007 of 27 July 2005 on the Criminal Procedure Code.
[39] CAC/COSP/IRG/1016/CRP.22 available at https://www.unodc.org consulted 4/3/2024.
[40] Ibid.
[41] American Constitution Society, Available at https://www.acslaw.org. Consulted 4/3/2024.

material. Yet for the first time, the indictment provided extensive detail about how one aspect of this Russian meddling in the 2016 election occurred. The indictment, however, likely will never see the inside of a courtroom as none of the defendants have since then been arrested given that all 13 of them are said to be based in Russia[42]. In this regard, the United States is essentially powerless to extradite them and bring them to justice due to issues of jurisdiction, given that Russia is against any extradition of its citizens for trial in a foreign jurisdiction. In this regard, the requesting state has no choice other than to abide by that decision of not commencing extradition. By this, the objective of criminal justice is marred as the enforcement of applicable cybercrime law is defeated by the legal hurdles placed in the path of justice.

II - PROSECUTION IMPEDIMENTS AGAINST GUARANTEEING A SAFE HAVE TO SOCIAL MEDIA USERS IN CAMEROON

Several factors make tackling cybercrime unique and challenging when it comes to prosecution. The persistent rise in the rate of social media crimes could be a result of impediments linked to the prosecution procedure. Prosecution impediments within the reasoning of this paper are the challenges encountered in the prosecution of social media crimes in Cameroon. These challenges that are in their numbers have acted as a brake puzzle to the effective implementation of the available regulatory and legal mechanisms on social media that could afford effective and efficient protection to social media users in their daily predicaments orchestrated by cybercriminals. The challenges encountered turn around problems relating to proving social media crimes, the problem of trained personnel, ineffective cooperation of stakeholders, etc.

A - Constraints in proving social media offences

It is no news that in criminal matters, the conviction of an accused is based on the weightage of the evidence tendered against him by the prosecutor. Evidence must exist relating to the person of another, other than the prosecuting counsel for such person to be convicted. Evidence can be said to be a declaration or proclamation made to establish or prove the existence of certain facts or incidents. According to Cross[43], "the evidence of fact is that which tends to prove it. Something which may satisfy an

[42] American Constitution Society, Available at https://www.acslaw.org. Consulted 4/3/2024.

[43] See Evidence by RUPERT Cross, reviewed by G.D. Nokes, The Modern Law Review vol. 21, No. 4 (July 1958), pp. 448-450 available at https://www.jstor.org/stable/1090722. Consulted 28/2/2024.

inquirer of the fact existing". Evidence is how facts are proved excluding inferences and arguments.[44] It is as such the acceptance of the statement of things presented by the person testifying in establishing the existence of certain facts by the court that occasions a proven fact. But the fact is that such evidence must be readily available in order to be admissible[45]. The difficulty in making evidence readily available and admissible, however, lies in the controversial nature of the evidence and the identity of the accused person. This is so as the available evidence may not relate to the accused person due to the subsequent discovery of issues of identity theft as aforementioned. In other circumstances, the required evidence is either inaccessible or merely inexistent to inculpate an accused person. These factors and others, definitely render difficult the smooth administration of justice. But for there to be prosecution, there must have been a partial attempt or a full consummation of the act of the offense[46] and the victim must have brought legal action against an identifiable or an unidentifiable individual.

The nature of evidence during investigation and trial poses a great deal of problems in cybercrimes. The evidence may consist of oral testimony, documentary evidence, or real evidence for it to be admissible. The principles governing evidence in a trial present the conditions under which such evidence can be admissible. The rules of evidence in any criminal trial in Cameroon are laid down in sections 307 to 321 of the Criminal Procedure Code. Section 313(1) of that Law provides that: the contents of a document may only be proved by primary evidence or, where necessary, by secondary evidence. Oral evidence in proof thereof shall not be admissible. Evidence could take any form such as circumstantial, conclusive, direct, extrinsic, primary, secondary or expert opinion. However, the purview of evidence concerning cybercrimes is the application of science to decide questions arising from crime or litigation known as forensics.[47]It is the role of the prosecution to secure a conviction and to prove its case beyond reasonable doubt.

