MAKERERE LAW JOURNAL SEPTEMBER 2023

Volume 52 Issue 5

PROCEDURAL ASPECTS OF CYBER CRIMES INVESTIGATIONS IN RWANDA: A COMPARATIVE STUDY

Kabano Jacques & Habarurema Jean Pierre

Recommended Citation: Kabano Jacques & Habarurema Jean Pierre (2023); "Procedural Aspects of Cyber Crimes Investigations in Rwanda: A Comparative Study" Volume 52 Issue 5 Makerere Law Journal pp. 240-266

PROCEDURAL ASPECTS OF CYBER CRIMES INVESTIGATIONS IN RWANDA: A COMPARATIVE STUDY

Kabano Jacques*
Habarurema Jean Pierre*

ABSTRACT

The use of internet technology has dramatically affected our ways of learning, communication and information sharing. The routine of daily use of social media makes it nearly impossible to conceive any illicit activity not having a cyber component. The multinational nature of Internet raises a dilemma for states wishing to apply their laws in the cyberspace. Individuals are increasingly involved in transactions that cross international territorial borders, which significantly reduces the ability of the state to exercise its authority to combat the consequences of these acts on its population. Within a comparative approach, this work basically focuses on the Rwandan law regarding the investigation of cybercrimes and procedures surrounding the collection of evidences in the Rwandan cyberspace.

1.0 INTRODUCTION

The internet has transformed the world into a global village. It improves business productivity, revolutionises working methods and makes possible the emergence

* Jacques Kabano is a full time Lecturer at the University of Lay Adventists of Kigali (UNILAK), He is a PhD holder in Public Law from Ankara University (Turkey). kabano@ankara.edu.tr, ORCID no https://orcid.org/0000-0002-0248-9204.

* Habarurema Jean Pierre is a National Prosecutor at National Public Prosecution Authority of Rwanda, and a Part Time Lecturer at the Institute of Legal Practice and Development (ILPD), Kigali Independent University (ULK), and University Lay Adventists of Kigali (UNILAK). habaruremaj.pierre@yahoo.fr.

of new business models allowing communication, negotiation, exchange and marketing in real time. In this sense, its contribution is essential for societies. It has become so indispensable over time that few organizations and individuals can do without it today. However, this revolution has also made possible new forms of crime linked to cyberspace.

Indeed, the Internet was not developed, from the start, in a secure way. Its multiple hardware, software and protocol components were and remain marked by numerous security flaws such as Injection flaws[3] which enable attackers to submit hostile data to an application. this can have very real consequences in the event of exploitation.[4] This has encouraged the emergence of deviant behaviour in cyberspace.

The Computer Crime and Abuse Act enacted in 1986 in the United States is the first ever legal instrument to establish criminal liability for malicious activities committed over computers.[5] Since then, many nations across the globe, step by step, undertook a long process of adopting different regulations within their cyber capabilities to fight cybercrimes. In this direction, the most important instrument was the Cybercrime convention of 2001 as the first international instrument to address the issues of computer crime and harmonisation of national laws to improve the investigation of malicious activities operated over computers.

---

3 Peter Loshin, 'Application Security' (techtarget.com, January 2022) available at<https://www.techtarget.com/searchsoftwarequality/definition/application-security> [Accessed on 4 May 2023]

4 Diane Hosfelt, 'Fearless Security: Memory Safety' (hacks.mozilla.org 23 January 2019 available at <https://hacks.mozilla.org/2019/01/fearless-security-memory-safety/> [Accessed on 4 May 2023]

5 Leighton Johnson, Security Controls Evaluation, Testing, and Assessment Handbook (2nd Edn, Academic Press 2019) 115-120

Besides having cybercrimes preventing provisions scattered around different laws and regulations, the fully established law on the investigation and punishment of cybercrimes in Rwanda was adopted in 2018.[6] The task to establish regulations of the implementation of the 2018 cybercrime law was left to the National Cyber Security Authority created on 31 May 2017.[7] Apart from cyber legal frameworks, Rwanda like other countries has adopted a system of strategizing its national cyber policies into a National Cyber Security Strategic Plan. This is a five-year plan where the country displays all activities toward an effective cybersecurity framework and their costs throughout that period of time.

