International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 10-11-2023, Accepted: 25-11-2023, Published: 11-12-2023
Volume 9, Issue 6, 2023, Page No. 189-195

An assement of aplicability of the cybercrime act no.14 of 2015 in Zanziabar

Noman Thabit Noman[1*], Sikujua Omar Hamdan[2]
[1] Faculty of Law, Zanzibar University, Zanzibar
[2] Lecturer of Law, Faculty of Law, Zanzibar University, Zanzibar

Abstract
The study investigated the applicability of the Cybercrime Act No.14 of 2015 in Zanzibar. The research objectives were to; examine Existence of Cybercrimes in Zanzibar, examine the Nature and Scope of the Cybercrime Act no 14 of 2015 in Tanzania, examine the Legal Frameworks on a Cybercrime Laws in Zanzibar, assess the applicability of the cyberlaws in Zanzibar and to suggest and recommend on applicability of Cybercrime Act No. 14 of 2015 in Zanzibar. A research design was used in this study is qualitative approaches. The research used a sample of 30 respondents. Purposive sampling was used. Method of data collection was by interviews. Qualitative data was analyzed through descriptive way. Findings of the study revealed that it is an indisputable fact that, the researcher was able to find answers that were different from his idea, but his concern was real, because according to this research he was able to discover that, an Act since the day of enactment in 2015 were not used in Zanzibar up to 2022 that was stated to use it. The researcher concluded that, the ratification information for the Cybercrime Act No. 14 of 2015 has not been officially announced, the study recommends that in Publication of Laws of Cybercrime, Amendment of Penal Act No.6 of 2018 and Cybersecurity training by enforcement agencies.

Keywords: Cybersecurity, legal frameworks, cybercrime laws, Zanzibar

Introduction
The issue of cybercrime in Zanzibar is an alarming situation. There are different common types of cybercrime in Zanzibar, such as pornography, cyber defamation, forgery, and cyber bullying, which are committed in Zanzibar and distributed to the Zanzibar community. In this study, therefore, the researcher shows and studies the existing laws on cybercrime and traces out the specific laws dealing with cybercrime in Zanzibar. It also shows the extent of Zanzibar laws in controlling cybercrime. The research traces out the Cybercrime Act No. 14 of 2015 in Tanzania and its effects and application in Zanzibar. Additionally, the researcher traced out the tools used to combat cybercrime in Zanzibar and their effectiveness.

Historical background of the Study
Zanzibar is a country with internal authority to administer its affairs. As preserved in Sections 1 and 2 of the Constitution of Zanzibar, it states that:

"Zanzibar is a country whose border area is the entire area of the islands of Unguja and Pemba as well as the small islands that surround it and its sea, which was known as the Republic of the people of Zanzibar before the union of Tanganyika and Zanzibar".

For more than 200 years, Zanzibar was ruled by colonials who came from far away from the African continent. Zanzibar was administered by two colonials, the Arab kings of Oman and the United Kingdom, which at that time was known as Great Britain.
Since the colonial period, the development of information and communication technology has begun to arise in Zanzibar. Although it did not rise as big as it did in European countries at that time, there are a number of laws that are enacted in order to regulate people due to the development of technology and punish criminals who violate the freedom of using technology. It is remembered that in the 1930's, the colonial government introduced the Post Office in Zanzibar, which was used to send and receive different documents in a short period of time. Due to this process using electronic means and highly secrecy, it was feared some people could use it to plan different criminal activity. The colonial government decided to exact a law known as the Postal Office Decree No. 66 of 1936. The colonial government created this law with special provisions to regulate citizen behavior because this office would deal with sensitive information about citizens. For example, Section 25 [1] of this law gave the postmaster the authority to open documents if something was thought to be against the law.
In the 1930s in Zanzibar, various newspapers were established with the goal of transmitting messages to citizens. The colonial government of that time decided to enact the law, which was known as Newspaper Decree No. 156 of 1938. This law set up guidelines to reduce pollution and false news writing in order to ensure that people did not abuse their freedom of expression.
Cinema is a place of enjoyment, it is a place that requires great privacy, in this area of enjoyment videos, pictures and various publications are shown. Because various performances are shown in those Cinema areas, anything can happen, so the colonial government decided to enact The Stage Play and Cinematograph to preserve evil things in check. Under Section 10 of this Law, it said

"Showing movies without the permission of Cinema Matters Authority officials was strictly prohibited by law".