The nature of evidence required for cyber criminality is generally electronic. Electronic evidence in cybercrime cases in the court is any data

---

[44] AKINOLA T. Aguda, The Law of Evidence in Nigeria, London: Sweet and Maxwell; Lagos: African Universities Press, 2009, (Law in Africa Series No.22). 1966.
[45] SKORUPKA Jerzy, "The rule of admissibility of evidence in the criminal process of continental Europe." *Revista Brazileira de Direito Processual Penal, Porto Alegre,* vol. 7, n.1. 2021, pp. 93-122.
[46] BARNES Henry, "1946, Liability for Crime", *Cambridge Law Journal, Vol.9, No.2*, pp. 210-238.
[47] AJAYI, (E-G), op. cit, p. 7.

related to electronic devices whether it is created, stored, manipulated or transmitted in a digital form[48]. This evidence can be stored and retrieved from hard disks or memory banks of electronic devices like computers and Smartphones, whereas, for their fragile nature, electronic files are pruned to damage, destruction or it can be altered which poses a question of its authenticity bearing little or no significance before the court. Other concerns relate to the fact that electronic evidence of such crimes may be difficult to collect, owing to the volatility of data, and may require specific expertise[49]. Proving cybercrimes is thus a difficult and frustrating task as even when it is believed that a person is a cybercriminal, the courts require substantial evidence to link the accused to a particular cybercrime. In addition, electronic evidence can be freely moved across national borders and easily taken out of an investigator's reach by being deleted, transferred to a new jurisdiction or encrypted[50]. The evidence that is generally not readily available to the court and which is difficult to come by renders prosecution difficult and at times frustrates ongoing proceedings which mostly end up in acquittal and discharge due to want of sufficient evidence to convict the accused.

It is even more of a 'technical challenge' for police investigators and other criminal justice agencies to understand and deal with electronic evidence. This has to do especially, with its preservation and extraction process. Hence, if the evidence is not properly dealt with, the court judgment of cybercrime-related offenses could be different[51]. Besides, digital evidence is better than the defendants' confession and seized material evidence. Cybercrime investigators must be familiar with the technology underlying a cybercrime case[52].

Additionally, the uncertainty about the availability of electronic evidence results from the absence of any streamlined legal framework for data retention. However, this issue is not exclusive to cybercrime investigations; the same problem can be detected in phone communication

---

[48] SA'DI M. Mustapa, Kamarudin A Mohamed, D., and RAMLEE Z. Saad "Authentication of electronic evidence in cybercrime cases based on Malaysian laws". Pertanika Journal of Social Science and Humanities, 23 October, 2015, pp. 153-168.

[49] EUROJUST, Challenges and best practices from Eurojust's casework in the area of cybercrime, 2020, p. 3 at http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx (accessed on the 18th of July 2022).

[50] EUROJUST, (2020), *op.cit*, p. 4.

[51] Ibid.

[52] WINMILL B. Lynn, METCALF L. David, BAND E. Michael, "Cybercrime: Issues and Challenges in the United States", Digital Evidence and Electronic Signature Law Review, Vol 7, 2010, p. 27.

data, as telecommunications service providers have no uniform legislation in place establishing minimum standards for data retention.

In criminal justice systems, information traditionally has been textual, linear, impersonal, and paper-based and flowed in one direction across loosely coupled criminal justice agencies. Social media content, in contrast, is multi-medium, digital, holistic, emotional, and image-dominated[53]. The fact that information now flows from diverse angles has equally affected the nature of the evidence that is required by the law courts. This therefore makes it more complex to gather such evidence and is thus advantageous to cybercriminals who may go unpunished because of these challenges. An illustrative example is in the case of The People of Cameroon v. Ekume Otte Sakwe[54] where the accused with elected residence in Buea, South West Region of Cameroon was charged with the offense of publication of fake information relating to three companies to wit : Yadikwa Immobilier, Agro Agricultural Cooperative Ltd and Darling Home without being able to attest its veracity under Section 78(1) of the Cyber Law[55]. After the Examining Magistrate had conducted the Preliminary Inquiry, the defendant Mr Sakwe was discharged for want of sufficient evidence to establish that his acts were in any way linked to the cybercrime. Most of the time, evidence available to the prosecutor in cybercrimes is never enough to secure such a conviction to bring cybercriminals to book. Unlike in traditional crimes where physical evidence could be presented to the court, such evidence is rare in cybercrime prosecution. The investigators and prosecutors may sometimes only rely on footprints on the computers used by the criminals and traces left on the internet. The value attached to this evidence does not have weight and may slightly leave an open door to the culprit. This digitalized evidence is very delicate and may be contaminated or damaged by an inexperienced investigator. It equally needs the availability of forensic equipment to be able to carry out proper investigations which is so costly.