In 2017, Rwanda established an independent investigative organ, Rwanda Investigation Bureau (RIB), amongst its missions was to '*prevent and pre-empt criminal acts by identifying and investigating all kinds of physical or cyber-attacks'*.[8] From this mission, RIB operates under eleven divisions including the *Cyber-crime Investigation Division*.[9] In the same year, Rwanda also created the National Cyber Security Agency (NCSA) with different responsibilities such as:

> "*Conducting cyber intelligence on any national security threat in cyberspace and provide information from such intelligence to the relevant organs; and establishing guidelines on the basis of national, regional and international ICT security principles."*[10]

---

6 'Law N° 60/2018 of 22 August 2018 on Prevention and Punishment of Cybercrime' (amategeko.gov.rw, 22 August 2018) available at <https://amategeko.gov.rw/document/legislation/2018> [Accessed on 23 April 2023]

7 Ibid Article 53.

8 Art. 9 of the 'Law N°12/2017 of 07/04/2017 Establishing the Rwanda Investigation Bureau and Determining Its Mission, Powers, Organisation and Functioning' (amategeko.gov.rw 7 April 2017) <Law N°12/2017 of 07/04/2017 Establishing the Rwanda Investigation Bureau and Determining Its Mission, Powers, Organisation and Functioning> [Accessed on 23 April 2023]

9 'RIB Leadership Structure' (rib.gov.rw) available at <https://www.rib.gov.rw/index.php?id=23> [Accessed on 23 April 2023]

10 Art. 9 of the 'Law No 26/2017 Of 31/05/2017 Establishing the National Cyber Security Authority and Determining Its Mission, Organisation and Functioning' (amategeko.gov.rw) available at <https://amategeko.gov.rw/document/legislation/2017> [Accessed on 10 May 2023]

This work examines the cyber investigations in Rwanda in comparison with the high level of uncertainties and complexes surrounding cybersecurity today with the aim to propose an extension of viable options fit for the Rwandan context.

2.0 CYBERCRIME INVESTIGATIONS AND EVIDENCE GATHERING IN RWANDA

The question of the application of legal frameworks to cyberspace and their implementation is ardently debated while generating a lot of confusion.[11]By its nature, as a cross-border space and cantered on the flow of immaterial data, cyberspace raises challenges for governance, traditionally defined in relation to the territorial state. Indeed, while the physical infrastructure of cyberspace may be subject to the jurisdiction and authority of the State, the latter can, on the other hand, find it difficult to exercise "effective control" over the flow of data and information.

This has led many actors to call for the development of new normative regimes to regulate cyberspace.[12]The transition from analog to digital system has instigated a new age of technology whose multiple legal consequences do not leave indifferent on the question of national criminal procedure, in particular that of digital criminal evidence, which remains a crucial issue today in the fight against cybercrime on the national level. The question raised by digital criminal evidence in cyberspace is mainly related to its constitution and reliability rather than its legality.

---

11 United Nations, 'UNCITRAL Expedited Arbitration Rules 2021: UNCITRAL Rules on Transparency in Treaty-Based Investor-State Arbitration' (United Nations 2022) available at <https://www.unilibrary.org/content/books/9789210021753> [Accessed on 23 April 2023]

12 'UN OEWG in 2023 - DW Observatory' (30 September 1998 available at <https://dig.watch/processes/un-gge> [Accessed on 23 April 2023]

2.1 Problematic of Cyber Crime Definition.

Cybercrime has not received a unanimous definition both nationally and internationally. This lack of consensus on the concept would indeed be at the origin of a myriad of definitions proposed on all sides by States and official international organizations, which confront several interests and systems. Classically, these definitions limit cybercrime to the modus operandi of the cyber-offenders or to the object of the offence.

This is the case, among others, of the definition developed by the Organization for Economic Co-operation and Development (OECD) which, alluding to the processing or security of data, adopts cybercrime as '*any unlawful or unethical or unauthorized conduct relating to automatic data processing and/or data transmission'*.[13] Similarly, the United Nations also limits cybercrime to attacks on the security of computer systems.[14]

Other definitions, in particular those of the United States[15] and the United Kingdom, are limited solely to fraudulent access to a computer system, which undoubtedly excludes a significant part of the offense spectrum of cybercrime, namely, all offenses which can be committed through a system.[16] In Rwanda, cybercrime has not been defined either in the Penal Code, Criminal Procedure or in any other legal text, regardless the fact that the Law N° 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes has mentioned this term from start to finish.

---

13 OECD (Ed), Computer Related Criminality: Analysis of Legal Politics in the OECD Area, (OECD, 1986)

14 'Model United Nations Topic-Cybercrime' (unodc.org) available at <https://www.unodc.org/e4j/en/mun/crime-prevention/cybercrime.html#/top> [Accessed on 10 May 2023]

15 Chris Kim; Barrie Newberger; Brian Shack, 'Computer Crime' (2012) *49 ACLR 443*

16 National Crime Agency, 'Cybercrime' (nationalcrimeagency.gov.uk) available at <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime> [Accessed on 10 May 2023]

This law only stipulates acts that should count as cybercrimes rather than defining what does cybercrime really mean. Be that as it may, cybercrime is a protean notion that is generally analysed under two meanings.[17] Literally composed of two words, "cyber" which comes from the Latin "*kubernan*", that is to say to govern or pilot, and "crime" which constitutes all the criminal acts or omissions committed at a given period in a society. Cybercrime, in the strict sense, includes cyberattacks, which correspond to attacks on automatic data processing systems utilising viruses or malware. Additionally, it is equally used to describe traditional criminal activities in which computers or networks are used to carry out illicit activity.