Sections 13, 23, and 26 of this Decree give the cinema the authority to enter and examine any films brought here.

Additionally, they granted the cinema the right to censor any films that were considered immoral or threatened the safety of their government at the time.

After Zanzibar gained its independence through a revolution, technological development was still very low, and they continued to use the same colonial systems, but by the 1980s, many African countries had started to enter the systems of democratic reform and globalization.

Tanzania, particularly in Zanzibar, had entered into multi-party politics in the 1990s. At that time, technology had begun to grow up, and people had started to violate the principles of freedom of opinion and expression due to the development of technology. That scenario led the Government of the United Republic of Tanzania, in relations with the Government of the Revolution of Zanzibar, to decide to fight against those people who were using the development of technology as a loophole to commit a different crime. They started creating the laws that were going together with the new technology phenomenon.

The Following the terrorist attacks in Tanzania and Kenya in 1998 and also in New York in the United States in September 2001 carried out by the Al-Qaeda terrorist group and resulting in the deaths of over 3000 people in the commercial buildings of the World Trade Center, many countries concentrated on increasing intelligence and search, particularly on various people's communications, and since Tanzania was a victim of terrorism in 1998, they decided to introduce a law called the Prevention of Terrorism Act, Cap. 19 of 2002. This law contains various offenses that look similar to the Cybercrime Act.

Even though the governments of URT and RGZ enacted a harsh law aimed at combating various offenses that emerged due to the development of technology from the 1990s to the 2000s, the number of cyber offenses has increased. It's agreeable that, at the beginning of the 21st century, the development of science and technology was rapid; the use of electronic devices such as mobile phones, computers, and different software's was increased a lot, even to the point of causing a new crime of connecting with computers.

In 2003, the Government of Tanzania decided to amend Tanzania's communication law of 1993, and created a new Act known as Tanzania communication regulatory authority The aim of this Act was to up to regulating the commination and any means of technologies, TCRA regulating all mobile network in Tanzania, broadcasting and any kind of social media.

From 2005 to 2010, it can be said that it was the fourth stage of the development of information and communication technology in Tanzania. Various social networks were invented in the world during those years, and because Zanzibar and Tanzania in general are not villages, they entered the world directly to join other countries in the use of information and communication technology, particularly social networks.

Although the advancement of information and communication technology has greatly aided various countries in developing, it has also become a major source of crime, giving rise to a new crime known as cybercrime.

From 2010 to 2015, cybercrime in Zanzibar started to develop, and the crime that took place seemed to destroy the honor of people in the community by insulting and humiliating people through networks such as Facebook, Twitter, and WhatsApp, and criminals have been Using networks, which is also based on distributing sexual pictures, also emerged in the style of taking sexual pictures and posting them on social networks. Cybercriminals were committing crimes to get money, which, for that reason, made a researcher decide to conduct research on the topic of the Assessment of Applicability of Cybercrime Act No. 14 of 2015 in order to bring a better solution.

Research Methodology

The researcher used qualitative design as a methodology for obtaining different types of information. The methods used specify how the information's were collected, what type of information was collected, and how the information was analyzed and displayed in order to put the other required thesis in an understandable way. Also, the researcher was using primary and secondary methods for collecting different data. Examples of primary sources used by a researcher are legislation and decrees, court cases, text books, articles, and journals, while secondary sources are websites and reports.

1. Study area

The study area of the research is Zanzibar, in the Urban West Region.

Sample population and Sample size

These studies targeted 30 persons from different institutions, which included three staff from a judicial office (3), three staff from the DDP office (3), five police personnel from the department of the police force in Zanzibar (5), four staff from the Attorney General's Office in Zanzibar (4), five people from the House of Representatives in Zanzibar (5), three staff from the Law Review Commission of Zanzibar (3), two staff from the TCRA head office in Zanzibar (2), two advocates from different chambers, and three local persons.