Cybercriminals who are targeted or afraid that they might be caught may wilfully destroy evidence in their computer systems or other digital equipment and files that may implicate them or create a password that cannot be easily decoded. When this is done, investigators will find it

---

[53] SURETTE Ray, "How Social media is Changing the way people commit crimes and police Fight them" Crime, media, culture: *International Journal, USAPP United States politics and Policy,*2016 blogs.ise.ac.uk. 102CFIB/017b/2015 (Unreported).
[54] CFIB/017b/2015 (Unreported).
[55] Law n° 2010/012 of 21st December 2010 relating to Cyber Security and Cyber Criminality in Cameroon.

difficult to follow up with such criminals in order to track them down and prosecute them. The fact that internet fraudsters do create fake accounts (it could be by identity theft[56] or cloning) permits them to hide from investigators the true identity of the criminal and moreover make unavailable inculpatory evidence[57] in cases where they could be suspects. Furthermore, evidence collected because of its technical and complex nature may not stand the test of time in court. For instance, suppose a victim of a cyber-offense has an accurate log file that shows an intruder breaking into his computer system or mobile app, he can copy that log[58] or screenshot the post or message and give it to the investigating police or the agency but rarely will that information withstand proof of the alleged illegal act before the court of law. This argument can logically be that; the victim stands the challenge of proving that: the log file or the image or message has not been tampered with or is not fake; he could access the log file; there is accuracy of time and date when such information was accessed; his computer or phone/tablet is accurate in detecting the originating Internet Protocol (IP) address against 'fake'; the experience of the investigating agency in obtaining legal forensic evidence. Courts in Cameroon have thus found it difficult to convict cyber criminals because of the complicated nature of building evidence on cybercrimes in the country[59]. This can be seen in the case : The People of Cameroon v. Kadji Valery[60]. In this case, Kadji, a University of Buea student, fraudulently acquired a sum of money from a lady in Yaoundé. The matter was reported to ANTIC which investigated and traced Kadji's account at BICEC Buea credited with the sum of 1.090.000FCFA Francs. With this, ANTIC held that Kadji could not have had such an amount in his account if not for scamming and so he was charged under Section 73(2) of the Cyber Law. Unfortunately, the matter was discharged for lack of evidence to prove that money in his account was taken from an illegal act.

Given the complicated nature of gathering forensic evidence during the investigation of cybercrimes, it is very discouraging to engage in the same. The cost of such scientific crimes and time is so expensive as opposed to investigating terrestrial crimes. Investigators of cybercrimes need high-tech equipment, materials and the assistance of expertise.

---

[56] See section 43 of Law n° 2010/012 of 2 December 2010 relating to cyber-Security and Cyber criminality in Cameroon.
[57] Inculpatory evidence is evidence that establish the guilt of an accused or information that shows a defendant's involvement in a crime.
[58] ROGER (A-G), op. cit, p. 12.
[59] TANTOH (E.Y) and NJI (E.B), op. cit, p. 893.
[60] CFI Buea/011A/2013, unreported.

Transnational cybercrimes are deemed to be more costly and time-consuming in investigation and prosecution. For instance, the investigation of cybercrimes in two jurisdictions may require the physical presence of the investigators[61]. In the latter case, investigators will have to embark on air travel and whose stay will require accommodation, feeding, transportation, entertainment and other costs. Another problem often encountered during the investigation is the language barrier[62]. A glaring example is when Chinese investigators are obliged to work with English or French counterparts or English to work with French counterparts. To sort out these issues will require additional costs because translators will often be recruited. The difference in culture and the perception of cyber criminality should not be overlooked.

