RCMOS – Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. Sao Paulo-SP.

Year V, v.1, n.1, Jan/July 2025. | submission: 04/05/2025 | accepted: 06/05/2025 | publication: 08/05/2025

Cybercrimes in the Mozambican legal system

Computer crimes in the Mozambican legal system

Computer crimes in the Mozambican legal system

Raul by Miguel Benjamin Jofrisse Nhamitambo1

SUMMARY

This research aims to address computer or cyber crimes in Mozambique. Having in view of the paradigmatic changes promoted by globalization and advances in technology, with the use of The Internet has become an environment that facilitates the practice of violence in the virtual world. The information society made possible several technical and social changes, creating global and instant communication, facilitating communication in different areas. An analysis was made on ICTs and Law, presenting their main aspects, terminological analysis and concept of computer or cyber crime, as well as the classification of crimes computer or cybernetic agents and active and passive subjects. The practice of this type of crime has increased with the skills that the internet offers its users (anonymity, simplicity, agility of communication, ease of cross-border data sharing and potential to reach target audiences). Cyberspace has become if so, an instrument for "good" users, as well as for individuals who take advantage of the benefits of the network universal information with a view to executing the most diverse types of crime. In this logic, there is a need for justice to take action and provide solutions to current problems, seeking to apply a law that proves to be current.

[1] PhD in Legal Sciences, from the University for International Cooperation in Mexico (UCIMEXICO) - Mexico (2020); Master in Corporate Legal Advice, from the University of Madrid (UDIMA) - Madrid (2016); Degree in Legal Sciences and Criminal Investigation, from the now defunct Alberto Chipande Higher Institute of Sciences and Technology (ISCTAC) - Beira (2011); Lawyer and Member of the Mozambican Bar Association (since April 2018); Assistant Professor of Information and Communications Technology Law (ICT Law) - at the Joaquim Chissano University (UJC) - Maputo (since February 2020), in the Degree Course in Information Technology and Systems Engineering; Assistant Professor of Administrative Law and Notions of Administrative Law – at the Pedagogical University of Maputo (UP - Maputo), in the Bachelor's Degree Courses in Human Resources Management and Public and Educational Management;

Senior Legal Assistant – Legal Office (UP - Maputo); University Lecturer in Introduction to Law, Administrative Law I and II and Labour Law, in the Bachelor's Degrees in Law, Accounting and Auditing and Public and Local Government Administration – at the Instituto Superior Maria Mãe de África (ISMMA); Assistant Professor at the Instituto Superior de Contabilidade e Audiria de Moçambique (ISCAM), teaching the subject Taxation Complements in the Master's Degree in Auditing; Author, Reviewer, External Evaluator and Reviewer in the Multidisciplinary Scientific Journal O Saber (since the 2nd Semester of 2024); Author, Evaluator and Reviewer in the Multidisciplinary Journal RECIMA21 (since the 1st Semester of 2025)

and in the Consinter International Law Journal (International Council for Contemporary Studies in Postgraduate Studies – CONSINTER), since the 2nd Semester of 2025 and Organizer of the Digital Scientific Publisher (Since the 1st Semester of 2025). Matola – Maputo.

ORCID: 0009-0006-4118-1970. rnhamitambo@gmail.com.(+258) 872058783/847417800.

Keywords: Computer or cyber crimes; cyberspace; current problems.

ABSTRACT

The purpose of this research is to address computer or cyber crimes in Mozambique. In view of the paradigmatic changes promoted by globalization and advances in technology, the use of the internet has become an environment that facilitates the practice of violence in the virtual world. The information society has enabled several technical and social changes, creating global and instant communication, facilitating communication in different areas. An analysis was made on ICTs and Law, presenting their main aspects, the terminological analysis and concept of computer or cyber crime, as well as the classification of computer or cyber crimes and active and passive subjects. The practice of this type of crime has increased with the capabilities that the Internet offers its users (anonymity, simplicity, agility of communication, ease of sharing cross-border data and potential to reach the target audience). Cyberspace has thus become an instrument for "good" users, as well as for individuals who take advantage of the benefits of the universal information network with a view to carrying out the most diverse types of crime. In this logic, there is a need for justice to take action and provide solutions to current problems, seeking to apply a law that is up to date.
Keywords: Computer or cybercrimes; cyberspace; current problems.

