STUDIA IURIS

Jogtudományi Tanulmányok / Journal of Legal Studies

2024. I. évfolyam 4. szám

Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.
A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.
A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.
A folyóirat online verziója szabadon letölthető (open access).

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola
Székhely: 1042 Budapest, Viola utca 2-4
Felelős Kiadó: Tóth J. Zoltán

A tipográfia és a nyomdai előkészítés Csernák Krisztina (L'Harmattan) munkája
A nyomdai munkákat a Robinco Kft. végezte, felelős vezető Gembela Zsolt

Honlap: https://ajk.kre.hu/index.php/jdi-kezdolap.html
E-mail: doktori.ajk@kre.hu
ISSN 3057-9058 (Print)
ISSN 3057-9392 (Online)
URL: KRE ÁJK - Studia Iuris
https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html

CHALLENGES IN THE LEGAL FRAMEWORK FOR UTILIZING ELECTRONIC EVIDENCE IN CYBER-CRIME IN RWANDA

Francois Regis Nshimiyimana[1]

ABSZTRAKT ■ Ez a tanulmány a Ruandában jelentkező azon kihívásokkal foglalkozik, amelyek az elektronikus bizonyítékok hatékony felhasználásával kapcsolatosak a kiberbűnözés elleni küzdelemben, ami , ami kulcsfontosságú a mai digitális korban. Fejlődő országként Ruanda akadályokba ütközik az elektronikus bizonyítékok jogrendszerébe való integrálása terén, ami akadályozza a kiberfenyegetések hatékony leküzdését. A tanulmány jogi és technikai szempontból vizsgálja ezeket az akadályokat, azzal a céllal, hogy megértse hatásukat Ruanda kiberbűnözés elleni erőfeszítéseire.A feltárt kulcskérdések a következők: milyen jogi keretbeli kihívások akadályozzák az elektronikus bizonyítékok hatékony felhasználását a kiberbűnözési ügyekben Ruandában? Léteznek-e Ruandán belül stratégiák vagy jogi reformok ezen akadályok leküzdésére? Hogyan segíthetnek a legjobb nemzetközi gyakorlatokból származó tapasztalatok a kiberbűnözési ügyekben alkalmazott elektronikus bizonyítékokkal kapcsolatos ruandai jogi keret lehetséges megoldásaiban? A kutatási módszertanmagában foglalja a jogi keretekre, kiberbűnözésre és elektronikus bizonyítékokra vonatkozó szakirodalom mélyreható áttekintését,, valamint a vonatkozó ruandai jogszabályok és politikák elemzését. A tanulmány zárásként potenciális megoldásokat javasol Ruanda jogrendszere hatékonyságának növelésére a kiberfenyegetések elektronikus bizonyítékok felhasználásán keresztül történő leküzdésében.

ABSTRACT ■ This paper delves into Rwanda's challenges in effectively utilizing electronic evidence to combat cybercrimes, a critical need in today's digital era. As a developing nation, Rwanda faces hurdles in integrating electronic evidence into its legal system, hindering its ability to tackle cyber threats efficiently. The paper examines these obstacles from legal and technical perspectives, aiming to understand their impact on Rwanda's cybercrime efforts. Key questions explored include: What legal framework challenges impede the effective use of electronic evidence in cybercrime cases in Rwanda? Are there existing strategies or legal reforms within Rwanda to address these obstacles? How can insights from international best practices inform potential solutions for Rwanda's legal framework regarding electronic evidence in cybercrime cases? The research methodology involves an in-depth review of the literature on legal frameworks, cybercrimes, and electronic evidence, coupled with an

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

analysis of relevant Rwandan laws and policies. The paper concludes by proposing potential solutions to enhance Rwanda's legal system's effectiveness in combating cyber threats through electronic evidence.

Keywords: electronic evidence, cyber-crime

1. Introduction

Cybercrime, including in Rwanda, has become a significant problem everywhere in the digital era. The techniques employed by cybercriminals to perpetrate crimes also evolve along with technology. The legal framework for using electronic evidence is essential to guarantee successful prosecution and justice in cybercrime situations. Due to the difficulties in obtaining, maintaining, and presenting electronic evidence within its judicial system, Rwanda, like many other nations, needs help. That is why Rwanda felt an obligation to join the Convention on Cybercrime and its additional Protocol concerning the criminalization of acts of racist and xenophobic nature committed through computer systems[2]. It has made significant strides in addressing cybercrime and enhancing its legal framework to accommodate electronic evidence. However, challenges persist in effectively utilizing electronic evidence in cybercrime cases.

1.1. Background and development of electronic evidence in cybercrime in Rwanda

The evolution of electronic evidence in Rwanda began in the early 2000s, coinciding with an increase in cyber-related crimes in the country. In response to this trend, the Rwanda Information and Communication Technology Authority (RITC) was established in 2002 to oversee the information and communication technology sector.[3] This year marked the initiation of Rwanda's efforts to incorporate electronic evidence into cybercrime investigations.

[2] The Convention on Cyber Crime, done in Budapest, Hungary, on November 21, 2001, and its additional Protocol concerning the criminalization of acts of racist and xenophobic nature committed through computer systems, done in Strasbourg, France, on January 28, 2023.

[3] Ronald Serwanga: *Legal mechanisms for enforcing electronic transactions in Rwanda. Diss.* University of Rwanda, 2019. 8-9.

In 2007, the Rwanda National Police (RNP) established its Cyber Crime Unit to investigate and prosecute cybercrime cases[4]. This unit has played a crucial role in integrating electronic evidence into Rwanda's justice system by training officers to handle digital evidence and fostering collaboration with international partners to exchange best practices.

1.2. Definition of cyber-crime and its increasing prevalence

Any illegal behavior involving a computer, networked device, or network is cyber-crime[5]. While most cyber-crimes are committed to making money for the perpetrators, some are explicitly committed to harming or destroying computers or other devices. Others disseminate viruses, illicit information, photographs, and other items via computers or networks. Certain cyber-crimes combine the two tactics of targeting computers and infecting them with a virus that spreads to different devices and, occasionally, even entire networks.

One of cybercrimes' main consequences is their financial impact. Cybercriminal activities often aim for monetary gain and can encompass various profit-motivated offenses.[6] These can range from ransomware attacks and internet scams to identity theft and efforts to pilfer financial account details, credit cards, or other payment card information.