B - Inadequacy of Well-Trained and Well-Equipped Personnel to Gather Evidence

The inadequacy of well-equipped and trained personnel stands out as another challenge encountered in the prosecution of cybercrimes, given that cybercrimes are complex and can be unfamiliar to those within the criminal justice field. Investigation and prosecution of cybercrimes require well-trained and knowledgeable personnel afforded with appropriate technological facilities coupled with effective legislation[63]. In Cameroon for example, most investigating officers lack adequate training in the field of ICT. This is evident by the fact that, in some years past, there was no special training on ICT given generally to all categories of law enforcement officers during their training course and seemingly is the case with some categories of this core nowadays. It is only in the last two decades, that it has dawned on the authority to recruit ICT technicians, and even with this initiative, the number recruited is very insignificant to a country with an estimated 30 million inhabitants[64]. This is even more complex with the judiciary where there is no course on ICT taught to magistrates undergoing training. This presents a serious setback as it is difficult for these investigation officers to prove or present sufficient evidence on most alleged cybercrimes. This has only permitted an increase in the rate of social media crimes as they keep multiplying by the day,

[61] See Section 57 of Law n° 2010/012 of 2 December 2010 Cybersecurity and Cyber Criminality in Cameroon.
[62] E.F.G Ajayi, op. cit, (note 83), p. 9.
[63] Sheelagh Brady & Caitríona Heinl, *Cybercrime: Current Threats and Responses*, Department of Justice and Equality, Research and Data Analysis Unit, 2020, p. 75.
[64] Arrete No. 55/DGSN/SG/DARH/SDROPS/SR on the recruitment of 3 technicians in electro-technic into the 1st year course for the National Police School as from 24th February 2024.

especially hate speech, defamation, and child pornography, where most youths including teenagers between the ages of 16 and 18 are involved.

Social media-related crimes have specifically been defined in our legal system following the introduction of Law n° 2010/012 of 21st December 2010 relating to Cyber Security and Cyber Criminality in Cameroon. This has placed investigators and prosecutors in the position of continuous learning with the sophisticated skills that accompany internet activities. Our legal system has traditionally been directed at the physical world for physical crimes. Investigators find it difficult to investigate such complex crimes especially when it involves trans-border actors. Cybercriminals are very smart and always look for avenues to make unlawful wealth or in rare cases wreak havoc on computer systems. They often use sophisticated programs in their computers and passwords which only experts in computer science can decode. They have been described as professional thieves and soldiers of fortune.[65] The investigation of cybercrimes requires highly skilled personnel in cyber security. In Cameroon for instance, ANTIC in collaboration with ART is the competent body to regulate and monitor electronic security activities; it also does investigations assisted by Judicial Police Officers[66]. It is quite saddling to affirm that these officials are not well equipped with the appropriate technology required to track down cybercriminals who have very sophisticated equipment and methods of operation.

Furthermore, the dearth of experts in the prosecution of cybercrimes is another challenge. It is a well-known fact that even if law enforcement agencies do a good job in the investigation of computer crimes, at the litigation stage, the expertise of prosecution attorneys is still very important to secure the conviction of cybercriminals as it is incumbent on the attorney to prove his case beyond reasonable doubts. Unfortunately, this is not the case as there is a dearth of savvy prosecutors in government justice departments[67]. On the contrary, cybercriminals have unfettered access to renowned private attorneys who charge very high legal fees which is not a problem to them. Cybercriminals could readily afford to pay high professional fees to the finest lawyers who specialize in computer

[65] Legal Brief E Law & Management Cyber law & Technology Watch Issue No.1581, 29 2015, p. 1.
[66] NDI Rodrick, "Reflection on Police Power of Arrest, Detention and the Treatment of Suspects under the Cameroonian Criminal Procedure Code and Extra-National Laws: Human Rights Digest." *National Journal of Criminal Law. 2(1)*: 2019, pp. 4-12.
[67] Legal Brief E Law & management cyber law & technology watch issue no: 1581 29th 2015 p. l.

crime practice[68]. These identified gaps unfortunately are a plus for cybercriminals who in addition to technicalities in computer crime cases have more than enough funds to hire first-class attorneys[69].

C - Ineffective cooperation in the prosecution of social media offences

There are many stakeholders in the prosecution of social media offences who are bound to cooperate to be able to achieve reasonable results. It all begins from when the act is committed; there should be someone to lay a complaint against an identified or unidentified offender, except in a flagrante delicto procedure. Public-private partnerships and collaboration between the various law enforcement agencies should be effective. Unfortunately, that is not often the case.