ABSTRACT

The purpose of this investigation is to address computer and cyber crimes in Mozambique. Before them paradigmatic changes promoted by globalization and technological advances, the use of internet has converted into an environment that facilitates the practice of violence in the virtual world. The information society has allowed several technical and social changes, creating global and instantaneous communication, facilitating communication in different areas. An analysis was carried out on ICT and Law, presenting their main aspects, the terminological analysis and concept of computer or cybernetic crime, as well as the classification of them computer or cyber crimes and active and passive subjects. The practice of this type of crime has increased with the capabilities that the Internet offers to its users (anonymity, sencility, communication agility, ease to share cross-border data and potential to reach the target audience). Cyberspace has been converted as an instrument for both "good" users and individuals who benefit from the benefits of the universal information network to commit the most diverse types of crimes. In this logic, there is a need that the justice system acts and provides solutions to current problems, seeking to apply updated law.
Keywords: Computer or cyber crimes; cyberspace; current problems.

INTRODUCTION

In this work we will address computer or cyber crimes in Mozambique.

Based on the premise that Law follows social facts and that anonymity influences in the commission of unlawful acts, the intervention of the Law arises, aiming, at the very least, to reduce the incidence of these practices. Because, at the same time, the problem related to the absence of punishment for those who committed conduct considered typical, illicit and culpable, generating consequently, legal instability. Therefore, it is necessary to analyze the delay evidentiary, whose identification of the active agent is complex due to the anonymity granted by network.

Given the social relevance and complexity of the topic, there is no possibility of exhausting the subject, However, the aim is to encourage discussion and analyse references that confirm, or not, improvements and clarifications on the subject. To this end, regarding the methodology, the deductive method as a way of approaching research and the procedure used as technique was the literature review – doctrine, jurisprudence, scientific articles and legislation – of in order to have a real perception and general conclusion on the topic.

The increasing access to ICT services, including the Internet, is also accompanied by growing vulnerabilities to which citizens are subject and with this also the growth of cybercrimes. The Government of Mozambique is also fully aware of the threat and negative effects of computer or cybercrime on your Nation and for efforts have been made to ensure that there are instruments that can protect citizens and penalize those who commit these crimes using ICTs. These efforts include:

ÿ The Penal Code, approved by Law No. 24/2019, published on December 24, 2019, which covers computer crimes, namely: Child pornography (article 211), Use of minors in pornography (Article 212), Distribution or possession of pornography of minors (article 213), Invasion of private life (article 252), Violation of correspondence or communications (article 253), Automated database (article 254), Unlawful access (article 256), Illegal recordings (article 257), Theft of fluids (article 276), Fraud information technology and communications (article 289), Frauds relating to instruments and electronic payment channels (article 294), Abuse of means of payment electronic data (article 295), Computer fraud (article 336), Data interference (article 337), Interference in systems (article 338), Abusive use of devices (article

339), Public incitement to a crime (article 345), Public apology for a crime (article 346), Publication of the conviction decision (article 448);

ÿ Law 3/2017, the Electronic Transactions Law, enacted in January 2017, which aims to protect consumers and regulate the use of electronic systems in the government, private and civil society;

ÿ Regulation on the control of Telecommunications Traffic, Decree No. 75/214, of 12 December;

ÿ SIM Card Registration Regulation, Decree 18/2015;

ÿ Telecommunications Law, Law No. 4/2016, of June 3.

According to Nhamitambo (2025), Crime or offense is the voluntary act declared punishable by law. criminal, under the terms of art. 1 of the Criminal Code.