2.2 Digital Criminal Evidence

Evidence means the demonstration of the reality of a fact or a law. French Jurist Jean Domat conceptualised evidence as "what persuades the mind of a truth".[18] It is present in all legal matters, including criminal law where it consists precisely in establishing the constitution of an offence and in seeking the perpetrator. Unlike civil law, which includes the constitution of evidence in a set of legal and contractual obligations, the Rwandan criminal law through the law on evidence and its production, provides a relative freedom of the production of the evidence i.e., the proof of a fact or a law, in criminal matter, "*evidence can be established by all means of fact or law provided they are subject to adversarial proceedings*."[19]

The history of criminal law experienced several modes of evidence ranging from rational evidence (admission, testimony and writing) to irrational evidence, which was widely practiced in ancient societies in the framework of sacred

---

17 Myriam Quéméner, *Sécurité et stratégie, "Concilier la lutte contre la cybercriminalité et l'éthique de liberté''*(cairn, 2011) 59.

18 J. Domat, Les lois civiles dans leur ordre naturel (éd. Cavelier, 1771)204.

19 'Law N° 15/2004 of 12/6/2004 Relating to Evidence and Its Production in Rwanda', Art.119.

justice, which ended up disappearing. These are the judicial duel and ordeals.[20] Today the so-called digital evidence, has emerged as a new form of evidence on the digital market.

2.2.1. The Challenge of Digital Criminal Evidence in Cybercrime Investigation

The proliferation of clandestine servers that allow criminal organizations to sell stolen information (personal data issued by governments, credit or debit cards, personal identification numbers, bank account numbers, email address lists) to facilitate identity theft clearly demonstrates the growth enjoyed by cybercriminal activity. With the popularisation of cybercriminal operating methods on the Internet, today it is not necessary to have technical skills to launch a cybercriminal operation.

The level of technical expertise required for a cybercriminal project no longer makes sense when it is possible today to freely buy the most elaborated spyware as well as the data collected by this same software: banking information and sufficient personal information to purchase online or transfer funds. In addition, it is also possible to order a cybercriminal act from time to time from specialised service providers who bring their share of expertise to the operation, each link generating profits whose amount responds solely to the laws of supply and demand, with the rarity of a skill increasing prices accordingly.

However, this human-internet dependence or correlation, although favouring human activity, has negative consequences both with regard to the global economy and to the private and professional lives of users of this network, because it causes the explosion in the rate of cybercrime. According to

[20] A form of medieval justice which consists in subjecting a person accused of a crime to a painful ordeal in which only a god can help him to succeed if he were innocent.

Symantec,[21] cybercrime costs each year, in terms of global damage, approximately 114 billion euros, almost eight (8) times more than the cost of the 2012 Olympic Games in London.

This sum increased astronomically in 2020 (over a trillion dollars) according to a study by the computer company McAfee.[22] However, criminal justice will benefit from this technological revolution and, like the fingerprints or DNA used in conventional forensics, the digital traces left by cybercriminals can help to find the perpetrators and possibly reconstitute the acts. Hence the usefulness of digital evidence in the context of cybercrime proceedings.

2.2.2 Collection of Digital Evidence in Rwanda.

The Rwandan law on evidence and its production does not in any way help in the collection of digital evidence. The only provision regarding digital evidence under this law is the recording of voices using electronic devices and filming using cameras in the article 121, the rest is about production of evidence in the traditional ways for tradition crimes. From Article 8 to article 15 of the Law on the prevention and punishment of cybercrimes in Rwanda, there is a section about investigation of cybercrimes. This law although not a standalone reference, remains the most important gate to the methods used to collect digital evidence in Rwanda.

---

21 Fahmida Y Rashid, 'Cost of Cybercrime Dips to $110 Billion: Symantec' (*SecurityWeek*, 5 September 2012) <https://www.securityweek.com/cost-cybercrime> [Accessed on 23 April 2023].

22 James Andrew Lewis, Zhanna L Malekos Smith and Eugenia Lostri, 'The Hidden Costs of Cybercrime' available at <https://www.csis.org/analysis/hidden-costs-cybercrime> [Accessed on 23 April 2023].

a. Obligation to Collaborate with Organs in Charge of Investigations.

The law on prevention and punishment of cybercrime in Rwanda in its article 5 obliges any concerned person *to*:

> *"Cooperate with the organ in charge of investigations or prosecution where this person has to respond to any inquiry about the investigation, comply with any lawful directions including disclosing access code to a computer system and also to disclose all data required for the purposes of investigation and of prosecution of an offence."*[23]

This article does not mention a level of cooperation, whether it is at national or international. However, given the transnational nature of cybercrime restricting this cooperation national level without seeking an expended collaboration beyond the territorial boundaries would definitely constitute a mistake.