1 - Problems of effective reporting of social media crimes

Though many countries in the world have applicable laws and policies against computer crime, the enforcement of the same is a challenge and part of the challenge is not unconnected with the lack of effective reporting of incidences of computer crimes to the appropriate authorities across the globe. This has discouraged bringing global attention and appreciation to the extent of the menace of computer crimes. Closely related to reluctance to the disclosure of computer crimes is the lack of cooperation on the part of the victims, other stakeholders and witnesses with police or other agencies concerned with investigation and prosecution of cybercriminals. It is immaterial whether private corporations or institutional entities are the victims.

Several reasons are advanced for reluctance to report computer crimes and these include but are not limited to costs arising from follow-up by the victim of the computer crimes which more often than not will outweigh the benefit derivable thereof, the damage to the reputation and goodwill of victims especially. Many individuals and families have benefitted from the money gotten from scamming in Cameroon, which has of course increased their living standards and spending ability. Such beneficiaries, who are quite aware of the affairs of scammers, cannot at the same time be the ones to report.

A rapid rise in low-threshold, high-impact cyberattacks, for example as part of an extortion scenario (for example using ransomware),

---

[68] ATUHEIRE Herbet, The Challenges in Investigating and Prosecuting Computer Crimes : A Reflection on Online Fraud in Uganda, LL.M Dissertation Kampala International University Law School, 2017, p.29 (Published).
[69] Ibid.

brings completely new types of problems. Owing to the scale of such criminality, a massive number of victims located in several jurisdictions – it can be extremely difficult to identify and/or properly involve the victims in criminal proceedings. This is so because many types of victims are not inclined to report these kinds of attacks, as their reputation would suffer, with economic consequences (for example, accounting companies and banks do not like to discuss the loss of partners' sensitive data). In the USA for example, General Keith Alexander, the head of the National Security Agency and the U.S. Cyber Command in 2013, called the loss of American business secrets and intellectual property to cyber criminals "the greatest transfer of wealth in history"[70].

It is common to know that there are scammers in our community but no one dares to report them. This could be explained by the fact that most people have no idea of where and how to report internet crimes and even if they do report, rarely does anything come out of it due to lack of evidence. Some victims are never even satisfied with the outcome of the investigation. For instance, empirical evidence of a survey carried out by the consultancy firm Ernst and Young[71] found that only one quarter (¼) of frauds reported in the survey were referred to the police and further, that only 28% of those respondents were satisfied with the said investigation[72]. For businesses that are in a competitive environment, reporting cyber incursion is viewed as exposing the weakness or vulnerability of systems which will reduce the clientele confidence thus engendering consumer turn-away. The owners and operators would rather keep silent and try as much as possible to rectify the system than report to authorities in charge of cybercrimes. We can neither roll out the dubious habits of some security officials who often trade the arrest of such culprits for financial benefits[73]. This denial to denounce or report cybercriminals renders difficult the proper administration of Justice by the Judiciary in Cameroon, as investigations and prosecution in most circumstances get frustrated due to the unavailability of evidence strongly caused by the non-cooperation of the civil society.

[70] SEABROOK John, Network Insecurity, NEW YORKER, May 20, 2013, at 64 (quoting Gen. Keith Alexande).
[71] ERNST and YOUNG, Global information Security Survey under cyber-attack, 2013 available at: https://www.acfe.de,retrieved on the 2/09/2021.
[72] Ajayi, E.F.G., (2016), *op. cit.,* p. 8.
[73] BORAINE (A) and LENO (N-D), op. cit, p. 94.

2 - Challenges of Public-Private Partnerships

Cooperation with the private sector is vital in combating cybercrime. The private sector holds much of the evidence of cybercrimes. The private party could easily take down criminal infrastructures; remove illicit contents and report data breaches to law enforcement officers. These are amongst the most effective measures that could be employed to fight cyber criminality. A public-private partnership therefore plays a key role in mitigating cybercrime and increasing cyber security through prevention and awareness. However, little consensus exists on the legal framework that is required to facilitate effective and trust-based cooperation with the private sector, while at the same time regulating legal and transparency issues surrounding that cooperation. Moreover, data protection regulation and fear of liability may result in limitations to cooperation with the private industry. A need has been demonstrated for standardized rules of engagement with private industry, as well as a clear understanding of the extent to which private parties can obtain evidence themselves and the legal implications of their actions, such as for the admissibility of such evidence in court proceedings[74].