According to Marques and Martins (2000, p.493) cited by Nhamitambo (2025), "crime computer science is any act in which the computer serves as a means to achieve an objective criminal or in which the computer is the target of that act."

THEORETICAL BASIS

Internet and Law: Contextualization and Important Aspects

Access to the internet, as a Fundamental Right, arises from the values of human dignity and citizenship, constitutionally guaranteed. “Currently, the role of the Internet extends beyond a simple means of communication, as it has become part of life itself in society as a facilitator and maintainer of human relations.” (PIMENTEL; CARDOSO, 2015, p. 48).

Thus, the legal order and constitutional regulations guarantee the fundamental right to information. formation and freedom of expression, hyper-dimensioned by the use of the internet, new technologies and development of computer science.

In the context of globalization, the Internet has become the main means of communication and information. tion. It is present, according to Sorg et.tal (2019, p. 9), in almost all activities of life

private. The amount and diversity of information that can be accessed and shared, the ease communication ability, makes it possible to share messages and post opinions, producing a new way of organizing information and communication.

In this new perspective, computers, smartphones, tablets, GPS, digital cameras, and others electronic devices are used in crimes and illegal actions. The spread of technologies technologies and electronic resources “are not only being used by companies, but also also being used more in the practice of various crimes” (CAIADO, CAIADO, 2018, p. 10).

In the same sense: Practically all individuals and legal entities, in one way or another, interact in cyberspace, as the Internet has become indispensable in our lives, enabling providing numerous facilities ranging from simple social contacts to banking operations.

However, precisely because it expands to practically all homes, businesses and organizations public, its free access results in problems related to the security of this system, especially when it comes to operations involving non-public information, such as confidential data, personal and banking information (GIMENES, 2013).

Due to the legal uncertainty that is caused in the digital sphere and the social fear throughout the world, world, there is a need to update legislation and introduce more rigorous monitoring methods, aiming at optimizing the agent's search methods. The internet has created a new paradigm, not only to improve the quality of life, but currently represents a facilitating means of criminal practices.

Caiado, Caiado (2018, p.10), explains that, with this new paradigm, the development of technology improves the standard of living, however, at the same time, it increases exponentially and pro-proportionately, the carrying out of different criminal practices, “among them the creation of one of the most infamous crimes in modern society: child pornography, and also facilitating access to it and the distribution of material related to it.”

Crimes committed in digital media have taken on enormous proportions with the advent of society. digital age and represent a huge challenge to the proper identification and prosecution of the sentence.

Therefore, it is important to highlight that: Access to new technologies in an increasingly more connected have ensured several advances in social and economic relations. However, all this technology can also be used to commit crimes. Cybercrimes are a reality, several types of crimes have originated and others already known have gained a new look in light of technological advances (ARAÚJO, 2018, p. 90).

Thus, with the establishment of the internet, new social, political and economic situations arise.
and, consequently, new legal issues. In the words of Reale (2010, p. 2), Law is
“a social fact or phenomenon; it exists only in society and cannot be conceived outside
of it. One of the characteristics of legal reality is, as we can see, its sociality, its qua-
ability to be social.”

Therefore, Law needs to be adapted to new realities. “Therefore, in Law,
Penal a ultima ratio for the inhibition or punishment of the performance of a certain fact or act
human not tolerated by society at a certain time.” (SANTOS, 2018, p. 159). This time,
with the benefits of the internet, new risks have emerged. With digital inclusion: [...] dissemination
new forms of personal harassment and abuse of children and adolescents have emerged, and the privacy of
individuals are increasingly under threat. The Internet has become a stage for cybercrimes, for practices
of mass content censorship and illegal surveillance and espionage carried out by States
national. Their tools have come to be used by groups that promote violations of human rights.
human rights and exploit the fragility of public services and infrastructure, including attacks
cybernetics to military systems (SORJ et al; 2018, p. 9).

