OPEN ACCESS

Scholars International Journal of Law, Crime and Justice
Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) | ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Review Article

Transnational Challenges to the Prosecution of Cyber-Crimes in Cameroon: A Legal Analysis

Joseph Ule Ule[1*]

[1]Ph.D. Research Scholar in Law, Faculty of Law and Political Sciences, University of Dschang, Dschang, Cameroon

DOI: 10.36348/sijlcj.2024.v07i07.004 | **Received:** 14.06.2024 | **Accepted:** 20.07.2024 | **Published:** 27.07.2024

***Corresponding author:** Joseph Ule Ule
Ph.D. Research Scholar in Law, Faculty of Law and Political Sciences, University of Dschang, Dschang, Cameroon

Abstract

In this era of computer technology, computer-related crime as well as cybercrime has become a substantial worldwide threat. The computer has empowered cybercriminals to attack their victims in any part of the world. Transnational crimes are very challenging to track, and more often than not, the offenders are hardly apprehended. Thus, the entire community requires a vigorous and an inclusive effort to identify invaders, preserve evidence, and prosecute those guilty, irrespective of where they are located. This Article contends that irrespective of Cameroon's relevant laws and regulations against cybercrimes in place, coupled with the various bilateral and multilateral conventions duly ratified the challenges of cybercrimes remains pigheaded and mystifying. This Article intends to analyze the reasons for the rise in cybercrime, the laws in place and the challenges in its prosecution. Through a content analysis of primary and secondary data, we therefore, opine that, proper sensitization needs to be done to avert the spirit of cybercrimes in the cyber space.

Keywords: Transnational, Cyber, Challenges, Cybercrimes, Prosecution, Economic Losses, Cameroon.

Copyright © 2024 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

INTRODUCTION

The advent of globalization coupled with the rapid advancement in Information and Communication technology has enabled economic and social growth in Cameroon and the world at large, especially with an increasing dependence on Internet and computers for most of our daily transactions. Cybercrime is one of the embryonic forms of transnational crime. The inherent cross-border nature of this new type of crime is one that takes place in the borderless dominion of cyberspace. This dynamics has equally contributed to the rise of a new class of actors who operate outside the traditional nation-state system, thus making detection, intervention, prevention, investigation and prosecution very challenging. And have thus created an irritating situation with severe implications on the socio-economic, political and psychological wellbeing of countries of the world. Consequently, it is for this reason that many states have paid close attention to cyber security threats and the need to mount an urgent, dynamic, and international response across their national borders [1].

The cyber threats in the world and Cameroon in particular often manifest itself in the form of cybercrime as well as computer crime, though interchangeably used to mean the same thing, whereas they are not. According to McGuire and Dowling, Cyber-crime is an umbrella term used to designate two distinct, but closely related criminal activities: that is, cyber dependent and cyber-enabled crimes. To the authors, cyber dependent crimes notably; the spread of viruses and other malicious software, and the distributed denial of service attacks, are mainly offences which are only committed by using a computer, computer networks, or other form of Information Communication Technology although there may be inferior outcomes from the attacks, such as fraud [2]. While cyber-enabled crimes are the usual crimes that are increased in their scale or reach by the use of computers, computer networks or other Information Communication Technology like fraud includes; mass-marketing frauds, 'phishing' e-mails and other scams; online banking and e-commerce frauds; theft like; theft of personal information and identification-related data; and sexual offences against children like; grooming

[1]Aluede, J.A (2017). Nigeria's Foreign Policy and Trans-Border Crime: a Historical Analysis of the Nigeria-Benin Border, 1960-2013. A Thesis Submitted to University of Lagos School of Postgraduate Studies Phd Thesis, 428p.

[2]McGuire M, Dowling S (2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom, October. 30p.

(training), and the possession, creation and or distribution of sexual images [3].

On the other hand, Computer crimes, are committed against the computer hardware, the materials contained or associated with the computer notably; the software and data; typical examples of computer crimes includes but not limited to embezzlement, fraud, financial scams and hacking just to name a few.

According to Alison Peters, and Amy Jordan [4], most cybercrime acts are transnational. In 2017, the cost of transnational attacks across the world amounted to $600 billion, equivalent to 0.8 percent of global GDP. Cybercrime could cost the private sector a whopping $5.2 trillion by 2022. Transnational attacks frequently result in victims being outside the legal jurisdiction of the attackers [5]. Cyber security Ventures, holds that cybercrime, was said to have cost the global community $6 trillion per year by 2021, up from $3 trillion in 2015, signifying the largest transfer of economic wealth in history and more profitable than the worldwide trade in all major illegal narcotics combined [6].

More than half of all cybercrime investigations involve cross-border requests to access various kinds of evidence. This evidence is needed to attribute guilt for the attacks, for both prosecution and the defense case [7].

Cameroon has not been spared by this negative trend of cybercrime whose pessimistic effect over the years have been enormous and devastating in terms of its impact on the national economy, security and the livelihood of its people. The Minister of Post and Tele-Communication [8], intimated that interferences into computers systems cost the public and private administrations at least 2.5-billion CFA each year. Cameroon lost no fewer than 12.2-billion CFA to cybercrime in 2021, double the amount lost in 2019 [9]. This she said is;

> *"Due to the complexity of telecommunication links and ICT infrastructures, cyber threats are also becoming increasingly complex and jeopardising national security, the economy, social cohesion, democracy, health, culture and our different ways of life"* [10].

The National Agency for Information and Communication Technologies (ANTIC) on its part reported that over 90% of software and operating systems used in Cameroon are hacked including email addresses and social media accounts of businesses, individuals, and government members resulting in lamentable losses for operators, individuals, businesses and the state [11].