International cooperation in the field of cybercrime is of crucial importance because the fight against this type of internationalized crime meets a common need of States. However, the development of mutual assistance remains conditional. Moreover, with regard to the specificity of this crime, international cooperation also includes technical service providers who play a major role. However, cooperation between public authorities and technical service providers is inconsistent.

The fight against cybercrime is specific in terms of digital evidence, which is fragile. Therefore, the prosecution of cybercriminals leads public authorities to deal with economic actors. On this point, the regulatory mechanisms are multifaceted: first, the judicial authorities can take injunction measures, either to provide information, or to block sites from technical service providers. It is a forced cooperation with ineffective results; then, a form of self-regulation is put in place through the development of charters and codes of conduct.

---

[23] Article 5 of the Law on Prevention and Punishment of Cybercrime in Rwanda

This is a contractualised cooperation suffering from a lack of supervision and revealing the absence of a global policy to fight against cybercrime. Firstly, with regard to injunction measures, the judicial authorities can contact Internet service providers (ISP) and hosts in order to obtain information on the offences committed and the perpetrators thereof. ISPs and hosts benefit from the principle of civil and criminal liability.

They are also not subject to a general obligation to monitor the information they store and transmit, or even to seek out violations. However, judicial injunction measures with these service providers are possible. These may be computer requisitions provided for during investigations and instructions: service providers are then required, under penalty of a fine, to provide the information requested.[24]

This leads to the question of data retention by technical service providers. However, the retention of data does not obey an unequivocal regime allowing cooperation at the international level. The obligation to preserving data is the means of obtaining evidence**.** The law on prevention and punishment of cybercrime in Rwanda obliges Internet service Providers to retain:

> *"Any information which may be of assistance in investigating the offence including particularly information which shows the communication's origin, destination, route, time, date, size, duration and the type of the underlying services".*[25]

There is no mention of how long this information should be kept by the service providers anywhere in this law. In the same direction, the Rwandan Law relating the protection of personal data and privacy, provides that an electronic personal data can be retained *until the purposes of the processing of personal data are*

24 Article 5 of the Law on the prevention and punishment of cybercrimes in Rwanda.
25 Article 5 (2).

fulfilled or even longer when there is investigation or prosecution.[26]The same provision also proposes other grounds for a longer retention of personal data depending on the regulation of such grounds under the direction of the supervisory authority.[27]

As a comparative matter, Directive 2006/24/EC of March 15, 2006 requires Member States to provide for this storage obligation to be borne by fixed and mobile telephone operators and Internet access providers for a period between 6 and 24 months from the communication.[28] French law provides for a duration of one year.[29] However, if, in Europe, the duration of data retention does not pose great difficulties, it is different for American commercial companies: the latter have diversified practices. For example, the Google search engine erases data from accounts that have become inactive after an indefinite period;[30]
Twitter refers to a maximum duration of 18 months[31], while practice has revealed a retention period of 2-3 months. Moreover, this heterogeneity is aggravated by refusals to submit to requisitions. The will to cooperate then has varying degrees depending on the companies and their locations. Thus, Google and Facebook only partially respond to information requisitions on the condition that the users are European and if the communication of information is limited to the criterion of the IP address.[32]

---

26 Article 52 of the Law no 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy.

27 Ibid. Art.3 (23º) defines a supervisory authority as a public authority in charge of cyber security. In this sense, NCSA (National Cyber Security Agency) is in charge.

28 Directive 2006/24/EC of March 15, 2006.

29 'Légifrance - Publications Officielles - Journal Officiel - JORF N° 0242 Du 18/10/2022' <https://www.legifrance.gouv.fr> [Accessed on 23 April 2023]

30 'How Google Retains Data We Collect – Privacy & Terms – Google' available at <https://policies.google.com/technologies> [Accessed on 23 April 2023]

31 Twitter Privacy policy available at <https://twitter.com/en/privacy/previous/version_15> [Accessed on 23 April 2023]

32 Regulation (Eu) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Some service providers refuse any transmission of information, but notify the authorities of the country concerned (Facebook); Twitter limits the transmission of information to serious crimes, eliminating any cooperation in matters of press offences.[33] The result is a greatly slowed cooperation in terms of cybercrime. These refusals to cooperate by the major operators denote the extended cooperation of these same service providers with the services of the Federal Bureau Investigation (FBI) and the National Security Agency (NSA).[34]

The problem is the same in terms of injunctions to block illegal sites, cooperation causing difficulties in implementation and revealing the inconsistent nature of practices. It is therefore clear that the fight against cybercrime is under construction. This construction is not due to the lack or absence of the norm, but to its abundance without a global international policy being determined. While this is decisive as cybercrime covers a global dimension, cooperation remains limited.