1.3. Significance of electronic evidence in combating cyber crimes

Electronic evidence in cybercrime cases pertains to data stored, transmitted, or accessed on digital devices and networks, represented in binary code. This type of evidence holds significant importance in legal proceedings, as it can be used to construct a case against a defendant and presented in court. Similar to how physical evidence, such as fingerprints or DNA, can link a person to a crime, digital evidence provides insight into activities, interactions, and intentions. Much like physical evidence can create a timeline of events in a crime; digital

4 Bernard Walumoli: *A Critical Analysis of the Challenges Facing Countercybercrime in 21st Century Africa: a Focused Comparison of Kenya and Rwanda. Diss*. University of Nairobi, 2021. 53-77.

5 Brian Payne: Defining cybercrime. In: Thomas J. Holt – Adam M. Bossler (eds.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Cham, Springer, 2020. 3-25. https://link.springer.com/referencework/10.1007/978-3-319-78440-3.

6 Ki Hong Steve Chon: *Cybercrime precursors. Towards a model of offender resources. Doctor of Philosophy dissertation*. Australian National University, 2016. 20.

evidence serves a similar purpose in the virtual world.[7] It helps create a narrative of what occurred, why, and how it unfolded.

Similar to how physical evidence, such as fingerprints or DNA, assists in understanding the sequence of events in a crime, digital evidence serves a similar function in the digital domain. It aids in creating a narrative of the events, motivations, and actions that are believed to have occurred. By gathering and examining digital evidence, legal experts can reconstruct timelines, validate assertions, and potentially reveal discrepancies or omissions in the Prosecution's argument. Thus, grasping the intricacies of digital evidence and its significance is crucial for legal professionals and individuals accused of cyber-crime.

2. Current legal provisions on electronic evidence and cyber crime under Rwandan law

The spread of the Internet has been the most significant social and technological change in recent times, reducing trade barriers and playing a considerable role in supporting sustainable development in Rwanda. However, our increased dependence on the Internet and digital technologies increases our vulnerability to cyber threats, and our increasing reliance on cyberspace has brought new risks; criminals are increasingly using cyber-space to gain access to personal information, steal businesses and intellectual property, and gain knowledge of sensitive government-held information for financial or political gain or other malicious purposes.

Rwanda's legal framework for handling electronic evidence is primarily governed by Law n°68/2018 of 30/08/2018 on Electronic Messages, Electronic Signatures, and Electronic Transactions. While this Law provides a foundation for dealing with electronic evidence, its application to cybercrime cases presents complexities that must be addressed. The Law outlines provisions related to electronic signatures, messages, and transactions but lacks specific guidelines on the admissibility and authenticity of electronic evidence in criminal proceedings. The government of Rwanda established Law n°60/2018 of 22/8/2018 on the prevention and punishment of cybercrimes; it aims to prevent and punish cyber-crimes.[8] Regarding electronic evidence, the same law states, *"If the person holding*

[7] Lars Daniel: Digital Forensics—What Exactly Is Digital Evidence? *Forbes*, November 17, 2024, 04:11 PM EST. Updated November 17, 2024, 05:29 PM EST, https://www.forbes.com/sites/larsdaniel/2024/11/17/what-exactly-is-digital-evidence/.

[8] Article 1 of the Law n°60/2018 of 22/8/2018 on prevention and punishment of cybercrimes, Official Gazette n°Special of 25/09/2018.

data or the evidential value of data is not willing to cooperate in disclosure or preservation of data, the prosecution authority may seek a court order compelling such person to do so." In terms of authorization to employ a forensic method, the law also stipulates that: *"if the prosecution authority has reasonable grounds to believe that essential evidence cannot be collected without the use of the scientific method, it may request the court to order for the use of a forensic method. The order is valid for thirty days. Upon application made by the organ in charge of Prosecution, the court may extend that period for a further period of thirty days or to such other period as it considers necessary".*

Rwanda also established law n°24/2016 of 18/06/2016 governing information and communication technologies, which aims to develop a framework of Information and Communication Technologies (ICT) policy and regulation, with emphasis on promoting national Information and Communication Technologies policy objectives, establishing a licensing and regulatory framework in support of national policy objectives for the Information and Communication Technologies industry taking into account the convergence of technologies; establishing and strengthen the relevant institutions by providing them with the powers and procedures that are necessary for the implementation; establishing Rwanda as a major global center and hub for communications and multimedia information; promoting an information society for the enhancement of quality of both life and work and ensuring an equitable provision of affordable services over ubiquitous national infrastructure.[9]

Concerning the admissibility and evidential weight of electronic records, the same law in Article 14 states that: *"in any legal proceedings, an electronic record has admissibility and evidential value."* In terms of the admissibility of an electronic signature, the above-mentioned law in Article 146 states that: *"where it is required to have a signature of a person on an electronic record, an electronic signature has admissibility and evidential value in any legal proceedings if the method used indicates the originator of the record and that the originator approves the information contained in the record, and that method is reliable for the purpose for which the electronic record was generated or communicated, in the light of agreement."*

The law n°24/2016 of 18/06/2016 governing information and communication technologies aligns with *"the principle of equivalence"*, asserting that electronic evidence, encompassing emails, digital documents, social media posts, and various digital communications, should be treated on par with traditional forms of evidence like physical documents or witness testimony[10]. It emphasizes that

[9] Article 1 of the Law n°24/2016 of 18/06/2016 governing information and communication technologies, Official Gazette n°26 of 27/06/2016.

[10] Bradley Lawrence Schatz: *Digital evidence, representation, and assurance. Diss*. Queensland University of Technology, 2007. 30-32.

courts and legal systems should not unfairly disregard or dismiss electronic evidence solely based on its digital format.

3. Challenges in the legal framework for utilizing electronic evidence in cyber-crime in Rwanda

In the past two decades, a significant increase in interest in cyber crime has led to a substantial body of literature. However, there are notable gaps in this existing knowledge. For instance, there is a need for more accurate and valid data on the frequency, characteristics, and patterns of cyber-crime. Additionally, there is a lack of research on effective strategies for combating and preventing cybercrime[11]. In Rwanda, using electronic evidence in cyber crime cases presents various legal challenges. These challenges encompass legal, technical, privacy, and data protection aspects that must be carefully addressed to handle cyber-crime incidents effectively.