Grappled with the above threats, the Government of Cameroon called on stakeholders to unite in their response and thus enacted Law N° 2010/012 of 21 December 2010 relating to Cyber Security and Cyber Criminality, alongside institutions relating to fight against Cyber Criminality [12] and periodically trained personnel's to combat cybercrime in the country [13]. It is against this scenery, that this article seeks to briefly examine some of the facilitating features of cyber-crime; Legislations and the institutions regulating as well as the challenges encountered in its prosecution in Cameroon.

REASONS FOR THE RISE OF CYBERCRIME IN CAMEROON

Apart from the usual facilitating features such as unemployment; quest for wealth by youth's incompetent security and control on a personal computer, there are some other factor advanced for the rise cybercrime which includes;

[3] Ibid

[4] Alison P., and Amy Jordan; (2019) Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime e Journal of National Security Law and Policy [Vol. 10:487; pp. 487-524

[5] Tom Olzak (2021); Why Transnational Cooperation Is Key in the Battle Against Cross-Border Cybercrime Cyber security Researcher, Author & Educator

[6] In their analysis titled "2017 Crime Report," Cyber security Ventures, the world's premier researcher and publisher covering the global cyber market, recognized cyber-attacks as the fastest rising crime in the United States, adding that their scale, sophistication, and cost are all increasing. Cited from Akeem O. A. & Akora L., (2022) Trends, Patterns and Consequences of Cybercrime in Nigeria Gusau International Journal of Management and Social Sciences, Federal University, Gusau, Vol.5 , No. 1, April, 2022. Available at: https://gijmss.com.ng/index.php/gijmss/article/download/107/89, visited on the 14/05/2023

[7] Jennifer Daskal and DeBrae Kennedy-Mayo, Budapest Convention: what is it and how is it being updated articleOpens a new window; July 2020.

[8] *Libom Li Likeng, Minister of Post and Tele-Communication Cameroon* during the second edition of the National Forum on Cyber security and the Fight against Cybercrime held in October 2022. Available at https://itweb.africa/amp/content/KA3Ww7dzzELqrydZ (visited on the 03/04/2023)

[9] Statistics of the National Agency for Information and Communication Technologies (ANTIC); during the second edition of the National Forum on Cyber security and the Fight against Cybercrime held in October 2022. Available at https://itweb.africa/amp/content/KA3Ww7dzzELqrydZ (visited on the 03/04/2023)

[10] Ibid

[11] Ibid

[12] Hereinafter referred to as Cyber law.

[13] Ibid

The lack of awareness and education about cyber security; many individuals and organizations do not possess the necessary knowledge to identify potential threats or take appropriate preventive measures. This however, makes them easy targets for cybercriminals.

Cybercrime is still evolving, and it faces significant challenges in keeping up with the ever-evolving tactics of cybercriminals. Insufficient investment in cyber security measures, outdated systems, and a lack of coordination between government agencies and private organizations have left critical gaps that cybercriminals can exploit.

Besides, the digital transformation wave in Cameroon has led to a boom in e-commerce, online banking, and digital transactions. While this has made life more convenient, it has also opened up new avenues for cybercriminals to exploit vulnerabilities in online platforms, steal personal information, and carry out financial frauds.

Finally, Cameroon has witnessed a significant surge in internet penetration over the past decade. With more people gaining access to the internet, the potential victim pool for cybercriminals has expanded exponentially. Lack of awareness and inadequate cyber security measures make individuals and organizations vulnerable to cyber-attacks.

CYBERCRIMES LEGISLATIONS AND INSTITUTIONS IN CAMEROON

The main legislative text criminalizing cyber offences in Cameroon is Law N° 2010/012 of 21 December 2010 on cyber security and cybercrime in Cameroon, herein referred to as the 2010 Cyber Law. It is worth noting that this specific cybercrime and cyber security legislation includes; criminal substantive rules, procedural rules as well as provisions on international cooperation. By virtue of Law N° 2022/002 of April 27 2022, the President of the Republic of Cameroon was authorized to proceed with Cameroon's accession to the Budapest Convention on Cybercrime. Decree N° 2022/169 of May 23 2022 then proclaimed accession to the Budapest Convention. This proclamation is without prejudice to the completion of the necessary procedures for accession set out under the Budapest Convention [14]. There is no specific data protection or privacy law in Cameroon. Nonetheless, the preamble of the 1996 Constitution [15] guarantees privacy of communications.

Worthy of note is the fact that the 2010 Cyber Law protects "protect basic human rights, in particular the right to human dignity, honour and respect of privacy, as well as the legitimate interests of corporate bodies" [16]. These rights are equally enshrined in the preamble of the 1996 Constitution, which has thus affirmed our attachment to the fundamental freedoms treasured in the Universal Declaration of Human Rights 1948, the Charter of the United Nations and The African Charter on Human and Peoples' Rights 1966, and all duly ratified international conventions relating thereto.

The criminalization of cyber offences are provided for in sections 60-89 of the 2010 cyber Law, notably; unlawful interception [17], illegal access [18] system interference [19], misuse of device [20], data interference [21], computer-related fraud [22], Offences related to child pornography and grooming are also punished under sections 76, 80, 81, and 83 respectively.

Apart from the general procedure in criminal matters meted out by the Criminal Procedure Code [23], Specific procedural measures are recognized under Sections 52 to 59 of the 2010 Cyber Law. These provisions give the law enforcement and judicial authorities the competence to investigate and prosecute cybercrime offences. According to article 49, the Judicial Police officers may intercept and record electronic data, they may also search and seize computer data [24] as well as on the use of electronic communications for the hearing of any person in criminal proceedings [25], although no details are given on the type of data concerned. Besides, the 2010 Cyber Law, there are a series of other laws and regulations which are helpful in the fight against Cybercrime, for instance, laws on electronic communications in Cameroon [26]; Banking Secrecy [27] and Decrees on the modalities of the protection of consumers of services of electronic communications [28]; and to set-up of a universal service and the development of electronic communications [29], Just to name a few.