Therefore, if the repressive tool is dense, its effectiveness is tempered by multifaceted interstate cooperation. The extension of this cooperation must bring Rwanda to team up with other countries in forms of mutual understanding with other nations and join available cooperation initiatives.[35] In this context, Rwanda is ready to join the *Budapest Convention on Cybercrime and its additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer and computer system.*[36]

---

33 M. Robert (ed.), Report on cybercrime, Protecting Internet users, 2014, p. 179.

34 Indeed, Google, Yahoo, Microsoft, Skype, YouTube, Apple, AOL, Facebook, Paltalk have allowed access to their users' data through the Prism system.

35 It is evident that the country is involved in many platforms against cybercrime, but nothing beats bilateral and multilateral agreements. e.g. the working group against cybercrime available at <https://www.coe.int/en/web/cybercrime/-/interpol-and-glacy> [Accessed on 22 February 2023].

36 Cabinet Meeting Resolutions of 24th March 2023 available at <https://www.primature.gov.rw/index.php?> [Accessed on 25th March 2023]

This means that once the presidential order acceding to this convention is published in the official gazette,[37] the country will join cooperation in investigation with other 50 signatories and will be obliged to amend the law on protection and punishment of cybercrime to the international standards available in the Convention.[38]

b. Search And Seizure

In the practice of searches, the seizure of computer data at the home of the person likely to hold information relating to the incriminated facts now constitutes one of the essential probative tools of the criminal investigation. Indeed, the systematization of the use of digital tools has led all subjects of law; natural and legal persons, to register a considerable amount of personal information, about themselves and third parties, in digital files which are themselves materially stored on one or more computer media.[39] The evolution of digital technologies has led, in terms of territoriality, to make a distinction between the material medium for storing information and the one from which this same information is accessible. For example, it has become common practice in companies for this data to be stored on servers located in a dedicated room, or even in another building or at a third party's, the user only having a screen and a keyboard, making it possible to modify this data, without however having material access to the storage medium itself.

In practice, accessibility takes precedence over the physical storage of data. For the investigator, it is more important to have access to the screen enabling the document to be read than to the server on which it is stored: having access to a

---

37 Council of Europe, Convention on Cybercrime, Budapest 2001. Art. 23-36 European Treaty Series - No. 185.

38 Ibid, Article 2-22.

39 The informative content is not limited to the information contained in each file, since the reading of the mass of files themselves is information (one will think in particular of the metadata).

server room does not usually allow the investigator to read the e-mails nor to have access to the accounts of a company. On the other hand, this informative content can be delivered to anyone who is at the location of the screen delivering the information, that is to say the screen connected to the server in question. It shows that in the criminal investigation, it is not the server, but the access to the server, which is fundamental.

In the same way, the user of an electronic mailbox consults, via his or her computer, content which may be stored thousands of kilometres away, on servers possibly located abroad. It is even possible that this content is simultaneously stored on several servers and that, materially, and often without the user even being aware of it, the storage is split over several different countries.

Whether it is the personal computer of a natural person, in the context of common law offences, terrorism or organized crime, or the computer system of a company or association in the context of repression of economic, financial and fiscal offences, access to dematerialized data storage media constitutes an essential phase of the criminal investigation, and this during the flagrance investigation, the preliminary investigation and judicial information.

In Rwandan law, particularly in the provisions of article 9 of the Law on prevention and punishment of cybercrime, the organ in charge of prosecution may issue an order to enter into any area premise and search or seize a computer or a computer system; secure the computer or computer system data accessed; extend the search and access a computer or any another computer system where the data being sought is stored. This legal extension of the scope of the search thus allows investigators to access a computer system located outside the premises searched, in order to collect data relevant to the investigation.

Additionally, during an investigation a computer or a computer system may be preserved for a period not exceeding thirty (30) days as per the order of the prosecution with fear that the data in question may be modified or lost.[40] However, the question of the legal basis for the search for data arises specifically for dematerialized data, which may be accessible from the premises of the person searched, while being stored in a separate place.

Likewise, the Rwandan law, is silent about investigation of data which may be stored abroad. Indeed, it would therefore be sufficient for any person searched to mention to the investigators, from the start of the operations, the storage of their data outside the national territory, for the investigation officer to find rely to the international commitments in force to continue the search. The reason for the absence of prior information from the investigation officer on the location of the servers abroad lies in the attack on the sovereignty of the foreign State that would constitute the recognition of a power to access and copy data stored outside the national territory by Rwandan investigators and prosecutors.

This provision subjects them to the principle of national jurisdiction and does not seem to adversely affect the person searched. Thus, when the investigation officer begins the search, an alternative is possible: either he or she ignores or unaware of the situation of the servers abroad, and in this case the search will be legal, or he or she is aware of it, and in this case he or she must comply with Rwanda's international commitments in force. The problem is that such kind of international commitments are likely to face political wills of other countries, because it is not under the obligation they have to comply with according to international law.