At the same pace as technological evolution, space opens up for virtual crimes, which
have been causing several losses to society. As Maues, Duarte and Cardoso (2018,
p. 170), the immateriality of the internet favors the absence of spatial and temporal limits; its
broad and generic access “leverages risks arising from the vulnerability of the digital environment, being
thus, the greater the use of the internet in human interactions, the more it enhances
tendency for legal problems to arise, including the birth of new types of cri-
month."

As Spinieli (2018, p. 206) explains, it was from the great uprising of computer invasions
global pains that brought to the State the unique responsibility of monitoring and, at the same time,
ensure the protection of legal assets relevant to the social environment that was at risk,
in addition to punishing those who transgress such values.

Evolution has led us to the cybernetic age, with advantages and disadvantages “that this technological evolution
nological can provide. There has been, all over the world, the creation of new cyber crimes
netics, arising from the need to order, discipline and limit the improper use of modern
and advanced cybernetic technology.” (BITENCOURT, 2018, p. 554).

The internet, associated with the dissemination of information and communication technologies, is a new path to the practice of crimes already provided for in the criminal incriminating norm, being necessary that legislation be adapted to crimes committed virtually.

RESULTS AND DISCUSSION

Computer Crime

According to Marques and Martins (2000, p.493), cited by Nhamitambo (2025), "computer crime is any act in which the computer serves as a means to achieve a criminal objective or in that the computer is the target of this act."

Although there is no specific definition of “Computer Crime”, several doctrinaires address the subject and have strived to elucidate a clear and concise concept about the new age crime.

According to Perez (2003), broadly speaking, cybercrime is: “any criminogenic or criminal conduct that in its execution makes use of electronic technology as method, means or end and that, in a way”.

In the strict sense, Cybercrime is any criminal act in which computers, its techniques and functions play a role as method, means or end.”

RODRÍGUEZ, defines Cybercrime as: “the execution of an action that, when combined with the characteristics that delimit the concept of crime, is carried out through a computer and/or telematic element, or which violates the rights of the owner of a computer element, whether hardware or software.”

Characteristics of Computer Crimes

People who commit such crimes have certain characteristics that do not present the common denominator of criminals. That is, active subjects have the ability to deal

with computer systems and, in general, because of their employment situation, they are in strategic locations where sensitive information is handled; or are qualified in the use of computerized systems, even though, in many cases, they do not carry out activities that facilitate the practice of this type of crime.

According to TELLEZ, cybercrimes have the following main characteristics:

a) These are crimes that involve white-collar criminal conduct, provided that only one a certain number of people with certain knowledge (in this case technicians) can commit them.

b) They are occupational actions, as they are frequently carried out when the subject is work.

c) They are opportunity actions because they take advantage of a created or highly intensified in the field of functions and organizations of the technological and economic system.

d) They cause serious economic losses, as they almost always produce "profits" of more than five digits for whoever gets them.

e) They offer ease of time and space, as they can be practiced in thousandths of a second and without the necessary physical presence.

f) There are many cases and few complaints, due to the lack of legal regulation at the national level. International.

g) They are very sophisticated and relatively common in the military field.

h) They present great difficulties in verification, due to their technical nature.

i) Most of them are malicious or intentional, although there are also many of a harmful nature. negligent or reckless.

j) They offer facilities to minors for their commission.

k) They tend to proliferate more and more, which is why they require urgent action, regulation legal in the international sphere.

Classification of Computer or Virtual Crimes

There are several doctrinal classifications of cybercrimes. Two categories are are used: that of computer crimes proper or pure and that of computer crimes improper or impure.

Barreto and Brasil (2016, p.17) define virtual crime as those in which the device computerized system and/or its content is the target of criminals - computerized systems, databases, files or terminals (computers, smartphones, tablets) are attacked by criminals, usually after identifying vulnerabilities, either through programs malicious or socially engineered (scammer tricks victim into providing information) personal and/or strategic information).