[14] Article 37 of the Budapest Convention
[15] Law N° 96/06 of 18 January 1996 on the Cameroon Constitution as revised in 2008.
[16] Article 1 Ibid, added to this is Sections 41-48 which covers 'Protection of privacy'
[17] Section 65 (1), Ibid
[18] Section 65 (2), Ibid
[19] Sections 66 (1) and 67,
[20] Section 66 (2), section 86 (1),
[21] Sections71 and 72, 86 (2),
[22] Section 73 (1),
[23] Law N° 2005/007 of 27 July 2005 establishing the Criminal Procedure Code.
[24] Section 53 et seq 2010 Cyber Law
[25] Article 59 of the 2010 Cyber law
[26] Law N° 2010/013 of 21 December 2010 on electronic communications in Cameroon and its amendment of April 2015
[27] Law No 2003/004 of 21 April 2003 on Banking Secrecy
[28] Decree n° 2013/0399/pm of 27 February 2013 on the modalities of the protection of consumers of services of electronic communications;
[29] Decree n ° 2013/0398/pm of 27 February 2013 on the setting-up of a universal service and the development of electronic communications;

Cameroon being a member of the CEMAC the following legislations is also applicable notably: Regulation No. 21/08-UEAC-13-CM-18 of 19 December 2008 on the Harmonization of Regulations and Regulatory Policies on Electronic Communications in CEMAC Member States [30]. Directive No. 07/08-UEAC-133-CM-18 of 19 December 2008 on the Legal Framework for the Protection of Users of Electronic Communications Networks and Services within CEMAC; Directive No. 09/08-UEAC-133-CM-18 of 19 December 2008 Harmonizing the Legal Frameworks of Electronic Communications in the CEMAC Member States.

Specialized investigative institutions

Ministry of Posts and Telecommunications has created a ministerial division charged specially with the tasked to investigate cybercrimes. In addition, a Networks and Information Systems Security Department includes among its responsibilities "popularizing protective measures for the populations against cybernetic criminal acts" and "centralizing statistical data in the domain of cyber security and cybercrime".

The National Agency for Information and Communication Technologies (ANTIC) serves as the main institution established in Cameroon for the regulations and enforcement of cyber security [31].

Hence, in 2011, ANTIC became a member of the ITU-IMPACT, an international multilateral partnership against cyber threats that offers high-level training programmes to help partner countries to fight and prevent the scourge. In accordance with the law mentioned above and the Cameroon Cyber wellness Profile [32]. ANTIC has varied functions ranging from the regulation, control, monitoring of activities related to electronic security [33] detection and provision of information on computer risks and cybercrime activities and carries out criminal investigations in collaboration with the Telecommunications Regulatory Board and judicial police officers [34]. Most importantly, it regulates the internet thus becoming a key agent in the restriction of certain activities carryout on the internet [35]. It is responsible for the regulation, control and monitoring of activities related to security of electronic communication networks, information systems, and electronic certification on behalf of the State [36]. ANTIC is working with civil society organizations, NGOs, and academic institutions in order to educate the population and raise awareness in an effort to mitigate cyber risks.

The Telecom activities are regulated since 1998 by the Telecommunications Regulatory Authority (Agence de Régulation des Télécommunications), The National Cyber Expertise Centre opened in July 2015 to carry out research and train experts to develop cyber security protection measures, fight cyber criminality and thwart cyber terrorist threats.

In a generalized context of expansion of new information technologies, the Delegate General for National Security, by Service Note No. 47/DGSN/SG/ DPJ of 23 March 2018, created the Special Unit for the Fight against Cybercrime (USLUCC) within the Judicial Police Directorate. This Unit was made operational as soon as it was created. Its staff is made up of highly qualified and experienced police officers.

International cooperation

Being an evolving transnational crime, international cooperation in the prosecution of cybercrime is primordial and it is governed by Articles 90-94 of the 2010 Cybercrime Law. Cameroon is a Party to the United Nations Convention against Transnational Organized Crime (ratified on 6 February 2006), and United Nation Convention against Corruption (UNCAC) which encompasses provisions on international cooperation.

The Economic Community of Central African States (ECCAS) on its part has established an Agreement on judicial cooperation (adopted on 28 January 2004), as well as several bilateral agreements (e.g. with France, adopted on 21 February 1974).

When it comes to Law Enforcement Cameroon is a member of INTERPOL, CEMAC Criminal Police Cooperation Agreement as well as the Central African Police Chief Committee. The Cameroonian Criminal Procedural Code regulates Extradition in its Articles 635-675.

CHALLENGES TO THE PROSECUTION OF CYBERCRIME IN CAMEROON

The cybercrime challenges include; identity of criminal, impersonation or identity theft, jurisdictional challenges just to name a few; will be seen below.

[30] known as 'the Regulation on Harmonisation in CEMAC Member States';
[31] Law No. 2010/012 of 21 December 2010 relating to cyber security and cyber criminality in Cameroon
[32] United Nations Statistics Division, December 2012 Cited from Boraine A., Ngaundje L. D., 'the fight against cybercrime in Cameroon' International Journal of Computer (IJC) Global Society of Scientific Research and Researchers Available at http://ijcjournal.org/ (Visited o the 05/04/2023)
[33] Section 7(1), Cyber Law.
[34] Ibid.
[35] Decree No. 2012/180/PR of 10th April 2012.
[36] Section 7 of Law No. 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon.

Identity of cybercriminals

One of the greatest impediments against Cameroon's efforts to curb the ill of cybercrimes remains the anonymous nature of cybercriminal's identity. It is not easy identifying who is doing what and where is a user of the Internet situated at any point in time; the global information system is free and there is no condition that needs to be fulfilled, before a user login to connect with anywhere and anyone across the globe [37]. Thus, the freedom of information and communication enables the cybercriminals to hide their identity using different telecommunications devices so as to make it impossible to trace the online Internet Protocol (IP) address of any user. More so, if the IP address of a cybercriminal were traced to a particular location, the next hurdle cannot be scaled as the identity of a cybercriminal is undisclosed to the owner or operator of Internet service provider. Added to this, the identity of Internet users and communication are often routed through verious telecommunications devices such as Psiphon or the Onion Router (Tor) just to name a few and are used to shield through many servers which further compounds the possibility of cybercriminals being traced. From the above it will be a complete waste for the enacted laws if the identities of a cybercriminal cannot be traced.