In France for example, access to and copying of data on servers located abroad could be analysed, even without prior knowledge of the location of the servers

40 Article 12 of the Law on the Prevention and Punishment of Cybercrime.

abroad. This is in a violation of the rules of territorial jurisdiction of the judicial police provided for in Article 18 of the Code of Criminal Procedure, which considers the national territory as the maximum extent of territorial jurisdiction. Admittedly, the fifth paragraph of Article 18 of the Code of Criminal Procedure provides that judicial police officers may conduct hearings on the territory of a foreign State, but only with the agreement of the competent authorities of that State, on express rogatory commission or on requisitions, the extension of this competence being limited to this single act and not concerning either searches or seizures.

In a ruling of November 6, 2013, the Criminal Chamber of the Court of Cassation had to consider the compliance, with regard to article 57-1 of the code of criminal procedure,[41] of the consultation carried out by investigators on the occasion a search of password-protected data stored on a website, itself hosted on a server located in the United States. The judgment of the investigating chamber, validating the search, based the territorial jurisdiction of the investigators on article 32 of the Convention of November 23, 2001 on cybercrime, which provides that a party may access stored computer data accessible to the public, regardless of the geographical location of the data.

The IT tool now allows these same individuals to access this data, manipulate it and commit the offense without storing it, as it is stored on servers located abroad. The computer tool has therefore made it possible to be in possession of the instrument and the proceeds of the crime or offence, without this evidence being materially present on Rwandan territory. The legislators therefore should allow investigators, by adopting the same provisions as they are in Article 57-1 of the French Code of Criminal Procedure, to correct this asymmetry.

41 Crim. 6 Nov. 2013, n° 12-87.130, D. 2013. 2826.

c. Disclosure of Data and Collection of Electronic Traffic Data

Most institutions across the globe are prohibited by their laws from disclosing any information collected that could reveal the identity of any person, business or organization without their permission or without being authorized by law. Various confidentiality rules apply to all data disseminated or published in order to prevent the publication or disclosure of any information deemed confidential. Where necessary, data is removed to prevent direct disclosure or cross-referencing of recognizable data. This is an international practice. However, this practice is not immune to exceptions. The authorisation to collect data about a person without that person's knowledge is granted only in exceptional circumstances. In relation to cybercrime investigation in Rwanda, a person may be compelled to disclose the data or facilitate the investigating officer to enter a computer that is storing the data in question.[42] In case the holder of such information is not willing to disclose the data or allowing the officer in charge of investigation to record the data, the prosecutor applies for a court order which in return compel him or her to comply.[43]

In case an investigating officer is given a pass to enter someone's computer, he or she must only look for the data which is in the limits of his or her investigation, otherwise there is a possibility of oversharing even for the most sensitive information which has no link with the suspected cybercrimes. The Rwandan legislators should think of the risks of abuse of such authority and possibility of reporting in case of abuse and other judicial remedies.

42 Article 11 of the law on the prevention and punishment of Cybercrime in Rwanda.
43 Ibid. Article 14.

d. Authorization To Use a Forensic Method

The expansion of the use of sophisticated ICTs in the commission of criminal offenses represents an ongoing challenge for law enforcement and prosecution, which must keep abreast of all technological innovations, not only to detect new forms of cybercrime, but also to be able to collect evidence for their prosecution. Within the framework of the Council of Europe for example, The Recommendation No. R (95), of the Committee of Ministers to member states has already underlined that "*the creation of specialized units for the repression of offenses whose prosecution requires information technology should be considered*".[44]

This triggered countries under this council to consider two things, on the one hand, the creation of institutions which are responsible in general for the computerization of the procedure, the automation of the legal system and the technical equipment of the courts which in general depends on the Ministry of Justice (e.g. Austria, Belgium, Brazil, Croatia, Spain, Turkey); on the other hand, the establishment of specialized units within law enforcement agencies that deal with cybercrime, computer forensics and Internet surveillance.

Article 15 of the Law on the prevention and punishment of cybercrime in Rwanda provides the possibility to use forensic methods if the prosecution cannot be accomplished without relying on digital forensic. This article does not mention which unit should provide forensic evidence but establishes that using such method must be ordered by the court after the application by the prosecution authority. It also proposes that the court may order any service provider to provide a forensic tool in that procedure.

[44] Rec. No. R (95) 13, of the Committee of Ministers to member states on problems of criminal procedure related to information technology, adopted on 11 September 1995.

Although this law is silent about the unit that conduct such method, the practice shows that the Rwanda Forensic Laboratory which generally helps in other evidence seeking related scientific methods, provides also digital forensic.[45] Whether this Laboratory is well equipped and has sufficient human and technical resources in terms of cyber criminality is a question not covered by this work.