The researcher used different methods as means of collecting data. In order to obtain the information required, data were gathered using various methods, as follows:

2. Interviews

In this study, both structured and unstructured interviews were used to collect data. The goal of using this approach was to gather enough reliable information from the legal documents and respective persons in any format deemed useful.

3. Data analysis

The data are gathered from both organized and unstructured interviews and then analyzed using the descriptive method. The researcher similarly employed various sections from different pieces of legislation to address the entire subject of cybercrime.

Legal Framework on Cybercrime Laws in Zanzibar

1. The Zanzibar ICT Policy of 2013

The general objective of Zanzibar information and communication technology policy was to provide a reference framework for the harmonious and sustainable development of the ICT sector in Zanzibar, constituting the main base for legislation, development plans, and action in the future. And the specific objectives of the Zanzibar ICT Policy were to transform Zanzibar into an information-based society where everyone has equitable and affordable access to ICT and to ensure that ICT is part of national education

programs. To have a trusted and secure information infrastructure and a culture of cyber security at all levels of society to improve efficiency and transparency in the civil service and to have an enabling legal and institutional environment that ensures the growth and development of the ICT sector. Use ICT to create an enabling and conducive environment for the promotion of investment, the provision of health services, and the development of a vibrant and sustainable economy.

1.1 Challenges on Legal and Regulatory Framework of Zanzibar ICT Policy of 2013

Lack of Legal frameworks to provide enabling environment for development and provision of e-services, due to the development of science and technology, the demand of services from the difference institution increased to a great extent, the only way to solve those things, was for the government to enter the whole issue of e-service use.

E-services (electronic services) are services which make use of information and communication technologies (ICTs). The three main components of e-services are: service provider; service receiver; and the channels of service delivery (i.e., technology). For example, with respect to public e-service, public agencies are the service provider and citizens as well as businesses are the service receiver. For public e-service the internet is the main channel of e-service delivery while other classic channels (example telephone, call center, public kiosk, mobile phone, television) are also considered.

Increase of cyber-crime around the world. The growth of technology from the use of analogies to digital things made many things to be easier in the world, but at the same time cybercriminals used that opportunity to commit various types of crimes, so the Government of Zanzibar decided to come up with an ICT Policy especially in the field of laws to combat such crimes.

1.2 Strategies examined under Zanzibar ICT Policy of 2013

Due to the development of technology, there was an increase in the use of computers and various systems that brought productivity to the nation, and on the other hand, it became the source of an increase in criminal activities, so the government decided to introduce a policy in 2013 with the following strategies:

To establish a legal framework that addresses issues catering for computer and computer related crime, consumer protection, child's protection, data protection, privacy protection, intellectual property rights, dispute resolution and security from the organizational to an individual level. To review the existing legislations, taking consideration of international best practices, to foster a clear and supportive legal framework that promotes and supports the long-term development of the ICT sector. To provide training for the existing legal practitioners on ICT regulatory issues, including law enforcement agencies. To encourage a local training institution to provide courses related to ICT legal matters. To establish and operationalize e-justice to enhance judicial systems and cater for efficient and effective cases management and others day to day activities.

One of the effects of Zanzibar's ICT policy of 2013 led the Zanzibar government to make various major amendments to the different laws in order to comply with the requirements of Zanzibar's ICT policy of 2013. Among the acts that were amended or repealed in order to comply with the policy are as follows:

2. The Penal Act No. 6 of 2018 in Zanzibar.

The Penal Act is a special law enacted to classify various types of offenses and their punishments. This Act was enacted in 2018, which is the successor to the repealed Penal Act. This Act was enacted after the Zanzibar ICT Policy required improvements to some of the various laws, including the Penal Act. In this amendment, The Penal Act had elements of cybercrime which were found from section 372 to 381, making the total number of offenses mentioned in that part to be 10. The Penal Act no 6 of 2018 came to adopt and make amendments to some elements from the repealed Penal Act No.6 of 2004. Among the things that have been changed are offenses related to computer related crime from being Part 38 of the Act to being Part 35 of the Act, as well as the new Act removed the offense of trademarks from being an offense of computer related crime and become a regular crime. The offenses of computer-related crime (cybercrimes) that fall under Penal Act No. 6 of 2018 are as follows:

Offences against intellectual property result from any person's creativity and ideas. Such rights can exist in a book, a brand, an invention, a design, or a song. This. Under the criminal law, certain uses of copyright, registered designs, or trademarks without the owner's permission can amount to a criminal offense. These are often referred to as piracy, for a copyright infringement; intentional copying for registered designs; and counterfeiting, for a trade mark infringement. The intellectual property crime is one of the cybercrimes, and in the case of Zanzibar, this offense is found in the Penal Act in the section 369 which is illustrated as follows:

"A program, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network, commits an offence, if the offence is against, intellectual property, then the offender is guilty of an offence and is liable to imprisonment for a term of not exceeding five years, if the offence is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of an offence and is liable to imprisonment for a term of not exceeding ten years".

Offenses against computer equipment or supplies: this is an offense against computer equipment or supplies where a person's intentional modification or destruction, without consent, of computer equipment or supplies used or intended to be used in a computer, computer system, or computer network. as illustrated in the section of 370 and explained as follows:

"A person who willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network, commits an offence against computer equipment or supplies, and is liable to imprisonment for a term of not exceeding five years. If the offence is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of an offence and is liable to imprisonment for a term not exceeding ten years".

Offences of destruction of computer equipment, in order to prove destruction of computer equipment, the state must prove that the defendant recklessly or intentionally tampered with equipment used in a computer system without authorization. This might happen to a computer in a store, or it might happen to a computer that is someone else's private property. as defined in section 371 as follows.

"A person who willfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offence against computer equipment or supplies, and is liable to imprisonment for a term of not less than three years but not exceeding ten years".

Offences of interfering with data: this is the act of deleting, damaging, deteriorating, altering, or suppressing digital data on an information system or rendering such data inaccessible; it also includes theft of data, funds, economic resources, or intellectual property.
Section 372 Elaborate that;

"A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts; destroys or alters data, renders data meaningless, useless or effective, obstructs, interrupts or interferes with the lawful use of data, obstructs, interrupts or interferes with a person in the lawful use of data, or denies access to data to a person entitled to it commits an offence punishable, by imprisonment for a term not exceeding five years, or a fine not exceeding Five Million Shillings, or both".

In the case *of Guster Nsubu and Robinhoood Byamukama v Uganda*, The appellant and 2 others were indicted on 6 counts under the Computer Misuse Act, 2011 (CMA) and the East African Community Customs Management Act, 2009 (EACCMA) They were indicted in count 1 with unauthorized use and interception of computer services contrary to sections l5(l) and section 20 of the Computer Misuse Act 2011 in count 2 with electronic fraud contrary to section 19 of the Computer Misuse Act, 2011, in count 3 with unauthorized access to data contrary to Sections l2(2) and 20 of the Computer Misuse Act, 2011, in count 4 with producing' selling or procuring, designing an being in possession of devices, computers, computer programs designed to overcome security measures for protection of data contrary to Section l2(3) and 20 of the Computer Misuse Act, 2011, in Count 5 with unauthorized access to a customs computerized system contrary to Section 191 (1) of the East African Community Customs Management Act, 2009 and in count 5 with fraudulent evasion of payment of duty contrary to section 203(e) of the East African Community Customs Management Act,2009.
The appellants had been charged in 2012 and were sentenced in 2013, The matter then went on appeal and the Court of Appeal ordered a retrial.
Offences of interfering with computer systems, according to Article 5, define offenses of interfering with data as serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data. And according to section 373 Illustrated that;
"A person who intentionally or recklessly, without lawful excuse or justification hinders or interferes with the functioning of a computer system, or hinders or interferes with a person who is lawfully using or operating a computer system commits an offence punishable, by imprisonment for a term of not less than one year but not exceeding five years or a fine not less than One Million Shillings but not exceeding Five Million Shillings or both".
Offences of illegal interception of data: this is the crime whereby a person committed intentionally the interception without right, made by technical means, of non-public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A party may require that the offense be committed with dishonest intent or in relation to a computer system that is connected to another computer system, and according to Section 374 Elaborate that;
"A person who, intentionally without lawful excuse or justification, intercepts by technical; Any non-public transmission to, or within a computer system or electromagnetic emission from a computer system that are carrying computer data, commits an offence punishable, by imprisonment for a period not exceeding five years, or a fine not exceeding Five Million Shillings, or both".
Offences of illegal devices: this is the crime of production, sale, procurement for use, import, distribution, or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses, as illustrated in Section 375 as follows:
"A person commits an offence if the person intentionally or recklessly, without lawful excuse or justification, produces, sell, procures for use, imports, exports, distributes or otherwise makes available a device, including a computer program, that is designed or adapted for the purpose of committing an offence a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used by any person for the purpose of committing an offence against any law, is guilty of an offence, and is liable to imprisonment for a term of not exceeding five years or a fine not exceeding Five Million Shillings".
Offences against the computer user; this is kind of an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization, Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized, Disrupts or denies or causes the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another, the same as it was illustrated in section 376 as follow;