3.1. Legal challenges

Electronic evidence collection, admissibility, and authenticity in cybercrime cases present significant challenges. Matters such as the admissibility of digital evidence, chain of custody requirements, and ensuring compliance with international standards for electronic evidence are notable hurdles. The recent increase in cyber-crime has highlighted the critical importance of preserving electronic evidence, especially in countries like Rwanda, where legal frameworks must be adjusted to the digital era.

3.1.1. Issue relating to cyber-crime definition

Cyber-crime has yet to receive a unanimous definition, both nationally and internationally.[12] This lack of consensus on the concept originates from a myriad of definitions proposed on all sides by states and official international organizations, which confront several interests and systems. Classically, these definitions limit cyber-crime to the modus operandi of the cyber-offenders or the object of the

[11] Fawn T. Ngo – K. Jaishankar: Commemorating a Decade in Existence of the International Journal of Cyber Criminology. A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology*, 1/2017, 4-5.

[12] Charlie Plumb: Understanding the UN's New International Treaty to Fight Cybercrime. UN CPR, July 30, 2024. Available at: https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime.

offense. This is the case, among others, according to the framework established by the Organization for Economic Cooperation and Development (OECD), which, alluding to the processing or security of data, adopts cyber-crime as any unlawful, unethical, or unauthorized conduct relating to automatic data processing and data transmission.[13] Similarly, the United Nations also limits cyber-crime to attacks on the security of computer systems. Other definitions, particularly those of 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 that can be committed through a system.[14] In Rwanda, cyber-crime is not defined in the Penal Code, Criminal Procedure, or any other legal text, regardless of the fact that Law n°60/2018 of 22/8/2018 on prevention and punishment of cyber crimes mentions this term from start to finish.[15]

3.1.2.

Lack of legal provision on cybercrime under Rwandan Law relating to evidence and its productionRwandan Law n°15/2004 of 12/06/2004 relating to evidence and its production lacks a specific provision addressing electronic evidence under the Evidence and its Production Law of 2004. This Law applies to common offenses and cyber-crimes and does not explicitly cover electronic evidence. By recognizing this gap, an ongoing project has been started to revise the Law to incorporate provisions specifically addressing cyber-crimes. As we know, an electronic record has admissibility and probative value in any legal matter. An original electronic record is required to prove its content unless otherwise provided.

The requirement to produce the original electronic record is satisfied if the integrity of the electronic record system by or in which the electronic record was recorded or stored is proved or the integrity of an electronic record is proved or presumed. Under the current evidence law, an electronic record has no presumption of integrity.[16] At the same time, the competent organ may presume the integrity of an electronic record if the electronic record remains complete and unaltered except for the addition of any endorsement or any immaterial change that arises in the ordinary course of communication, storage, or display; the electronic record was certified or has been electronically signed by use of the

[13] OECD, Computer-Related Criminality. Analysis of Legal Politics in the OECD Area. 1986.

[14] Jacques Kabano – Jean Habarurema: Procedural Aspects of Cyber Crimes Investigations in Rwanda. A Comparative Study. *Makerere Law Journal*, 5/2023, 240–266.

[15] Law n°60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes, Official Gazette n° Special of 25/09/2018.

[16] Uniform Electronic Evidence Act 15A-1 (1998). Proceedings at page 77. https://ulcc-chlc.ca/ULCC/media/EN-Uniform-Acts/Uniform-Electronic-Evidence-Act_2.pdf.

method specified by an accredited certification entity; the integrity and content of the electronic record were notarized; the electronic record was recorded in a non-rewritable storage device or any other electronic means that do not allow alteration of the electronic records; the electronic record was examined and its integrity confirmed by an expert.

3.1.3. Lack of a comprehensive legislative framework to deal with electronic evidence

Rwanda grapples with a significant legal challenge due to a need for a comprehensive legislative framework tailored for electronic evidence in cyber-crime. Existing laws need to be updated, or there needs to be more specificity for addressing the complexities associated with cyber-crime and electronic evidence preservation. This gap can lead to confusion among law enforcement, judges, and other stakeholders as they navigate the intricacies of digital evidence. Jurisdictional issues pose another legal challenge.

3.1.4. Jurisdictional issues

Like many other nations, Rwanda grapples with the jurisdictional aspect of electronic evidence. This challenge is exemplified by the "Rwanda genocide trials", where electronic evidence played a pivotal role.

During the trials related to the 1994 Rwandan genocide, electronic evidence, including emails, digital photographs, and online communications, became crucial for establishing facts and prosecuting the perpetrators.[17] However, challenges emerged regarding jurisdiction when some of this electronic evidence was stored on servers outside Rwanda. This situation prompted questions about which legal framework should be applied to obtain and authenticate such evidence in Rwandan courts.

The jurisdictional challenge was compounded by the diversity of laws and regulations in different countries concerning the collection and admissibility of electronic evidence. Within the framework of Rwandan cyber Law, this case underscored the necessity for explicit guidelines on navigating jurisdictional issues when dealing with electronic evidence that extends beyond national borders.

3.1.5. Cross-border data access and sharing

In today's digital age, it is difficult to envision a criminal investigation that does not rely on digital evidence, considering that most of the world's information

[17] Allan Thompson (ed.): *The Media and the Rwanda Genocide*. London, Pluto Press, 2007. https://doi.org/10.2307/j.ctt18fs550.

is now stored in digital format.[18] Modern criminal evidence is not confined to digital formats; it also challenges traditional ideas of geographical boundaries and territorial jurisdiction.[19] Due to its international scope and intricate nature, cyber-crime poses substantial challenges that are hard for individual states to tackle independently[20]. With the widespread adoption of cloud computing, local storage in end-user devices has been replaced by remote storage. Consequently, data previously stored locally and accessible through domestic procedures is now frequently held by private companies and stored in jurisdictions beyond the investigating country's reach.