However, some efforts have been made, to obligatorily make identification a prerequisite in the use of internet but this was ruthlessly opposed by defenders of human rights on grounds that it infringes on privacy rights, thus continuing to operate unperturbed by making the laws in place a toothless bull dog.

Impersonation or identity theft

This is another main practice engaged by cybercriminals to compound evidence in cyberspace. This is intentionally done to sway and steer off investigation as to the real identity of cybercriminals, more often than not; innocent citizens in Cameroon are arrested and prosecuted for offences they know nothing about. In other words, digital technologies provide ample opportunities for impersonation by way of identity disguise so as make it difficult if not impossible to ascertain who is behind the said cybercrimes. The nature of cyber evidence is difficult to gather, since it is the said evidence is delicate and vulnerable to manipulation and destruction and thus requires an expensive forensic process.

Lack of expertise among investigating officers

The complex nature of cybercrimes requires expert knowledge in the recovery and interpretation of digital evidence, but most investigating officers do not have the skills needed to do so. Cameroon has very few forensic centers' in existence and the question that has continuously begs for an answer is how can evidence be presented to secure a conviction? Although the CPC [38] talks of proof is by any means, Electronic evidence are very difficult to assemble and vague to obtain evidence of a cybercrime. This difficulty arises from the use of sophisticated programs in their computers and passwords by culprits that only experts can decode. The sophisticated nature of the programs makes it easy for culprits to automatically destroy or delete evidence within a few seconds when assessed by anyone, especially the forces of law and order. The complex nature of cybercrimes and the difficulty in proving them should not be an excuse for resorting to illegal short cuts to secure a conviction. The non-observance of certain technicalities imposed by the law for the investigation and prosecution as a result of the wide nature of cyber space and discrete nature of cybercrimes make it very difficult to identify or locate a culprit, and thus to obtain evidence will always exonerate defaulters [39].

Jurisdictional challenges

There is no coherent and comprehensive set of transnational rules on trans-border criminal justice to coordinate competing jurisdictional claims. This lacuna can be explained by the fact that the purview of criminal justice has traditionally been limited to the territory of each state, thus the successful investigation or prosecution of trans-border cases are often hindered by the issue of sovereignty. Protecting sovereignty is a primary concern for national governments, often resulting in hesitancy when it comes to cooperating with other States [40].

Although, most states notably the Western countries, have begun to claim that certain rules may be apply universally; at the same time, and have set up rules governing trans-border criminal cases and have started to investigate and prosecute crime transnationally, notably; trafficking in human beings, trans-border bribery, and money laundering. In order to facilitate the transnational prosecution of these and other crimes, these states have established institutions such as UNODC and Europol, have established mechanisms for sharing information [41], and have even granted authority to perform acts of

[37] Ajayi E.F.G., (2015). The Challenges to Enforcement of Cybercrimes Laws and Policy; International Journal of Information Security and Cybercrime, 4(2):33-48. Available at: http://www.ijisc.com/year-2015-issue-2-article-4/ (visited on 12/05/2023)

[38] Sections 308 and 336 of the CPC

[39] *The People of Cameroon v Tamukum Fonjiyang Ferdinand and Song Charles Waindim*, CFIB/015f/2012 unreported.

[40] Stefano, B., New prospects for inter-state cooperation in criminal matters: The Palermo Convention.‖. International Criminal Law Review (2003) Vol. 3: 151-167. P. 155.

[41] For instance, ICAT Inter-Agency Coordination Group Against Trafficking in Persons.

© 2024 | Published by Scholars Middle East Publishers, Dubai, United Arab Emirates

investigation on their territory to agents of other states. But the jurisdiction to adjudicate is 'even today' still largely limited to the national state. In spite of the fact that the reality of investigations and prosecutions has changed, binding general rules on transnational investigations and prosecutions are still lacking.

This state of affair is explained by the fact that, transnational criminal law is generally not yet part of the curricula of institutions; specific knowledge to solve problems of investigations and prosecutions of criminal cases affecting more than one jurisdiction has often not been part of traditional training. These rules are still difficult to access and apply, especially for a lawyer not familiar with the cross-border dimension of criminal justice [42].

Therefore, it is necessary to find and communicate transnational soft (and hard) rules, aiming at coordinating the transnational case where it has contact points with different jurisdictions. From an academic perspective, the perception has been similar for a long time. A transnational body of general principles for transnational criminal matters has not been developed because scholars basically regarded criminal cases affecting more than one jurisdiction not as a transnational topic, but at most as a set of separate criminal cases scattered across national jurisdictions.

In other words, the transnational case of one individual who committed an act that affected two or more jurisdictions is split up among all the jurisdictions that are involved. The transnational case often ends up being prosecuted as a number of national cases involving extraterritorial conduct. Each of these national cases is subject to a self-contained set of rules that derive from the respective national and international legal frameworks.

The suspect's special status may at times limit jurisdiction. Most states recognize the concept that diplomatic or foreign officials under sovereign immunity cannot be prosecuted [43]. Most states also recognize the diplomatic immunity that shields diplomats and their families from most arrests and prosecutions [44]. Based on inter-governmental organizations, some states recognize this immunity for people who work and engage as peacekeepers in human trafficking for the United Nations [45]. In case of a minor offense for instance, the non-respect of parking regulations committed by a Head of State or a diplomat while they are on official duty, they will be immune from such prosecution.