For Albuquerque (2006, p.168), impure virtual crimes “would refer to crimes in which computer resources constitute the means of execution, having as their object legal assets that are already protected by existing criminal types”. In the information society, the incidence of criminal offences “have as their material object or means of execution the technological object of information topic: hardware, software, networks, etc.

Pure computer crimes, according to Amabélia Chuquela, are those in which the use of computer system is the means necessarily used for criminal practice.

Impure computer crimes, according to Amabélia Chuquela, are those in which the use of the computer system is just a new modus operandi. That is, they are those in that the use of the computer system is the means necessarily used to practice criminal.

Nucci (2017, p. 131) explains that the active subject (author or agent) is “the person who practices the conduct described by the criminal type”. In other words, it is the person who carries out the typical action or omission, in the crimes intentional or negligent. Only a human person can be an active subject, not animals or things.

The passive subject of the crime, according to Nucci (2017, p. 134), is the holder of the protected legal asset by the incriminating criminal type, injured or threatened with injury. The following may appear as passive subjects: you – victims, offended parties, the natural person or individual, even if incapacitated, the group of individuals duos, the legal entity, the collective, the State or the international community, according to the nature of the crime.

In cybercrimes, in the active pole, therefore, it is very common to associate hackers with the figure of internet criminals, however, hacker is just one expression given, among many others, to characterize a person who has a lot of knowledge in the computer field and who invades systems, but it does not necessarily target the illicit.

According to Assunção (2017, p. 33), the term hacker, since the 1970s and 1980s, used to designate “snoops”. Over time, it was used by the media to name system invaders, to this day this term is used in a peculiar way: it designates a boy from twelve years old who activates the school computer to change his grade or a fraudster who deceives people, sending them emails to capture access passwords.

Therefore, there are several other designations to differentiate the perpetrators of the crimes committed, such as for example, the figure of crackers, who are those who necessarily use their co- knowledge for evil, obtaining illicit advantages, through damaging systems, usurping tion of passwords, data, documents, among others. In general terms, it is the “name for someone who has great computer skills. Cracker, black-hat or script kiddie, in this environment, it refers to those hackers who have a hobby of attacking computers. Therefore, the word hacker is a genus, and cracker, a species.” (GIMENES, 2013).

Moisés Cassanti (2014, p. 2) makes a distinction between the concepts of hacker and cracker. Although both are terms that refer to computer experts, the main difference is in how each person uses this knowledge: Although the term hacker always appears as- associated with data theft and system invasion, in the understanding of computer experts. tation, the real criminals are referred to as crackers. The word derives from the verb in English “to crack”, which means to break. Among the actions are the practice of breaking systems

security codes, encryption codes and network access passwords, illegally and with the intention tion of invading and sabotaging for criminal purposes. The term hacker, in turn, is used to designate a programmer with extensive knowledge of systems, but without the intention of causing harm. In fact, the ability to deal with systems and programming is often used by police themselves in investigations or even in the development of software with the aim to fix security holes, create new features or adapt old ones.
In this way, the “issue of security in cyberspace is not only of interest to people individuals or companies, being highly relevant for public bodies, for political agents and for the State itself.” (GIMENES, 2013). Anyone can be a passive subject, even even companies and institutions, and, due to the techniques of cybercriminals, they end up having their information and goods violated.

The Legal Asset Protected in Cybercrimes

The issue regarding the protected legal asset raises one of the problems that raises the most doubts they arise in crimes of damage in general, and in crimes of computer damage in particular.

The protected legal asset in general is information, but it is considered in different ways, whether as an economic value, as an intrinsic value of the person, for its fluidity and legal traffic and, finally, by the systems that process or automate it; which are equivalent to goods traditional protected legal rights, such as:

a) The assets in the case of the wide range of computer scams and data manipulations to which gives rise to.

b) Confidentiality, privacy and confidentiality of data in the event of cyberattacks to the sphere of privacy in general, especially in the case of databases.

c) The security or reliability of legal and/or evidentiary traffic, in the case of falsifications of supporting data or documents through computer scientists.

d) The right of ownership, in this case over the information or over the physical elements and materials of a computer system, which are affected by damage and so-called terrorism computer.