Many countries have several specialized units, one in each of the institutions involved in the criminal justice system. Sometimes there is also another central unit to coordinate different law enforcement units or agencies (e.g., Belgium, Federal Computer Crime Unit, Japan, Netherlands, Spain, Turkey, or the United States). Taking the example of The United States,[46] the existence in of working groups, at least for law enforcement, involved in the implementation of ICT in the criminal justice system: the Internet Crimes Complaint Centre which is a clearinghouse for the investigation of Internet crime; the Resource Fusion Unit and the Cyber Initiative that analyse internet crime trends, but also filter out false leads before information on cybercrime reaches the prosecution service;[47] the United States Computer Emergency Preparedness Team, which does not investigate, but provides support, coordinates and conducts research projects; and finally InfraGard, part of the Department of Homeland Security, in which private and public actors share information, promote dialogue between the ICT community and law enforcement agencies.

The creation of special centres for research and training in ICT seems to be very useful. The Belgian report mentions the "Cybercrime Centre of Excellence" for training, education and research in the public sector, where universities, private ICT companies, the police, the prosecution and the judicial system work

45 RFL, 'Digital forensic service' (rfl.gov.rw) available at <https://www.rfl.gov.rw/index.php?id=164> [Accessed on 27 February 2023]

46 UNODC, *Comprehensive Study on Cybercrime*, (UN New York, 2013), pp. 152-156.

47 Ibid. In this unit what is interesting is the support obtained from different private companies, such as Microsoft or eBay.

together. However, in Rwanda like in other countries, it seems that specialization has been achieved at the police and investigative level, while the judiciary seems to remain largely unspecialised.[48]

In most cases, states must use commercial intermediaries such as social media platforms to monitor and regulate online behaviour.[49] The transnational nature of information disseminated on the Internet presents another challenge because this data may be stored on one or more servers located in different States. State authorities must therefore rely on a new form of cooperation with other States to be able to investigate, prosecute and convict cybercriminals. Cyberspace thus undermines good governance practices as it not only involves actors within the jurisdiction of a single state but also impacts a range of actors at the international level. Rwanda, a country which is aspiring to be one of the African tech hubs[50], should develop even cyber diplomacy than others.

3.0 CYBERCRIME SITUATION IN RWANDAN COURTS

According to the data collected through the Rwanda Integrated Electronic Case Management System Rwanda (IECMS) from the National Public Prosecution Authority in the Research Division, the number of claims rose since 2018.

48 Ibid. pp. 172-177.

49 Niva Elkin-Koren; Eldar Haber, "Governance by Proxy: Cyber Challenges to Civil Liberties," Brooklyn Law Review, 82 no. 1, p. 105.

50 Mwangi Karanja, Leveraging Rwanda's position as a tech hub, 02 August, 2021 available at <https://www.pwc.com/rw/en/publications/> [Accessed on 20 March 2023]

Table 1. Cyber Crimes Cases in Rwanda (2018-2022)[51]

Year	Received claims	Parties			Filed to Courts	Classified	Total reviewed	Under review	%
		Females	Males	Total					
2018-2019	125	25	128	153	75	50	125	0	100
2019-2020	158	33	153	186	86	71	157	1	99.4
2020-2021	286	86	253	339	168	118	286	0	100
2021-2022	535	141	486	627	230	294	524	11	97.9

Among all cyber-crimes committed from 2018-2022 in Rwanda, four crimes; Access to a computer or computer system data,[52] unauthorized access to a computer or a computer system data,[53] Cyber-stalking,[54] and access to data with intent to commit an offence seem to be the most committed crimes in this country.[55] Other common cybercrimes such as phishing,[56] spamming,[57]publication of rumours, and impersonation were also among the committed crimes.[58]

4.0. CONCLUSION

Despite the efforts by the Rwandan legislators to cover all the points related to the topic of computer crimes, there are still some legal gaps that are good to

51 This is first-hand information retrieved from the National Public Prosecution Authority by the authors.
52 Article 24 of the Law on protection and Punishment of Cybercrimes.
53 Ibid. Art. 18.
54 Ibid. Art. 35.
55 Ibid. Art. 17.
56 Ibid. Art. 36.
57 Ibid. Art. 37.
58 Ibid. Art. 39,40.

address. Crimes such as piracy, propagation of child pornography and the disproportionate diversion of data at a general level,[59]make cybercriminals occupy an important space to commit crimes. Computer crimes cannot be eliminated peremptorily, but current Laws can be upgraded effectively, even supported by the same technology, in order to fight these illegal acts on the web.

Rwanda needs to establish a security system, which allows the protection of information, especially when the information that is handled is first-line. To understand computer crimes, requires to take a multidisciplinary approach let alone leaving the matter to legal practitioners alone. Although Rwanda like some other states has adopted policies and frameworks in terms of cybersecurity and cyberspace governance, the general lack of knowledge in this area is a barrier to the proper investigation and collection of evidences in cyberspace.