Besides the above, another compelling challenge is the enforcement of cybercrime laws jurisdiction. Taking into consideration the principles of state independence, sovereignty and territorial integrity, each nation-state of the world, have the authority to make laws binding on things and all persons within its geographical entity (state). Thus making laws on the same matter from different jurisdictions, conflict of laws is inevitable. Jurisdiction may be defined as the power of a court or judge to entertain an action, petition or proceedings as was in the case of *Alade V. Alemuloke* [46].

The issue of jurisdiction is so radical that it forms the basis of any adjudication, stated otherwise; it goes into the roots of any matter before the courts. If a court lacks jurisdiction, it also lacks necessary competence to try the case. A defect in competence is fatal, for the proceedings are null and void *ab initio*. A defect in competence is extrinsic to adjudication. The court must first of all be competent, that is, possess jurisdiction before it can go ahead on any adjudication, *Oloba V. Akereja* [47] and *Madukolu & Ors. V. Mkemdilim* [48].

Given how fundamental the issue of jurisdiction is at law, and bearing in mind its radical nature, it has been asserted to the effect that, there is no technical word in the whole of conflict of laws that is more variously used and abused than jurisdiction. It is a word with too many meanings and all that can be done about it is to ascertain the sense in which it is being used at any given time [49].

Nonetheless, the concern of jurisdiction with respect to enforcement of cybercrime laws basically revolves around two issues, namely, geographical jurisdiction and jurisdiction in personam [50]. Geographical jurisdiction addresses the fundamental issue as to if a court have the power beyond the territory where it is situated, while jurisdiction in personam deals with whether a court is empowered to hear and determine a case of a cybercriminal not within its jurisdiction.

[42] Difficulties arise from the various layers of international and national law as well as from unclear relationships between the various legal frameworks, see for instance, W. Schomburg et al. (eds.), Internationale rechtshilfe in Strafsachen, 2006, Einleitung N 2 et seq.
[43] N.BOISTER, *supra*, at pp.273-75.
[44] *Ibid pp.* 275-77.
[45] Ibid p. 276.
[46] (1988) 1 N. W. L. R. (pt. 69) 207
[47] (1988) 1 N. W. L. R. pt. 84 at 587
[48] (1962) 1 All N. L. R. 587
[49] Leflar: Jurisdiction and Conflict of Laws P. 223 cited from: Ajayi EFG (2015). The Challenges to Enforcement of Cybercrimes Laws and Policy. International Journal of Information Security and Cybercrime, 4(2): pp. 33-48. Retrieved from: http://www.ijisc.com/year-2015-issue-2-article-4/ (Accessed on the 20/11/2021)
[50] Latin "against a person" opposite of in rem "against a thing" for example, property

© 2024 | Published by Scholars Middle East Publishers, Dubai, United Arab Emirates

With the peculiarity of the nature of cybercrime, it is in a class of its own, it is unique and distinct in character unlike traditional terrestrial crimes, which are committed in a particular locus and whereof, the effect(s) are felt by the victim(s); stated in another way, cybercrimes transcends states and jurisdictions; they are cross border or transnational crimes. Thus, a cybercriminal may sit in the comfort of his home, office, café or wherever he chooses, with a desktop, laptop, tablet or phone connected to the Internet and carry out his illegal activities that would be felt thousands of kilometers away, from where the act(s) took place.

The pervasiveness of cybercrime has been aptly expressed as "the ubiquity of information in modern communication systems makes it irrelevant as to where perpetrators and victims of crimes are situated in terms of geography. There is no need for the perpetrator or the victim of a crime to move or to meet in person. Unlawful actions such as computer manipulations in one country can have direct, immediate effects in the computer systems of another country...." [51].

To sum up jurisdictional challenge to enforcement most especially with cybercrime laws, means if the hurdle of anonymity is scaled and a cybercriminal is clearly identified but he is situate in another country aside from where the victim is domiciled, the court of the forum cannot effectively try such a criminal as the court lacks jurisdiction geographically and also *in rem;* a discerning mind would immediately jump at extradition of the criminal as a solution, but this process, that is, extradition is fraught with its own challenges aside from double criminality requirement [52], especially where there is not in existence extradition treaty or mutual legal assistance treaty between the requesting state and the state having custody of the criminal.

Conflicts of jurisdiction are a greater risk in cybercrime cases because of the phenomena of loss of data and loss of location. Cloud computing, anonymisation tools and the dark web have led to loss of location issues, where authorities cannot reasonably establish the physical location of the perpetrator, the criminal infrastructure or the electronic evidence. In these situations, it is often unclear which country has jurisdiction and what legal framework regulates the collection of evidence or the use of special investigative powers. In relation to cloud computing, not even the industry knows where its data are stored at any given moment, as the jurisdiction in question can change instantly as a result of the automatic load balancing of internet-based services.

The challenge to the collection of digital evidence

It is settled and far beyond controversy that in criminal prosecution, it is incumbent on the prosecution to prove his case beyond reasonable doubt before a conviction can be secured against an accused; thus the nature of fact or documentary proof adduced as evidence in the prosecution of cybercriminals goes to the root of any trial; unfortunately, evidence available to prosecutors may be defined as unstable, and thus frustrated all efforts to bring cyber criminals to justice.

Unlike cases were the accused is present and very willing to testify in court, this form of physical evidence is rare in cybercrime prosecution; all what the investigators and prosecution can have and rely on, are mere footprints on the computers used by the criminals and traces left on the Internet; the nature of these proofs have little evidential value and same is hardly convincing to courts seized of such criminal trials [53]; since the nature of evidence in cyber prosecution is basically digital. The challenge of digital invention of electronics in cyberspace is overwhelming in view of evidential nature being a representation of sound or light waves as number by means discrete signals interpreted as numbers, usually in the binary system; this peculiar nature of evidence arising from digitalization is delicate in character and makes it vulnerable to damage whether intentional or otherwise, ditto manipulations, which naturally would render such evidence to be of little or no value and thus inadmissible by the courts [54].