Therefore, the protected legal asset is subject to confidentiality, integrity, availability of information and computer systems where it is stored or transferred.

From another doctrinal perspective, it is assumed that the emerging Information Society makes absolutely necessary to incorporate intangible values and the information itself as legal protection assets, taking into account the differences that exist, for example, between tangible and intangible property.

This is because, in Palazzi's opinion, information cannot be treated in the same way, in the same way that current legislation applies to tangible goods2 , although. These goods have a shared intrinsic value, which is its economic value, which is why information and other intangible assets are objects of property, which is constitutionally protected. In In short, the protection of information as a protected legal asset must always take into account the principle of the necessary protection of legal assets which indicates that the penalization of the conduct develops within the framework of the principle of “harm” or “harmfulness”.

Thus, conduct can only be punished when it is completely incompatible with the assumptions of a peaceful, free and shared life materially secure.

The social interest worthy of criminal protection would be: Information - stored, processed and transmitted through computer systems - without prejudice to any that derive from it or bring with it a wide range of legal assets protected and safeguarded by the law and legislation of each country.

[2] Tangible goods are physical objects, that is, they have material substance and can be touched. They are goods that can be seen, felt and perceived by the senses, unlike intangible goods, which are intangible assets. Examples of tangible assets include real estate, vehicles, equipment, furniture, and merchandise.

RCMOS - Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. Sao Paulo-SP.

Legal Type of Computer Crimes and Their Characteristics

MORRAIS (2015), cited by Nhamitambo (2025), states that:

> "Information and communication technologies, in addition to enabling the exchange of information, data and information that materialize from interpersonal relationships to agreements commercial transactions involving large financial transactions, created new types of crimes, which are cyber crimes. However, using conceptual analysis, we bring common aspects in relation to the concept of cybercrime. In this corollary, we can refute that cybercrimes behave like an action or typical, unlawful, culpable and punishable omission under criminal law and characterized by use of the computer (typical instrument of crime) and the internet to commit criminal acts, such as", under Law No. 24/2019, of December 24 (which approves the Penal Code):

Pornography of minors (article 211), is characterized by visual representation of a minor or person appearing to be a minor engaged in sexually explicit through support or platform.

Use of minors in pornography (article 212), is characterized by the use of minors 18 years of age in pornographic photography, filming or recording, regardless of their support, or enticement for that purpose; or in a pornographic show or enticement for that purpose end. Whose penal framework varies from 1 to 5 years of imprisonment. And, of 12 years, whose framework criminal penalty ranges from 2 to 8 years in prison.

Distribution or possession of child pornography (article 213) is characterized by distribution, import, export, disclosure, display or transfer professionally or for profit, in any capacity or by any means, pornographic photography, film or recording materials of minors under the age of eighteen; mere sharing, display, transfer, import, export or distribution of the material, when it is not for profit or professional purposes, regardless of the support or

platform, acquire, hold or preserve the materials referred to above, even for personal use. Any attempt to do so is punishable.

Invasion of private life (article 252), is characterized by interception, recording, recording, use, transmission or disclosure of conversation, telephone communication, image, photography, video, audio, detailed billing, email messages electronic, social network or other data transmission platform; capture, for photographing, filming, manipulating, recording or disseminating images of people or intimate objects or spaces; secretly observing or listening to people who are in a private place; or disclose facts relating to the private life or serious illness of another person – the latter is not punishable when it is practiced as an appropriate means to achieve a legitimate and relevant public interest. And, it is punished with imprisonment up to 1 year and corresponding fine, whoever, without consent and with the intention of violating the people's private lives, particularly the intimacy of family or sexual life.

Violation of correspondence or communications (article 253), is characterized by interference in the content of telecommunications or taking knowledge of it, without consent, the penalty for which is up to 1 year in prison and a corresponding fine. and, by disclosure of the contents of letters, parcels, closed writings, or contents of telecommunications, the penalty ranges from 6 months to 1 year in prison and a corresponding fine.