"A person who willfully, knowingly, and without authorization: Accesses or causes to be accessed any computer, computer or computer network; or system. Denies or causes the denial of computer system services to an authorized user of such computer system services, which,

in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another, is guilty of an offence against computer users, and is liable to imprisonment for a term not exceeding five years or a fine not exceeding Five Million Shillings".

Offences against fraud and related activity on Government computer. According to the section 377 said;

"A person who, having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained, information that has been determined by the Government pursuant to an Executive order or written law to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, with reason to believe that, such information so obtained could be used to the injury of Zanzibar, …… is guilty of an offence, and is liable to imprisonment for a term not exceeding fifteen years or fine not exceeding Fifteen Million Shillings".

Data Presentation, Analysis and Discussion

1. Data Analysis

This part delivers the answers to the facts accessible during the data collection process. The practical situation was to see the reality of the applicability of the Cybercrime Act on Zanzibar Island. In this study, the local people and institutions that were interviewed were given short acronyms that represented those people or institutions, where the acronyms are the following:

The House of Representative of Zanzibar represented by sign (HRZ1.), The Attorney General chamber of Zanzibar by (AGZ2.), The Law Reviews Commissions of Zanzibar (LRCZ3.), The Office of Director of Public Prosecutions Zanzibar (DPPZ4.), The Judicial Department (JD5.), The Tanzania Communications Regulatory Authority (TCRAZ6.), The Tanzania Police Force (PT7), The Advocate (AD8.), and Local people from Community (LP9).

Mendations and Conclusions

1. Findings

1.1 The ratification information for the Cybercrime Act No. 14 of 2015 has not been officially announced.

During the research, the researcher found out the main reason why the law could not be applied in Zanzibar. The reason is that the notification of the approval of the law by the Zanzibar House of Representatives was not officially announced by recognized official media bodies. This resulted in stakeholders and some enforcement agencies having no official notification.

1.2 The Increase in Cybercrime Criminal Activity.

As the researcher of this study continued his research, he was able to discover the crimes mentioned in Cybercrime Act No. 14 of 2015. There were 29 offenses, but in Zanzibar, despite the introduction of the law, law enforcement only had to contend with one type of offense, which is cyberbullying, a situation that is leading to an increase in crime. This is because the remaining 28 cases cited in cybercrime are increasing because the perpetrators of these crimes believe they will face no punishment if they commit them.

1.3 Inadequacy of the Law enforcement Agencies of Zanzibar on Cybercrime Cases.

In this regard, the researcher found that law enforcement agencies do not have sufficient knowledge of cybercrime cases, which leads to many cases not appearing in court due to a lack of sufficient evidence.

1.4 Inadequacy of The Penal Act No. 6 of 2018 to fight cybercrime.

In this regard, the researcher was able to discover the Penal Act, despite the fact that it has become the law that deals with the criminalization of all types of offenses. The researcher learned that the law, through Part 35, which mentioned the offenses related to computer-related crime, has developed large gaps and is not in line with the present time because the law has only mentioned 9 offenses, most of which do not occur on the island of Zanzibar, leaving behind dozens of offenses committed in the community, but there is no law that can make people guilty because the law is silent for many crimes of cyber origin.