The process of seeking evidence across borders and dealing with jurisdictional limits in law enforcement is not recent. Governments have long established formal and informal cooperative arrangements to exchange evidence across borders while respecting each nation's territorial sovereignty. The Mutual Legal Assistance Treaty (MLAT) system, which relies on agreements between countries, sets out a formal procedure where one country can request assistance from another country to obtain evidence within its jurisdiction.[21]

The problem is that the advent of the Internet, particularly cloud computing, has disrupted the functioning of such a system of cross-border legal cooperation. As cross-border access to electronic evidence becomes familiar, it creates a unique jurisdictional conflict, as described by Andrew K. Woods. This situation arises when a criminal investigation typically confined to domestic borders now requires international cooperation.[22] Even in cases where the criminal investigation involves local suspects and victims, and the data belong to a citizen of the investigating country, authorities might still need diplomatic channels for cross-border legal cooperation.

[18] European Commission. *"Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying down Harmonized Rules on the Appointment of Legal Representatives to Gather Evidence in Criminal Proceedings." COM(2018) 225 Final - COM(2018) 226 Final - SWD(2018) 119 Final*, 14. Brussels: European Commission, 2018.

[19] IAPP. "The Globalization of Criminal Evidence." *International Association of Privacy Professionals*, 16 October 2018. https://iapp.org/news/a/the-globalization-of-criminal-evidence.

[20] Ikenga K. E. Oraegbunam: Jurisdictional Challenges in Fighting Cybercrimes. Any Panacea from International Law. *Nigerian Journal of International Law and Jurisprudence*, 6/2015, 57–65.

[21] Council of Europe: Convention on Cybercrime of the Council of Europe, opened for signature on November 23, 2001, in Budapest, Hungary, Council of Europe Treaty Series - No. 185.

[22] Jonah Force Hill – Matthew Noyes: *Rethinking Data, Geography, and Jurisdiction. Towards A Common Framework for Harmonizing Global Data Flow Controls*. New America and Cybersecurity Initiative, 2018. 32.

Rwanda has witnessed a surge in cyber-crime, which encompasses fraud, identity theft, and cyberstalking. Effectively combating these offenses requires law enforcement agencies to obtain electronic evidence stored internationally.[23] However, a cohesive legal framework for cross-border data access and sharing complicates this process. As discussed earlier, Rwanda has enacted several laws and regulations to tackle cyber-crime, offering a legal foundation for managing electronic evidence in criminal investigations and legal proceedings. Despite these measures, challenges emerge when accessing data in different jurisdictions. Infact, when the electronic evidence, vital to the investigation, is located on servers outside of Rwanda, that require collaboration and legal assistance from authorities in other jurisdictions. Obtaining and ensuring the admissibility of this evidence in Rwandan courts posed challenges due to differences in legal frameworks, data protection laws, and jurisdictional issues.

3.2. Technical challenges

Utilizing electronic evidence in cyber-crimes presents several technical challenges in Rwanda. These challenges arise from various factors, including the dynamic nature of technology, the necessity for specialized expertise, and the intricate nature of digital forensics.

3.2.1. Shortage of specialized equipment and expertise

Technical hurdles in preserving electronic evidence in developping countries like Rwanda arise from the shortage of specialized equipment and expertise. Law enforcement officers and forensic experts need more training and resources to handle and analyze digital evidence effectively.[24] This deficiency increases the risk of losing or contaminating critical evidence, potentially compromising case outcomes. The rapidly evolving nature of technology presents another technical challenge. The emergence of new devices and platforms provides cyber-criminals with new areas to exploit. This constant evolution makes it challenging for

[23] Minijust. "Law Enforcement Agencies Must Step Up by Enhancing Measures to Detect and Prevent the Cyber-Attacks from the Source." *9th Africa Working Group Meeting on Cybercrime for Heads of Units*, Kigali, Rwanda. https://www.minijust.gov.rw/news-detail/law-enforcement-agencies-must-step-up-by-enhancing-measures-to-detect-and-prevent-the-cyber-attacks-from-the-source.

[24] Scott H. Belshaw: Next Generation of Evidence Collecting. The Need for Digital Forensics in Criminal Justice Education. *Journal of Cybersecurity Education, Research and Practice*, 1/2019. https://files.eric.ed.gov/fulltext/EJ1341743.pdf.

Rwandan authorities to stay abreast of the latest cyber-crime trends and develop effective methods to preserve electronic evidence.

According to Wiles, ninety-seven percent of all high-tech crimes are estimated to go undetected[25]. It is not surprising, then, that officers assigned to investigate must possess specific knowledge and skills. Meyer and Short have proposed a job description for the ideal computer crime investigator.[26] The officer chosen to investigate computer crime should be an experienced, competent investigator with the ability to think analytically and a complete understanding of computer fraud-related laws and their application. The investigator should receive advanced training in computer crime investigation and be familiar with major operating systems. This investigator should develop professional contacts that would assist in conducting investigations.

The rapid advancements in technology and the evolving tactics of cyber-criminals necessitate that law enforcement agencies continuously update their technical tools and software, maintain current skills, conduct ongoing research, and develop effective countermeasures. Successfully investigating and prosecuting cybercrime requires individuals equipped with specialized skills and tools. However, the U.S. Government Accountability Office (GAO) has noted that the pool of qualified candidates remains limited.[27] Professionals tasked with investigating or examining cybercrime must possess unique law enforcement expertise and technical skills, including proficiency with various IT hardware, software, and forensic tools.[28] This talent scarcity creates significant challenges in recruiting such individuals, retaining them amidst competitive offers, and ensuring they remain updated on evolving technologies and increasingly sophisticated criminal techniques.

Additionally, the available technological infrastructure heavily influences the efficiency of employing electronic evidence in cybercrime investigations. In Rwanda, the lack of advanced technological infrastructure characterized by outdated or restricted forensic tools and software can impede the retrieval and analysis of electronic evidence from diverse devices. Enhancing capacity through targeted training and skill-building initiatives is essential to address

[25] Roger Wiles: *High-Tech Crime and Its Detection. A Comprehensive Study.* Cybersecurity Press, 2020, 189-230.

[26] John Franklin Meyer – Charles Short: Investigating Computer Crime. *Police Chief*, 5/1998, 28–35.

[27] United States Government Accountability Office. *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats.* Report to Congressional Requesters, GAO-07-705, June 2007. Accessed on December 28, 2024. https://www.gao.gov/assets/gao-07-705.pdf.