What is being emphasized as to nature of digital evidence is that, generally, they are delicate so much that mere examination by inexperienced investigator(s) may contaminate or out rightly damage such evidence and of course if that happens, experts in data recovery would have to be called in to carry out repairs which is not cheap.

Added to above is the tendency of willful destruction of evidence by cybercriminals so as to escape justice, in other words, when evidence that could provide solving of a crime in the cyberspace is destroyed, inexperienced investigators usually would have little or

[51] Sieber U., (1997). Memorandum on a European Model Penal Code. P. 2. United Nations Office On Drugs And Crime (2014). United Nations Convention Against Corruption. Retrieve from: https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf. (Accessed on the 20/11/2021)

[52] Principle that the offence for which an accused is sought to be extradited must be a criminal offence at the state making a request and also at the state where the accused is domiciled.

[53] Ajayi, E.F.G (2015). The Challenges to Enforcement of Cybercrimes Laws and Policy. International Journal of Information Security and Cybercrime, 4(2):33-48. Available at: http://www.ijisc.com/year-2015-issue-2-article-4/ (visited on 112/052023)

[54] Case of the *People of Cameroon v Tamukum Fonjiyang Ferdinand and Song Charles Waindim, Supra*

no clue to follow in the arrest and prosecution of such crime(s).

Shortcomings of the of 2010 Cyber Law

Cyber law has not adequately deterred scammers from committing crimes because the sanctions are less severe. The maximum imprisonment term meted out on scammers is ten years making scamming which is a serious offence a misdemeanour rather than a felony [55]. Also, the fine to be paid is greater, but it is an irony because scamming is a lucrative crime wherein scammers make much money, so paying a heavy fine will not have much effect on the culprit. This of course makes them very comfortable in committing further crimes. With this, one can adequately describe the Law as being a window dressing and can be circumvented. Scamming is a worldwide crime which requires international cooperation through ratification of many international instruments dealing with cyber criminality, but Cameroon has recently ratified many of such instruments [56]. This constitutes a big challenge making it practically difficult to combat cyber-crimes in Cameroon and across. In Cameroon today, it is revealed that more than 60% of the population have access to the internet [57], so are aware of the Law and cyber criminality, but still fall victims to scammers (limited knowledge of users). This is because most users of either the telephone or internet are not yet versed with some tactics used by scammers to perpetrate their acts. In a country where the opportunity to educate the entire population on cyber criminality and the tactics used by scammers does not usually present itself, it is easier for many scammers to steal from their victims and even receive money for goods sold without actually receiving the goods as was in the case of the *People of Cameroon v Tamukum Fonjiyang Ferdinand and Song Charles Waindim* [58]. Although we have a good law, the majority of the people are not aware of the existence of the law. Those who know of the law and cannot access it. The repetition of sections and improper connotations of terms makes it difficult for the people to understand.

Lack of effective reporting

By their nature, it is difficult for ordinary people to report cybercrime due to the technical skills they require that are only open to professional or specialized groups in the field of computer and information technology systems, cybercrimes remains concealed until its news reaches the competent authorities. Irrespective of the applicable law and policy against cybercrime, the prosecution is very challenging. In effect, this development has work against bringing to global attention the impact of the threat of cybercrimes; the reluctance to disclose cybercrimes is as a result of lack of cooperation on the part of the victims, other stake holders and witnesses with police or other agencies saddled with investigation and prosecution of cybercriminals, it is immaterial whether private, corporate or institutional entities are the victims [59].

In Cameroon, it is on very real situations that cybercrime cases are brought before the legal Department, more often than not, even when the cyber criminals are arrested with substantial evidence to secure a conviction, the law enforcement officers in charge of investigation are usually bought over by the said criminals. Most of the cases that come to court are those who have probably refused to share their booty with the officers in charge.

Several other reasons have been advanced for the reluctance to report cybercrimes and these includes but not limited to costs arising from follow up of cybercrimes which more often than not far outweigh the benefit derived thereof, the damage to the reputation and goodwill of victims especially corporate entities which are going concerns, of course, the protracted investigation and prosecution which are generally considered as effort and time wasting exercises, more importantly, the difficulty of diligent investigation which is usually rushed when a particular cybercrime investigation and prosecution traverses many jurisdictions thereby bringing to the fore issues in approach to cybercrimes [60].

This situation is thus supported by Ernst and Young [61] following an empirical evidence of a survey carried out. According to authors, they found out that only one quarter (1/4) 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. More so, for businesses that are in a competitive environment, reporting of cyber incursion is viewed as exposing the weakness or vulnerability of systems, which will thus wear down the clienteles confidence and may provoke consumer turn-away, thus the owners and operators would rather keep silent and try

[55] Section 73 (1), Cyber Law.
[56] The Budapest Convention of 23rd November 2001.
[57] Available at <www.antic.com> (Visited on the 29/011/2022)
[58] CFIB/015f/2012 unreported
[59] Ajayi, E.F.G (2015); 'the Challenges to Enforcement of Cybercrimes Laws and Policy', International Journal of Information Security and Cybercrime, 4(2):33-48. Available at: http://www.ijisc.com/year-2015-issue-2-article-4/ (visited on 12/052023)
[60] Ibid
[61] Enest, Young (2003). Fraud: Unmanaged risk. 8th global survey. Global investigations dispute advisory services, South Africa. Available at: https://www.whistleblowing.com.au/information/documents/EY8thGlobalSurvey2003.pd (visited on the on the 12/05/2023)

© 2024 | Published by Scholars Middle East Publishers, Dubai, United Arab Emirates

as much as possible to rectify the system than report to authorities in charge of cybercrimes [62].

Cost, time and efforts incurred in investigation and prosecution

The nature of evidence needed is forensic evidence in the prosecution of cybercrimes. As a scientific crime, it need a scientific solving approach as opposed to gathering of evidence in terrestrial crimes, which is not particularly cheap because of its high level of technological equipment, materials and expertise involved to carry out such investigations [63].