[59] Beside prohibiting publication of child pornography and provision of punishment by Article 34 of the law on the prevention and punishment of Cybercrime in Rwanda, Child pornography itself and related circumstances have never been determined by Rwandan Laws.

LIST OF REFERENCES

Cabinet Meeting Resolutions of 24th March 2023 available at <https://www.primature.gov.rw/index.php?eID=dumpFile&> [Accessed 25 March 2023]

Chris Kim; Barrie Newberger; Brian Shack, 'Computer Crime' (2012) *49 ACLR 443*

Council of Europe, Convention on Cybercrime, Budapest 2001. Art. 23-36 European Treaty Series - No. 185.

Diane Hosfelt, 'Fearless Security: Memory Safety' (hacks.mozilla.org 23 January 2019) available at <https://hacks.mozilla.org/2019/01/> [Accessed 4 May 2023]

Fahmida Y Rashid, 'Cost of Cybercrime Dips to $110 Billion: Symantec' (*SecurityWeek*, 5 September 2012) available at <https://www.securityweek.com/cost-cybercrime-dips-110-billion-symantec/> [Accessed 23 April 2023]

J. Domat, *Les lois civiles dans leur ordre naturel* (éd. Cavelier, 1771)

James Andrew Lewis, Zhanna L Malekos Smith and Eugenia Lostri, 'The Hidden Costs of Cybercrime' <https://www.csis.org/analysis/hidden-costs-cybercrime> [Accessed on 23 April 2023].

Law N° 60/2018 of 22 August 2018 on Prevention and Punishment of Cybercrime' (amategeko.gov.rw, 22 August 2018) <https://amategeko.gov.rw/document/legislation/2018> [Accessed on 23 April 2023.

Law no 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy.

Law No 26/2017 Of 31/05/2017 Establishing the National Cyber Security Authority and Determining Its Mission, Organisation and Functioning' (amategeko.gov.rw) available at <https://amategeko.gov.rw> [Accessed on 10 May 2023]

Law N°12/2017 of 07/04/2017 Establishing the Rwanda Investigation Bureau and Determining Its Mission, Powers, Organisation and Functioning' (amategeko.gov.rw 7 April 2017)

Law N° 15/2004 of 12/6/2004 Relating to Evidence and Its Production in Rwanda', Art.119.

Légifrance - Publications Officielles - Journal Officiel - JORF N° 0242 Du 18/10/2022' available at <https://www.legifrance.gouv.fr> [Accessed on 23 April 2023].

Leighton Johnson, Security Controls Evaluation, Testing, and Assessment Handbook (2nd Edn, Academic Press 2019) 115-120

M. Robert (ed.), Report on cybercrime, Protecting Internet users, 2014, p. 179.

Model United Nations Topic-Cybercrime' (unodc.org) available at <https://www.unodc.org/e4j/en/mun/> [Accessed 10 May 2023]

Mwangi Karanja, Leveraging Rwanda's position as a tech hub, 02 August, 2021 available at <https://www.pwc.com/rw/en/publications/> [Accessed on 23 March 2023].

Myriam Quéméner, *Sécurité et stratégie, "Concilier la lutte contre la cybercriminalité et l'éthique de liberté"*(cairn, 2011)

National Crime Agency, 'Cybercrime' (nationalcrimeagency.gov.uk) available at <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime> [Accessed on 10 May 2023]

Niva Elkin-Koren; Eldar Haber, "Governance by Proxy: Cyber Challenges to Civil Liberties," Brooklyn Law Review, 82 no. 1, p. 105.

OECD (Ed), Computer Related Criminality: Analysis of Legal Politics in the OECD Area, (OECD, 1986) 8

Peter Loshin, 'Application Security' (techtarget.com, January 2022) available at <https://www.techtarget.com/searchsoftwarequality/definition/application-security> [Accessed on 4 May 2023]

Rec. No. R (95) 13, of the Committee of Ministers to member states on problems of criminal procedure related to information technology, adopted on 11.9.1995.

Regulation (Eu) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

RFL, 'Digital forensic service' (rfl.gov.rw) available at <https://www.rfl.gov.rw/index.php?id=164> [Accessed on 27 February 2023]

RIB Leadership Structure, (rib.gov.rw) available at <https://www.rib.gov.rw/index.php?id=23> [Accessed 23 April `2023]

Twitter Privacy policy available at <https://twitter.com/en/privacy/previous/version_15> [Accessed 23 April 2023]

UN OEWG in 2023 - DW Observatory' (30 September 1998 available at <https://dig.watch/processes/un-gge> [Accessed 23 April 2023].

UNODC, *Comprehensive Study on Cybercrime*, (UN New York, 2013), pp. 152-156