[28] Cyber Talents. "Cybercrime Investigation Tools and Techniques You Must Know". *Cyber Talents Blog.* Accessed December 28, 2024. https://cybertalents.com/blog/cyber-crime-investigation.

these challenges. Training programs must equip law enforcement personnel with the expertise required to adapt to technological advancements and effectively manage the complexities of modern cybercrime investigations.

3.2.2. Challenges relating to identifying electronic forgery

Electronic forgery is a notable technical challenge in Rwanda's use of electronic evidence. As the country experiences a surge in reliance on electronic evidence in legal matters, especially those related to cyber-crime and fraud, the detection of electronic forgery emerges as an intricate technical obstacle.[29] Addressing this challenge is imperative to upholding the credibility and admissibility of electronic evidence in Rwandan legal proceedings.

Detecting electronic forgery poses a significant challenge due to the advanced digital manipulation techniques available to perpetrators. The complexity of modern technology has made it more difficult to distinguish between authentic and falsified electronics. Perpetrators can access various tools to precisely alter digital documents, images, videos, and other electronic data. This complexity hinders law enforcement agencies and legal professionals from reliably detecting and proving instances of electronic forgery beyond a reasonable doubt.

An exciting email forgery occurred in the National Bank of Rwanda (NBR) when the Rwanda National Police ordered the reimbursement of the command of the uniform worn (of Rwanda Police personnel). The National Police forwarded an order of payment (ordre de payment n°0701/0750/O.P./13) to the NBR of 477.264 American dollars, which should be transferred to account n°0169-FT0517-050 of Indusind Bank in New Delhi to pay Alps International Exports (vendor). The NBR personnel in charge of the transfer received misleading information from the counterfeit email of the Alps International Exports director (rajsab992002@yahoo.com), who said that the account that should have been used in the money transfer changed to account n°0288000260017022 of DBS Bank in Singapore.

This forged email rajsab99202@yahoo.com of the criminal group called Enjreni Trading Ltd is confusing because it looks like the real email rajsab992002@yahoo.com of the director of Alps International Exports; the only difference is the "0", which has been placed before the number two. From this forged email message, the money was transferred via the account of the criminals said above, and after that, the real businessman (vendor) claimed that he did not receive the money.[30]

[29] Bernard Walumoli: *A Critical Analysis of the Challenges Facing Countercybercrime in 21st Century Africa: a Focused Comparison of Kenya and Rwanda. Diss*. University of Nairobi, 2021. 35-40.

[30] Nyarugenge Intermediate Court: Judgment in the case of Prosecution of Rwanda vs Bamporiki et al., Case No. RP 0527/13/TGI/NYGE of April 30, 2015.

It is a well-known fact that even if law enforcement agencies have done an excellent job investigating cyber-crime, at the litigation stage, the expertise of prosecution attorneys is still significant to secure the conviction of cyber criminals as it is incumbent on the Prosecution to prove his case beyond doubts; unfortunately, this is not the case as there is a dearth of savvy prosecutors in government justice departments.[31]

3.3. Privacy and data protection challenge

Balancing the need to access digital information while protecting individuals' privacy rights is a delicate matter that requires explicit legal provisions and safeguards. In Rwanda, safeguarding privacy and data is a fundamental right embedded in the nation's legal framework. The constitution of Rwanda, particularly in Article 23, explicitly ensures the right to privacy, proclaiming that *"The privacy of the home and correspondences is inviolable."* Moreover, Rwanda has implemented specific legislation, including Law N°30/2013 of 24/05/2013, that protects personal data.

While Rwanda prioritizes protecting privacy and personal data, challenges arise in obtaining and utilizing electronic evidence in cyber-crime cases. Due to the constraints imposed by privacy laws and data protection regulations, law enforcement agencies and judicial authorities may frequently confront hurdles in accessing electronic evidence. This becomes especially pertinent when evidence is stored on private devices or servers, potentially violating individuals' privacy rights.

The case of Nsabimana Callixte alias Sankara et al. vs. the Prosecution[32] has brought attention to the challenges of obtaining electronic evidence in cyber-crime cases in Rwanda. This particular case has sparked discussions regarding the adequacy of the legal framework that governs the acquisition and utilization of electronic evidence, along with concerns about the capabilities of law enforcement agencies to conduct effective investigations into cyber-crime incidents. Furthermore, the case underscores the crucial need to enhance Rwanda's legal framework by tailoring it to address cybercrime specifically and the collection of electronic evidence. This involves the formulation of comprehensive legislation, providing training and capacity-building programs for law enforcement and

[31] Peter A. Joy: Prosecution Clinics. Dealing with Professional Role. *Mississippi Law Journal*, 4/2005, 955–981. 955. https://heinonline.org/HOL/LandingPage?handle=hein.journals/mislj74&div=40&id=&page=.

[32] Court of Appeal of Rwanda: Judgment in the case of Sankara Callixte et al. vs. the Prosecution of Rwanda. Case No. RPA 00060/2021/C of April 4, 2022.

judicial officials, and investing in technological infrastructure to facilitate the collection and analysis of electronic evidence.

The issue of privacy rights and surveillance related to electronic evidence is also apparent in the same case. The interception of communications and monitoring of social media activities raise substantial privacy concerns, especially when introduced as evidence in criminal proceedings. This case has sparked discussions about the legality and ethical considerations surrounding the collection of electronic evidence through surveillance methods.

4. Lessons and best practices for Rwanda from some EU countries in the utilization of electronic evidence in cyber-crimes

Rwanda faces the challenge of effectively utilizing electronic evidence to address cyber crime cases, whether during investigation, prosecution, or adjudication. Drawing insights and lessons from the experiences of European Union (EU) countries can provide valuable guidance for Rwanda to enhance its strategies in handling electronic evidence. Some EU countries are advanced in legal frameworks, technological infrastructure, and expertise in addressing cybercrimes, justifying the relevance of this selection.

Indeed, numerous countries in the EU have established sophisticated systems and methodologies for employing electronic evidence in cybercrime cases.[33] By studying the experiences of specific EU countries such as Germany, the Netherlands, Sweden, Estonia, etc., Rwanda can acquire valuable insights in this crucial domain. This article will focus on four specific countries: Germany, the Netherlands, Sweden, and Estonia. This focus is chosen due to the practical limitations of analyzing all EU countries comprehensively.