With specific reference to business and social interaction, the advent of technology has two divided outputs, one side represents the numerous advantages which are manifested in the speed and accuracy of information and communications to man wherever he is situate and which development has aptly described the world as one global village [64], on the other hand, is the rise in cybercrimes; and whenever these crimes occurred it thus presents a heavy burden to investigators and other law enforcement authorities to unravel, given the mass of information that needs scientific examination by passing through numerous files and breaking encrypted codes, thus passing through all this that would possibly lead to arrest and prosecution of cybercriminals at excessive costs aside time and efforts of experts which should have been usefully used in other ventures [65]. These cybercriminals are indifferent to the losses experienced by their victims as long as they obtain financial gains. This is why cybercrimes can lead to significant losses for the victims.

Barriers to Cooperation and Structural challenges

Despite the bilateral and multilateral cooperation instruments that Cameroon has adhered to, there are issues that hinder cooperation and effective prosecution. For instance, the Budapest Convention and other regional and multilateral treaties related to cybercrime lack any, sort of prosecution mechanism to ensure states adhere to its commitments. While some countries like Cameroon have acceded to the Budapest Convention, some have criticized the convention for being vague in some of its provisions that have allowed governments to skirt their obligations and of the concerns that its contents are outdated to deal with the evolving cybercrime threat, despite its defenders arguing that it is technology neutral [66].

Other regional instruments and policy documents, particularly with CEMAC, the problems of police cooperation are much more structural, that is to say linked to the police structures themselves. The police force of each State has its own nature, its own history, and therefore its own specificities. In each CEMAC member state, the police have their own administration and hierarchy. Notably; the Cameroonian police are organized within the General Delegation for National Security which is a service attached to the Presidency of the Republic, and is placed under the direct authority of the President of the Republic *"who is its supreme leader"* [67]. In Congo the police services come under the Ministry of the Interior and Decentralization, which is the same for other member states.

Furthermore, before cooperating at the community level, under the internal level, skills should already be well distributed between the various units making up the police services of each Member State. In Cameroon for example in addition to the National Central Office of INTRERPOL which is the vocation in essence [68], at least three other structures of the Cameroonian national police including the special operations group (GSO) [69] and the direction of the judicial police [70], intervene in intelligence. Added to this is an often very difficult coexistence between the different services contributing to maintaining order and repressing offenses like cyber criminality at the national level. Whether it is the police or the gendarmerie, or even customs, instead of operating in complementarities, we are settling into logic of competition, with everyone wanting to operate in self-sufficiency, refusing or forbidding any collaboration with the others [71].

[62] Ibid

[63] Ajayi, E.F.G (2015); *Op. cit p.*

[64] A term ascribed to McLuhan who described how the globe has been contracted into a village by electric technology and the instantaneous movement of information from every quarter to every point at the same time. See generally Marshall McLuhan, The Gutenberg Galaxy: The Making of Typographic Man (1962) and Understanding Media (1964). Cited from Ajayi, E.F.G (2015); The Challenges to Enforcement of Cybercrimes Laws and Policy. International Journal of Information Security and Cybercrime, 4(2):33-48. Available at: http://www.ijisc.com/year-2015-issue-2-article-4/ (visited on 112/052023)

[65] Ibid

[66] Jack Goldsmith, Cybersecurity Treaties: A Skeptical View, KORET-TAUBE TASK FORCE ON NAT'L SEC. & LAW, HOOVER INST. 3- 4 (Feb. 2011), https://perma.cc/F5LD-27C4 [hereinafter A Skeptical View].

[67] Article 2, décret n° 2012/540 du 19 Novembre 2012 portant organisation de la Délégation Générale à la Sureté Nationale.

[68] Article 23, décret n°2012/540 précité.

[69] Article 20, alinéa 1, troisièmement décret n° 2012-540 précité

[70] Article 118, alinéa 1, premièrement, décret n° 2012-540précité

[71] AYISSI AFANA (J. B.) , *la lutte contre le trafic illicite des stupéfiants au sein de l'OIPC-INTERPOL, le cas du BCN du Cameroun*, MASTER, Université Catholique d'Afrique Centrale, 2005, p. 91

Extradition

Cameroon does not have a general extradition law or MLA; she relies on the provision of the Criminal Procedure Code [72] on such issues. The only traditional legislation in this domain that clearly elaborates on these aspects is bilateral and multilateral agreements duly signed by Cameroon. There is equally no national legislation on MLA request when it comes to corporate bodies. Besides, the law does not really regulate special investigative techniques though Section 49 of the 2010 law on cyber criminality talks of electronic surveillance.

Basically, states would have no international obligation to extradite to one another unless a convention explicitly required otherwise [73]. As such, these treaties between governments would frequently be a type of bilateral agreement marked by reciprocity [74]. Both parties would need to extradite to the other by establishing the terms of extradition in the treaty [75]. If the State Parties to the UNTOC Convention did not have an extradition treaty between them, it would be held in force, but it would also be required to meet the internal conditions of each state, which would be different. Consequently, Cameroon could face circumstances in which the States Parties would not have an extradition treaty. Therefore, the UNTOC should set criteria for such situations and require the States Parties to submit to the listed instances without exception and attempt to minimize the use of legal discretion to consider extradition between them.

In the absence of bilateral treaties between the States Parties to the UNTOC Convention, the UNTOC Convention would continue to be regarded as the fundamental basis for extradition. There would be additional impediments to the submissions, such as the prohibition on extradition, observed according to the United Nations Model Treaty on Extradition [76]. Regarding the exclusion of extradition in cases of political offenses, if a person had committed a political offense, the political offense would not be subject to extradition [77]. Although it would be difficult to consider the criteria for establishing whether offenses were politically wrong because additional conditions could surround offenses claiming to be political in nature, they would be included in the same offense. Hence, defining which crimes would be political offenses would need to be as clear as how the court interpreted the extradition at the request of the requesting state. Such offenses would thus continue to form the primary impediment to the extradition. Therefore, the circumstances should be resolved by identifying the character or type of crime that would include a specific political offense.