2. Recommendations

As per the research findings the following recommendations are proposed:

2.1 Publication of Laws on Cybercrime.

It is the responsibility of the Ministry of Communications and Transport in Zanzibar, in cooperation with the Attorney General's Office, to ensure that the Cybercrime Act No. 14 is published in the official government gazette so that law enforcement agencies and legal stakeholders can obtain information about the official start of the law on the island of Zanzibar. According to the 23(3) say;

"Where it's provided in any Act that it shall come into operation on such date as the President or Minister may by notice in the Gazette appoint and the President or the Minister has notice in Gazette appoint such date it shall be lawful for the President or as the case may be the Minister at any time before the date so appointed to revoke the previous appointment by a subsequent notice and appoints another date".

2.2 Cybersecurity training by enforcement agencies.

The researcher points out that it is the government's responsibility to ensure that there are sufficient experts in the police departments, DPP office, and courts, as there is a shortage of experts with skills in conducting genealogical cases and investigations of cybercrime, which indicates they are in line with the current time to avoid the shame of losing the case simply because of a lack of expertise in the equipment used to commit the crime.

2.3 Amendment of Penal Act No.6 of 2018

The researcher recommends amending the Penal Act No. 6 of 2018, particularly in Part 35 of the Act, to be able to include the offenses that are most committed in Zanzibar society and to amend the existing ones that have been included in the law since 2004. In the time we have now, a lot of information technology has grown with great progress and has made the offenses mentioned in that part obsolete.

Conclusions

In this research, the researcher is satisfied that the research has a positive impact on the issues of the application of Cybercrime Law Act No. 14 of 2015 in Zanzibar.

At the time research began, it was based on the statement of the problem of this research, which was to assess the applicability of the Cybercrime Law Act No. 14 of 2015, which was enacted by Parliament and ratified by the House of Representatives in 2016. In the opinion of the researcher, he believed that the law was never being used in Zanzibar and believed they were using Penal Act No. 6 of 2018, especially in Part 35, to determine those crimes. But in the final stage of this research, the researcher has been able to learn new things as follows:

The Cybercrime Act No. 14 of 2015 has started to be applied in Zanzibar from 2022, thus slightly different from the statement of the problem where the researcher believed until now (2023) that the law is not applied in Zanzibar.

The researcher has learned that despite the law coming into force in 2022, the truth is that only one crime so far has been implemented, and they have been able to gather evidence and try to bring the criminals to court. The remaining 28 crimes so far have not been dealt with, and the perpetrators of those crimes are doing it, but the cases end up in the police station.

The researcher learned that despite the presence of computer-related crimes in Part 35 of Penal Act No. 6 of 2018, and for the purpose of this study, a researcher focused on the application of these laws from 2015 to 2023 and found that no one has ever been convicted for the offenses committed in that part of the Penal Act.

In conclusion, it is important for Zanzibar to do anything possible to fight those cybercrime offenses because many of the victims of these crimes are ordinary citizens, so urgent efforts must be made by the Revolutionary Government of Zanzibar to ensure that the Cybercrime Act No. 14 is officially announced through the official Gazette so that all law enforcement bodies have a consensus on the application of that law in Zanzibar.