4.1. Germany

Germany has made substantial progress in utilizing electronic evidence to counter cyber crimes. The nation has set up dedicated cyber-crime units within law enforcement agencies equipped with advanced technological capabilities for

[33] Adam Juszczak – Elisa Sason: The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. An Introduction to the New EU Package on E-evidence. *Eucrim*, 2/2023, 182–200. https://doi.org/10.30709/eucrim-2023-014.

managing electronic evidence.[34] Rwanda can benefit from Germany's focus on specialized training for law enforcement personnel, ensuring their effectiveness in collecting, analyzing, and presenting electronic evidence in court.

4.2. The Netherlands

The Netherlands is actively working to address challenges related to electronic evidence in cyber-crime investigations by promoting partnerships between law enforcement, technology experts, and academia.[35] Rwanda can benefit from adopting a similar strategy, fostering collaboration and knowledge exchange among multiple stakeholders to handle electronic evidence more effectively.

4.3. Sweden

Swede has placed a significant emphasis on investing in research and development to advance cuttin-edge technologies for digital forensics and the analysis of electronic evidence.[36] Rwanda can benefit from studying Sweden's initiatives, which highlight the importance of staying updated on emerging trends and advancements in digital forensics tools and techniques to address cyber-crimes effectively.

4.4. Estonia

Estonia serves as a model for the effective utilization of electronic evidence in combating cybercrime, showcasing a robust legal and technological framework. As a highly digitalized nation, Estonia has implemented advanced e-governance systems that integrate secure digital signatures, blockchain technology, and interoperable databases, ensuring the authenticity, integrity, and admissibility

[34] Nikolaus Forgó et al.: The Collection of Electronic Evidence in Germany. A Spotlight on Recent Legal Developments and Court Rulings. In: Marcelo Corrales – Mark Fenwick – Nikolaus Forgó (eds.): *New Technology, Big Data, and the Law*. Singapore, Springer, 2017. 251-279.

[35] Sander Veenstra et al.: Fighting Crime in a Digitized Society: The Criminal Justice System and Public-Private Partnerships in the Netherlands. In: Wouter Stol – Jurjen Jansen (eds.): *Cybercrime and the Police.* , Hague, Eleven International Publishers, 2013. 75-87.

[36] Maria Stoyanova et al.: A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 2/2020, 1191-1221.

of electronic evidence.[37] Its Cybersecurity Strategy emphasizes public-private partnerships, enabling seamless cooperation between law enforcement, technology companies, and judicial authorities in handling digital evidence. Estonia's adoption of the European Union's directives on electronic evidence, coupled with specialized cybercrime units and training for legal professionals, strengthens its capacity to address complex cybercrimes.[38] These practices offer valuable lessons for Rwanda, particularly in leveraging technology to enhance the collection, preservation, and presentation of electronic evidence within a clear legal framework.[39] This approach allows for a more efficient and knowledgeable handling of cyber-crime cases within the European Union.

5. Potential legal solutions for the efficient use of electronic evidence in cyber-crime within the Rwandan legal framework

The effective utilization of electronic evidence plays a pivotal role in the successful prosecution and adjudication of cyber-crimes. To enhance this aspect, the Rwandan legal framework can explore various potential legal solutions to ensure the efficient use of electronic evidence in the fight against cyber-crime.

5.1. Strengthening legal provisions for electronic evidence

One potential legal solution involves reinforcing the legal provisions on electronic evidence within the Rwandan legal framework. This may entail the creation of specific legislation addressing the admissibility, authenticity, and reliability of electronic evidence during court proceedings. By explicitly outlining the criteria for admitting electronic evidence and establishing protocols for its collection, preservation, and presentation in court, the legal framework can offer clear guidance and direction for law enforcement agencies and judicial authorities.

[37] Republic of Estonia, Information System Authority. *Cybersecurity in Estonia 2020.* Accessed on December 28, 2024. https://ria.ee/en/news/cyber-security-estonia-2020.

[38] Cyber Security in Estonia 2020 explains the landscape, the responsibilities and activities of different public sector organizations in Estonia who all contribute to keep Estonians safe online. From setting up a cyber security standard to combating cyber crime to training military cyber defence operators, every agency has a vital role to play.

[39] Heli Tiirmaa-Klaar et al.: Botnets, cybercrime and national security. In: Heli Tiirmaa-Klaar et al. (eds.): *Botnets*. Springer, 2013.1-40.

5.2. International cooperation and mutual legal assistance

International cooperation and mutual legal assistance can help Rwanda overcome challenges related to the efficient use of electronic evidence in cyber-crime within its legal framework. This can be done by exploring ways of international cooperation and mutual legal assistance in handling electronic evidence related to cyber-crimes. Establishing formal mechanisms for cooperation with other countries in areas such as data sharing, cross-border investigations and extradition of cyber criminals can significantly enhance Rwanda's ability to access electronic evidence stored outside its jurisdiction.[40] This can be achieved through bilateral or multilateral agreements that facilitate the exchange of electronic evidence while respecting data privacy and human rights considerations. Some benefits of international cooperation include:

5.2.1. Sharing of best practices

In Rwanda, the exchange of effective strategies to combat cyber-crimes is a critical element in tackling the increasing threats in the digital sphere. The nation has actively participated in regional and global efforts to strengthen cybersecurity measures and responses to cyber-crime. An example of this involvement is Rwanda hosting the 9th Africa Working Group Meeting on Cyber-Crime for Head of Units (AF-WGM) organized by INTERPOL. This event signifies Rwanda's commitment to collaborating with international partners and implementing best practices in addressing cyber threats. Collaboration with other countries allows Rwanda to learn from their experiences and implement best practices in handling cyber-crime cases.

5.2.2. Access to technical expertise

Partnering with countries possessing strong technical expertise presents a valuable opportunity for Rwanda to enhance its capacity to gather electronic evidence from digital devices and online platforms. Through knowledge transfer, capacity-building initiatives, access to advanced tools, international collaboration, enhanced credibility, legal framework alignment, resource allocation planning, and sustainability efforts, Rwanda can strengthen its capabilities in digital investigations and cyber-security.

[40] Roger Généreux Ishimwe: *Critical analysis on the impact of cybercrimes on intellectual property rights under Rwanda legal framework*. Kigali Independent University ULK, 2024. Available at: http://drepository.ulk.ac.rw:8080/xmlui/bitstream/handle/123456789/362/CRITICAL%20ANALYSIS%20ON%20THE%20IMPACT%20OF%20CYBERCRIMES.pdf?sequence=1&isAllowed=y.