There may be conflicts in partnership between the sectors preventing its success, including factors related to bureaucracy, regulations, data privacy and leakage of classified information. Cybercrime centers are too focused on protecting the government systems, and within it, public-private collaborators pose challenges when it comes to the fear of information leakage during the sharing of data and the private sector's worries that the government may penalize them. According to Ngair Teow-Hin, CEO of the Secure Age, many cybercrime centers are structured to focus on protecting government systems and critical infrastructures[75]. As such, they turn to leave out the private sector, and subsequently, they cannot benefit from such government efforts and their computer systems remain vulnerable to cyber-attacks.

Moreover, both sides are equally worried that information shared outside their respective organizations may be disclosed to unauthorized parties. For example, Japan National Police Agency (NPA) admitted facing difficulties working with private sector employees to leverage their skills for the cybercrime investigation, over concerns that classified information may be leaked[76]. Additionally, the private sector is also hesitant to

[74] EUROJUST and EUROPOL, (2019), *op. cit.*, p. 17.
[75] Ibid.
[76] Ibid.

collaborate with the public sector organization as they fear that opening up to the government may open an opportunity for them to find ways to penalize the private sector's activities or policies[77]. It is no news that some of the cybercrimes are even sponsored by private firms and businesses[78] that compete with other firms to remain in domination in their line of business. These difficulties therefore frustrate the effective collaboration between the private and public sectors in the fight against cyber criminality.

3 - Inadequate collaboration between law enforcement agencies

Judicial cooperation is essential to ensure the timely preservation of electronic evidence, which ensures its admissibility in judicial proceedings. International judicial cooperation may be hampered by significant differences in domestic legal frameworks (for example, regarding criminalisation of conduct or data retention legislation) and conflicts of jurisdiction. The whole phenomenon of cyber criminality is reshaping the traditional legal concept of the territoriality principle as a result of the supranational nature of the evidence required to ensure the successful prosecution of cybercriminals[79].

There may be insufficient expertise for a thorough examination and cross-examination of the intricacies of electronic evidence. Similarly, expertise is required within law enforcement authorities to capture and handle such evidence in a forensically sound fashion. Currently, there is no internationally agreed forensic standard for the collection of electronic evidence for the purpose of criminal investigations and prosecutions[80].

However, the state has some internal capacities and sources it could use to tackle this drawback in the investigation and prosecution of cybercrimes, but they are insufficient to respond to cyber-attacks of major dimensions. The limited knowledge of the internet by law enforcement officers, motivation and lack of collaboration between the different agencies put in place to tackle cybercrimes have improved the capability and facilitations that made cyberspace an attractive environment for

---

[77] PHNEAH Ellyne, Contributor on March 8, 2013, New York Times Breached by Chinese Hackers, New York Times. Available at https://www.zdnet.com accessed 20/9/2022.

[78] YONGU Zeng and BUIL-GIL David, Organizational and Organized Cybercrimes. In H. Pontell (ed), Oxford Research Encyclopedia of Criminology and Criminal Justice, New York and Oxford, Oxford University Press, 2023.

[79] YONGU (Z) and BUIL-GIL (D)., op. cit., p. 3.

[80] Ibid., p. 5

criminals. Cybercrime is a phenomenon that touches upon a series of competencies, such as informatics, criminology, economy, justice, etc. Therefore, cybercrime is to be considered as a complex phenomenon and the only way to confront it successfully is through a global approach in handling this problem. For this, there is a need for cooperation between experts in different fields to avoid partial solutions.[81]

CONCLUSION

This paper set out to unveil the intricacies of ensuring a haven for social media users in Cameroon. After identifying and analysing the existing legal and institutional mechanisms put in place as a response to the fight against cybercriminality, our analysis revealed that there are factors beyond national control that act as a shield to the prosecution of cybercrimes, putting to question the effectiveness and efficiency of both the existing legal and institutional mechanisms. Jurisdiction appears as a fundamental impediment because not only is it difficult to determine the physical location of the offenders, but in most situations of state-sponsored cyber-attacks, prosecution could be hampered by the state that initiated the cyber-attack. Still related to jurisdiction, extradition which permits the prosecution of a criminal from the requested by the requesting state, is hard to come by. The difficulty in extradition is also strongly related to sovereignty and state policies; Russia for instance, is against the trial of its citizens in any foreign court. Issues of identification coupled with the nature of evidence required and how to deal with it as well as inadequate training and equipment of personnel, are also paramount. The paper concludes that the legal and institutional frameworks in place cannot afford an effective protection to social media users in Cameroon. This, therefore, makes indispensable the need for global cooperation amongst states to combat cybercriminality.