References

1. Chris Reed, Computer Law, Printed in India by Saurabh printer, 2012.
2. Chris Reed, Internet Law, Published by Universal Law Publishing co. pvt. Ltd, 2004.
3. Mambi, Adam. J. ICT LAW BOOK (a source book for information and communication technologies and cyber law). Dar es salaam, 2010.
4. Angel M. Rabasa, The Muslim World After 9/11. 2004
5. Asherry Magalla, Prevention and Detection of Cyber Crimes in Tanzania as Described by the Cyber Crime Act, No.13 of 2015.
6. Abhishek Shah, Dhaval Chudasama, The Causes of Cybercrime Volume 5 - 2020, Issue 8 - August – 2020.
7. Back, S., & LaPrade, J, The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence, 2019.
8. Damas Daniel Ndumbaro, The Cyber Law and Freedom of Expression, The Tanzanian Perspectives, International Journal of Science Arts and Commerce Vol. 1 No. 8, October-2016.
9. Duff, Robin Antony, Intention, Agency and Criminal Liability: Philosophy of Action and the Criminal Law, 1990.
10. Howard Carter, Misuse of Library Public Access Computers, Journal of Library Administration, 2002.
11. J.A. Mshana, Cybercrime, An Empirical Study of its Impact in the Society- A Case Study of Tanzania, 2015.
12. John. Michael Marere, The Cybercrimes Act, A Weed in the Garden of Freedom of Expression in Tanzania, 2015.
13. Mac Dermott *et al*, The Internet of Things, Challenges and Considerations for Cybercrime Investigations and Digital Forensics, 2020.
14. Ramasubramani.M and Ragothaman.C.B, Theoretical revelation on Cybercrime and its impact on the society 2015.
15. Richards & Eboibi, African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law, 2021.
16. Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, and Steve Chon, Organizations and Cybercrime, October 11, 2013.
17. Usman, Mahboob, The Cybercrime, Pakistani Perspective, Islamabad Law Review, 2017.
18. Wada & Odulaja, Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A conceptual Review, 2015.
19. Yatharith Chauhan, Investigating Various Approaches and Ways to Detect Cybercrime. Journal of Network Security, 2021.
20. https://www.african-horizons.com/safari_web/uk/destination-history_of_zanzibar.awp
21. https://legalstudymaterial.com/oral-and-documentary-evidence
22. https://definitions.uslegal.com/d/documentary-evidence
23. https://www.definitions.net/definition/e-services
24. https://www.dotnek.com/Blog/Security/what-are-the-negative-effects-of-cybercrime
25. https://www.lawteacher.net/cases/campbell-v-mirror-group.php
26. https://www.dotnek.com/Blog/Security/what-are-the-negative-effects-of-cybercrime
27. https://www.33bedfordrow.co.uk/insights/articles/indecent-images-the-shift-in-recent-years-from-possession-to-making.
28. https://www.mediappadefence.org
29. https://www.umcjustice.org/articles/pornography-and-sexual-violence-62
30. https://dictionary.cambridge.org/dictionary/english/cyberbulling
31. https://www.britannica.com/topic/espionage
32. https://www.sciencedirect.com/topics/computer-science/search-warrant
33. https://www.african-horizons.com/safari_web/uk/destination-history_of_zanzibar.awp
34. https://www.ruaneattorneys.com/connecticut-criminal/computer-crimes/destruction-of-computer-equipment
35. https://old.ulii.org/ug/judgment/high-court-criminal-division/2013/13
36. https://definitions.uslegal.com/d/documentary-evidence
37. https://www.cps.gov.uk/legal-guidance/intellectual-property-crime
38. https://www.sciencedirect.com/topics/computer-science/search-warrant
39. https://legalstudymaterial.com/oral-and-documentary-evidence
40. https://www.britannica.com/topic/espionage

41. https://www.mediadefence.org
42. https://www.umcjustice.org/articles/pornography-and-sexual-violence-62
43. https://dictionary.cambridge.org/dictionary/english/cyberbulling
44. https://www.dotnek.com/Blog/Security/what-are-the-negative-effects-of-cybercrime
45. https://www.lawteacher.net/cases/campbell-v-mirror-group.php
46. https://www.dotnek.com/Blog/Security/what-are-the-negative-effects-of-cybercrime
47. https://krazytech.com/technical-papers/cyber-crime
48. https://www.britannica.com/topic/mens-rea
49. https://simplestudying.com/r-v-cropp-1991-7-clsr-168/
50. https://www.unodc.org/documents/cybercrime
51. https://www.bezaspeaks.com/cybercrime/history.htm#:~:text=In%201820%2C%20Joseph%2DMarie%20Jacquard,and%20livelihood%20were%20being%20threatened.
52. https://itcareerswitch.co.uk/the-history-of-cybercrime/
53. https://goosevpn.com/blog/origin-cybercrime
54. https://arcticwolf.com/resources/blog/decade-of-cybercrime/
55. https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022#:~:text=https://www.bezaspeaks.com/cybercrime/history.htm#:~:text=In%201820%2C%20Joseph%2
56. https://www.merriam-webster.com/dictionary/cybercrime
57. https://itcareerswitch.co.uk/the-history-of-cybercrime/
58. https://goosevpn.com/blog/origin-cybercrime
59. https://www.bezaspeaks.com/cybercrime/history.