5.2.3. Strengthening legal frameworks

Many types of crime, including terrorism, trafficking in human beings, child sexual abuse, and drug trafficking, have moved online or are facilitated online. As a consequence, most criminal investigations have a digital component.[41] Collaboration with other countries can help Rwanda update its legal framework to address cyber-crime better and improve the acquisition and admissibility of electronic evidence.

5.2.4. Enhancing cross-border cooperation

Cyber-criminals often operate from jurisdictions where they believe they can evade detection or prosecution. In such situations, international cooperation becomes essential to ensure that justice is served effectively. International cooperation enhances the fight against cyber-crime by sharing information and evidence. This collaboration allows law enforcement agencies to pool their resources and expertise to investigate and prosecute complex cyber-crime cases that may involve multiple jurisdictions. For instance, Rwanda may need assistance from foreign experts to analyze digital evidence or trace the origin of an attack. By working together, law enforcement agencies can increase their chances of identifying and apprehending cyber-criminals.

Moreover, international treaties and agreements provide a legal framework for cross-border cooperation in cybercrime investigations. For example, the Council of Europe's Convention on Cyber-Crime, known as the Budapest Convention, sets out specific provisions for mutual legal assistance and extradition in cyber-crime cases. The United Nations Convention on Transnational Organized Crime also includes provisions for addressing cyber-crime. These treaties help ensure that countries follow established procedures when requesting assistance from each other in cyber-crime investigations[42].

International cooperation can facilitate the exchange of information and evidence between countries, making it easier for Rwandan authorities to work with their foreign counterparts in investigating and prosecuting cyber- crime cases.

[41] Anita Lavorgna: *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes. Doctoral Thesis*. University of Trento, 2014. https://iris.unitn.it/handle/11572/368968.

[42] United Nations Office on Drugs and Crime (UNODC) (2020). *Global Cybercrime Report 2020.* https://www.unodc.org/global/publications/2020/e38547_global_cybercrime_report_2020.pdf.

5.3. Promoting public awareness and collaboration

Cyber-crimes' complex and evolving nature necessitates a collaborative strategy that engages various stakeholders. This strategy leverages diverse entities' expertise, resources, and authority, enabling them to cooperate in sharing information, advancing technology, and developing impactful policies. This multi-stakeholder approach strives to address cyber-crimes and comprehensively protect citizens' digital rights through united endeavors.

Enhancing public awareness about the importance of electronic evidence in combating cyber-crimes is crucial. Collaborative efforts involving government agencies, private sector entities, academic institutions and civil society organizations can raise awareness about cyber security risks, digital hygiene practices, and reporting mechanisms for cyber incidents. By fostering a culture of collaboration and information sharing, Rwanda can create a supportive environment for effectively leveraging electronic evidence to address cyber threats. This collaboration can lead to several benefits in addressing the challenges of electronic evidence in cyber crimes within the Rwandan legal system:

5.3.1. Improved capacity to investigate and prosecute cyber-crimes

Collaboration enables the sharing of resources, expertise, and technology, which can significantly enhance the capacity of law enforcement agencies to investigate and prosecute-cyber-crimes. By sharing resources, exchanging expertise, and integrating technology, these agencies can enhance their collective ability to combat the growing menace of cyber threats. Through coordinated efforts and mutual support, law enforcement can stay ahead of cyber-criminals and ensure a safer digital environment for individuals and organizations worldwide[43].

5.3.2. Enhanced cyber-security

Enhanced cyber-security through collaboration is crucial in combating the ever-evolving landscape of cyber threats. By leveraging collective expertise, resources, and innovation capabilities through collaborative initiatives, stakeholders can strengthen their defenses and better protect individuals and critical infrastructure from malicious cyber activities[44]. Collaboration can lead to the development of advanced cyber-security solutions that protect citizens and critical infrastructure from cyber threats.

[43] Federal Bureau of Investigation: Cyber Security Incident Management: Collaborating with Law Enforcement 2024, https://moldstud.com/articles/p-cyber-security-incident-management-collaborating-with-law-enforcement/pdf.

[44] Ibid. 33.

5.3.3. Strengthened legal framework. Collaboration can contribute to developing a robust legal framework that addresses the challenges of electronic evidence in cyber-crimes, including the admissibility of digital evidence in court. Collaboration among various stakeholders is indispensable for developing a robust legal framework that effectively addresses the challenges associated with electronic evidence in cybercrimes. By leveraging collective expertise, fostering cross-disciplinary partnerships, ensuring international cooperation, and promoting innovation, stakeholders can enhance legal practices related to digital evidence admissibility and strengthen the overall response to cyber threats[45].

5.3.4. Increased public awareness and trust

Collaboration among various stakeholders, including government agencies, law enforcement, cyber-security experts and the public, is crucial in raising awareness about cyber crimes and the importance of reporting such incidents. By working together, these entities can educate the public about the risks associated with cyber threats, the methods used by cyber-criminals and the potential impact of these crimes on individuals, businesses, and society as a whole[46]. Collaboration can also raise public awareness about cyber crimes and the importance of reporting such incidents, leading to increased confidence in the legal system and its ability to address these challenges.

5.4. Establishing digital forensics units

Establishing specialized digital forensics units within law enforcement agencies or judicial bodies is an essential step in establishing digital forensics units. These units can be equipped with the necessary expertise and technology to effectively collect, analyze, and present electronic evidence in cyber-crime investigations and court proceedings[47]. By investing in training programs and technological resources for digital forensics, Rwanda can enhance its capacity to handle electronic evidence in a manner that meets international forensic investigation standards.

[45] Council of Europe 2020, 31.

[46] Joanna Curtis – Gavin Oxburgh: Understanding cyber-crime in 'real world' policing and law enforcement. *The Police Journal*, 4/2023, 573–592. https://doi.org/10.1177/0032258X221107584.

[47] United Nations Office on Drugs and Crime: Establishing specialized digital forensic units within law enforcement agencies or judicial bodies 2019, https://www.unodc.org/documents/organized-crime/Publications/UNODC_Digital_Forensics_Handbook.pdf.