BIBLIOGRAPHY

- AKINOLA T. Aguda, *The Law of Evidence in Nigeria,* London: Sweet and Maxwell; Lagos: African Universities Press, Law in Africa Series No.22, 2009, pp. 1-403.
- ATUHEIRE Hebert, *The Challenges in Investigating and Prosecuting Computer Crimes: A Reflection on Online Fraud in*

[81] AHMET, "Challenges in Combating the Cyber Crime", Mediterranean Journal of Social Sciences MCSER Publishing, Rome-Italy Vol. 5 No. 19, 2014, p. 597.

Uganda, LL.M Dissertation Kampala International University Law School, 2017, pp. 1-35.

- BARNES Henry, Liability for Crime", *Cambridge Law Journal, Vol.9, No.2*, 1946, pp. 210-238.
- BEDI D.S., "Law and Practice of Extradition within the Commonwealth Countries", Journal of the Indian Law Institute, Vol.19, No 4, 1977, pp. 419-437.
- BORAINE Andre and NGAUNDJE LENO Doris, "The Fight against Cyber Criminality in Cameroon", International Journal of Computer (IJC) Volume 35, No.1, 2019, pp. 87-100.
- FEMI GBENGA Ajayi Emmanuel, "Challenges to enforcement of cyber-crimes laws and policy", *Journal of Internet and Information Systems, Vol. 6(1),* 2016, pp. 1-12.
- JARJOURA Roger G. and TRIPLETT Ruth A, "Delinquency and Class: A test of the Proximity Principle", *Justice Quarterly,* Vol. 14, Issue 4,1946, pp. 763-792.
- HELEN Mary, Cyber criminology, Oxford, Oxford University Press, 1st Edition, 2016, pp. 1-448.
- MCDOUGALL Robert, "Challenges in the Age of Cyberspace", Paper delivered at the Fifth Annual Judicial Seminar on Commercial Litigation, Hong Kong, 2016.
- NDI Rodrick, "Reflection on Police Power of Arrest, Detention and the Treatment of Suspects under the Cameroonian Criminal Procedure Code and Extra-National Laws: Human Rights Digest*." National Journal of Criminal Law. 2(1)*: 2019, pp. 4-12.
- NUREDINI Ahmet, "Challenges in Combating the Cyber Crime*", Mediterranean Journal of Social Sciences* MCSER Publishing, Rome-Italy Vol. 5 No. 19, 2014, pp. 592-598.
- SA'DI M. Mustapa, Kamarudin, A. R., Mohamed, D., & RAMLEE Z. Saad "Authentication of electronic evidence in cybercrime cases based on Malaysian laws". *Pertanika Journal of Social Science and Humanities,* 23 October, 2015, pp. 153-168.
- SKORUPKA Jerzy, "The rule of admissibility of evidence in the criminal process of continental Europe." *Revista Brazileira de Direito Processual Penal, Porto Alegre,* vol. 7, n°1. 2021, pp. 93-122.

- SURETTE Ray, "How Social media is Changing the way people commit crimes and police Fight them" Crime, media, culture: *International Journal, USAPP United States politics and Policy,* 2016.
- TANTOH E. Yata and NJI E. Bafuke, "Social Media and Cybercrimes: An Appraisal of Prosecution in Cameroon", *Revue Internationale de Droit et Science Politique (R.I.D.S.P),* Vol.1, No 3, 2021, pp. 857-885.
- WINMILL B. Lynn, METCALF L. David, BAND E. Michael, "Cybercrime: Issues and Challenges in the United States", *Digital Evidence and Electronic Signature Law Review*, Vol 7, 2010, p. 27.
- YONGU Zeng and BUIL-GIL David, Organizational and Organized Cybercrimes. In PONTEL H. (ed), *Oxford Research Encyclopedia of Criminology and Criminal Justice,* New York and Oxford, Oxford University Press, 2023.