In addition, there have been instances where arrests or extraditions have been made without the use of extradition laws. The visa was withdrawn, and the individual was deported because he/she was deemed as an arriving alien under the terms of immigration law. This instance precluded the court from investigating the capture or control, as those terms were specified in the extradition statute. This circumstance would be because immigration agencies would be regarded as having authority over the repatriation of the immigration laws. As a result, the legal immigration authorities could be returned outside Cameroon without submitting an extradition request. Thus, this would be deemed a gap in the enforcement of the law's extradition provisions. In this state of affairs, immigration authorities should be urged to behave appropriately under extradition principles by not avoiding enforcing the immigration regulations over which they have control.

Since cybercriminals operates through a network of countries, extradition might be complicated in cases involving more than one jurisdiction. In addition, the criteria of the extradition would need to be prioritized regarding how the extradition would be considered to avoid jeopardizing any international relations. Consequently, the court would be critical in evaluating whether an individual would be eligible for extradition on extradition grounds. As a result, courts should take an active role in fact-checking rather than relying on practice in typical situations [78].

Additionally, even efforts to reconcile and simplify procedures have not yielded very satisfactory

[72] Section 653-675 of the CPC

73 Amnesty International, *International Law Commission: The Obligation to Extradition or Prosecute (Aut Dedere Aut Judicare),* (2009), Retrieved from: https://www.amnesty.org/fr/wp-content/uploads/2021/07/ior400012009en.pdf (Accessed on the 22/5/2022)

[74] ROBERT O.KEOHANE, *Reciprocity in International Relations,* International Organization Vol. 40 No.1 (The MIT Press, Winter 1986) at 1-27, Retrieved from: https://www.jstor.org/stable/2706740 (Accessed on the 22/5/2022)

[75] United Nations, *Revised manuals on the Model Treaty on Extradition and the Model Treaty on Mutual Assistance in Criminal Matters,* E/CN.15/2004/CRP.11 (May 11, 2004), Part One, at n.12.

76 Article 14 of Report of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, U.N.Doc.A/CONF.144/28 (1990) at 64, as adopted by G.A. res. 45/116, annex, 45 U.N. GAOR Supp. (No. 49A) at 211-15, U.N. Doc. A/45/49 (1990), and subsequently amended by G.A. res. 52/88 [hereinafter Model Treaty on Extradition]

77 Prasit Piwattanapanich, (2010) *Extradition Exceptions,* (Junniti: January-February 2010) pp. 41-47

[78] Prasit Ekbutr. (2008). *Globalization and international criminal law* (Bangkok: Thammasat University Research and Consulting Institute: 2008) p. 185

results, and this may be for the same reasons. Otherwise how can we explain the non-ratification by all CEMAC States of the Judicial Cooperation Agreement, and the Extradition Agreement between CEMAC Member States [79], both adopted since January 28, 2004 and not yet entered into force. The gap that exists between the adoption and ratification or not of cooperation instruments [80] leave more to be desired on the real aspiration these States have to move forward in the direction of better cooperation. A similar challenge arose regarding the ratification of the Criminal Police Cooperation Agreement between the States of Central Africa before being resolved and now exempts from the ratification procedure all States in the Central African sub-region [81].

CONCLUSION

Cybercrime has continued to rise in scope in the world, thus creating new challenges just with the stroke of a keyboard. Cybercrime threats are borderless with a single cybercrime incident able to hit victims in numerous jurisdictions. The Cameroonian domestic laws on its own cannot effectively address the challenges of cybercrime, like; identity theft, conflict of jurisdiction and the collection of digital evidence, there is therefore, a need for international cooperation of laws and binding treaty agreements between countries (bilateral or multilateral) is timely due to the transnational nature of cyber-crime, since most countries have established treaty agreements in place while other countries are still struggling to adopt domestic Penal Law, however harmonization is necessary for both substantive and procedural laws [82]. The Cameroonian law, still need to reappraise and revise procedures for digital evidence, search and seizure, electronic spying, to cover digitized information in order to conform to modern computer and communication systems, and the global nature of the internet. Better coordination of procedural laws, therefore, would facilitate cooperation in investigations that cover multiple jurisdictions [83], for a better transnational prosecution in Cameroon.

The following recommendations were made;

The Law should provide clear meanings or definitions to key terminologies such as data, cybercrime and avoid repetition of sections and use of terms that are of no use, so as to avoid confusion. The duty of information and communication operators to conserve data for 10 years is repeated in various sections of the law, that is, sections 25, 35, 42 and 46. The repetition of these sections brings the law to 90 sections.

Cameroon's law needs to empower law enforcement officials with the necessary tools for carrying out modern investigations. In the case of more intrusive measures such as surveillance, conditions for further authorization of a competent authority must be regulated in a clear transparent manner and undertaken in accordance with law in order to be admissible in court such as the gathering of evidence.

Equally, the names of arrested co artists should be printed in a newspaper to deter others from committing such crimes. The premise here is that the fear of publicity will likely deter others from engaging in such activities.

[79] Le Tchad a ratifié les deux textes depuis 2006, le Cameroun l'a fait aussi par les décrets n°2006/048 et 049 du 30 Janvier 2006 portant ratification de l'accord d'extradition, et de l'accord de coopération judiciaire entre les Etats membres de la CEMAC

[80] NGAPA (T.), *La coopération judiciaire pénale dans la zone CEMAC*, Mémoire en vue de l'obtention du Diplôme d'Etudes Approfondies en droit communautaire et comparé CEMAC, Université de Dschang 2006, p.27.

[81] It was Resolved by the General Regulation No. 4 of the ICPO-INTERPOL

[82] Ani L., 'Cyber Crime and National Security: The Role of the Penal Code and Procedural Law' (2011) 2 Law and Security in Nigeria p. 222.

[83] Ibid