5.5. Capacity Building and Training

Capacity-building and training programs are essential for legal professionals, law enforcement officers, and judicial personnel handling electronic evidence. Comprehensive training on digital forensics, cyber-crime investigation techniques, and the legal aspects of electronic evidence can improve the competence of relevant stakeholders in dealing with complex cyber-crime cases. Additionally, continuous professional development initiatives can keep them abreast of evolving technologies and best practices in managing electronic evidence[48].

5.6. Creation of Specialized Cybercrime Courts

The criminal landscape has evolved with the advancement of technology, giving rise to a surge in cyber crimes. These crimes often involve electronic evidence and present unique investigation, prosecution, and adjudication challenges. While Rwanda has specialized courts for specific matters such as commerce, family and minors, economic crimes, and administrative labor cases, there must be a more significant gap in addressing cyber crimes.

Introducing specialized cybercrime courts is a potential legal solution to tackle the hurdles of using electronic evidence in Rwandan cyber-crime cases. Drawing inspiration from the best practices, such as those implemented in Estonia, these dedicated courts could feature judges with specialized knowledge in handling cyber-related cases. This approach ensures that electronic evidence is thoroughly assessed and effectively incorporated into the legal system.

6. Conclusion

This paper emphasizes the importance of effectively utilizing electronic evidence in addressing cybercrime within Rwanda's legal framework. Electronic evidence, stored on computers, smartphones, and other digital devices, plays a pivotal role in uncovering cyber-crimes' nature, scope, and perpetrators. Leveraging this evidence is essential for building strong cases and ensuring offenders are brought to justice.

A comprehensive, multi-faceted approach is necessary to address the challenges of integrating electronic evidence into Rwanda's legal processes. This includes

[48] Ibid. 14.

enacting specific legislation to guide the collection, storage, and presentation of electronic evidence in a manner that aligns with international best practices. Additionally, establishing digital forensic standards and providing specialized training for law enforcement, judges, and legal practitioners are crucial for effectively enhancing their capacity to handle electronic evidence in cybercrime cases. One of the key measures proposed is the creation of specialized cybercrime courts equipped with judges, prosecutors, and investigators trained in digital forensics and cybercrime investigations. These dedicated courts would have the expertise and authority to adjudicate cases involving hacking, online fraud, data breaches, and other cyber offenses, ensuring that legal proceedings meet both domestic and international standards. This approach would expedite the adjudication of cybercrime cases and foster the development of a deep pool of expertise in handling electronic evidence within the judicial system.

Moreover, the establishment of dedicated cybercrime units within law enforcement agencies, supported by advanced technological tools, will significantly enhance Rwanda's capacity to detect, investigate, and prosecute cybercriminals. Through cooperation with international partners, Rwanda can facilitate cross-border investigations and share vital intelligence on emerging cyber threats, further strengthening its ability to combat global cybercrime.

The paper highlights the need for a holistic strategy combining legal reforms, technical advancements, specialized training, and international collaboration to enhance Rwanda's capacity to combat cybercrime by effectively utilizing electronic evidence. By adopting these critical measures, Rwanda will improve its response to cyber threats and contribute to fostering a more secure and resilient digital environment, both nationally and globally. These reforms will ensure that Rwanda remains at the forefront of efforts to combat cybercrime in the digital age.

Bibliography

Scott H. Belshaw: Next Generation of Evidence Collecting. The Need for Digital Forensics in Criminal Justice Education. *Journal of Cybersecurity Education, Research and Practice*, 1/2019. https://files.eric.ed.gov/fulltext/EJ1341743.pdf.

Bernard Walumoli: *A Critical Analysis of the Challenges Facing Countercybercrime in 21st Century Africa: a Focused Comparison of Kenya and Rwanda. Diss.* University of Nairobi, 2021.

Nikolaus Forgó et al.: The Collection of Electronic Evidence in Germany. A Spotlight on Recent Legal Developments and Court Rulings. In: Marcelo Corrales – Mark Fenwick – Nikolaus Forgó (eds.): *New Technology, Big Data, and the Law*. Singapore, Springer, 2017. 251-279.

Jonah Force Hill – Matthew Noyes: *Rethinking Data, Geography, and Jurisdiction. Towards A Common Framework for Harmonizing Global Data Flow Controls*. New America and Cybersecurity Initiative, 2018.

Ki Hong Steve Chon: *Cybercrime precursors. Towards a model of offender resources. Doctor of Philosophy dissertation*. Australian National University, 2016.

Roger Généreux Ishimwe: *Critical analysis on the impact of cybercrimes on intellectual property rights under Rwanda legal framework*. Kigali Independent University ULK, 2024. Available at: http://drepository.ulk.ac.rw:8080/xmlui/bitstream/handle/123456789/362/CRITICAL%20ANALYSIS%20ON%20THE%20IMPACT%20OF%20CYBERCRIMES.pdf?sequence=1&isAllowed=y.

Adam Juszczak – Elisa Sason: The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. An Introduction to the New EU Package on E-evidence. *Eucrim*, 2/2023, 182–200. https://doi.org/10.30709/eucrim-2023-014.

Peter A. Joy: Prosecution Clinics. Dealing with Professional Role. *Mississippi Law Journal*, 4/2005, 955–981. https://heinonline.org/HOL/LandingPage?handle=hein.journals/mislj74&div=40&id=&page=.

Jacques Kabano – Jean Habarurema: Procedural Aspects of Cyber Crimes Investigations in Rwanda. A Comparative Study. *Makerere Law Journal*, 5/2023, 240–266.

Bradley Lawrence Schatz: *Digital evidence, representation, and assurance. Diss*. Queensland University of Technology, 2007.

Anita Lavorgna: *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes. Doctoral Thesis*. University of Trento, 2014. https://iris.unitn.it/handle/11572/368968.

Ronald Serwanga: *Legal mechanisms for enforcing electronic transactions in Rwanda. Diss.* University of Rwanda, 2019.

Maria Stoyanova et al.: A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 2/2020, 1191-1221.

Allan Thompson (ed.): *The Media and the Rwanda Genocide*. London, Pluto Press, 2007. https://doi.org/10.2307/j.ctt18fs550.

Heli Tiirmaa-Klaar et al.: Botnets, cybercrime and national security. In: Heli Tiirmaa-Klaar et al. (eds.): *Botnets*. Springer, 2013.1-40.