Automated database (article 254), is characterized by creating, maintaining or use an automated file of individually identifiable data relating to political, philosophical or ideological convictions, religious faith, party affiliation or trade union and private life, without due consent, or outside the established cases by law and punishable by imprisonment of up to 2 years and a corresponding fine.

Illegitimate access (article 256) is characterized by invading another person's device, fixed or mobile, connected or not to the computer network, in order to obtain information not public mail or private electronic communications, access to private data, commercial or industrial secrets, confidential information or remote access is not authorized device, without legal permission or without being authorized to do so by

owner, by another holder of the right to the system or part thereof and punishable by imprisonment from 1 to 2 years and a fine of up to 1 year. And, illegitimately, produce, sell, distribute or any other form disseminate or introduce into one or more computer systems devices, programs, an executable set of instructions, code, or other computer data intended to produce the unauthorized actions described previously in relation to the facts and the criminal framework.

Criminal proceedings depend on a complaint, as it is a private crime.

Illicit recordings (article 257), is characterized by recording words spoken by another person and not intended for the public, even if addressed to them; use or allow that the recordings described above are used, even if lawfully produced, against will and outside the cases permitted by law, whose penal framework is of imprisonment of up to 1 year and corresponding fine.

Theft of fluids (article 276) is characterized by stealing, for personal consumption or third, telephone signal, radio, television, internet, voice data, image, video or other intangible assets with economic value, by any means, is punished with a penalty of imprisonment for up to 1 year, if a more severe penalty is not applicable. Attempts are punishable.

Computer and communications fraud (article 289) is characterized by causing another person causing financial loss, interfering with the result of data processing or through incorrect structuring of a computer program, incorrect use or incomplete data, use of data without authorization or intervention by any otherwise unauthorized in the processing, with the intention of obtaining for oneself or for third illegitimate enrichment and; causing financial loss to others, using programs, electronic devices or other means that, separately or in combination, set, are intended to reduce, alter or prevent, in whole or in part, the normal operation or exploitation of telecommunications services, with the intention of obtaining for himself or for a third party an illegitimate benefit, and is punished with imprisonment of up to 3 years or with a fine.

Fraud relating to electronic payment instruments and channels (Article 294), is characterized by falsifying an electronic payment instrument or channel; accessing illegally to an electronic payment system, through undue violation of the security mechanisms; install objects that affect the operation of the channel or electronic payment system, aiming to obtain, adulterate or destroy data or information; unlawfully appropriating an electronic payment instrument others, including the corresponding secret code; possess, hold, import, export, receive, transport, sell or transfer to third parties payment instruments electronic data obtained improperly or that have been counterfeited or counterfeiting; and create computer programs, instruments, objects and other means deliberately prepared to commit offences relating to instruments electronic payment systems; and is punished with imprisonment from 1 to 3 years and a fine of up to 1 year. And, when the actions described above affect the data recorded or incorporated into a payment bank card or any other device that allow access to a payment system or means, to a communications system or to conditional access service, the penalty is imprisonment of up to 5 years and a fine of up to 1 year.

And, by importing, distributing, selling or possessing for commercial purposes any device that allows access to a system or means of payment on which the crime has been committed any of the actions provided for in paragraph 2, shall be punished with a prison sentence of up to 5 years.

Electronic payment instrument is the electronic device or record that allows the user to transfer funds or pay a beneficiary.

Abuse of electronic means of payment (article 295), characterized by abusing the possibility granted by the possession of electronic means of payment to take the issuer to make a payment or cause harm to this or to a third party, is punished with the following theft penalties.

Computer forgery (article 336), characterized by introducing, modifying, deleting or intentionally and unlawfully suppress computer data, producing data or non-genuine documents, with the intention that they be considered or used

for legal purposes as if they were; for acting with the intention of causing harm to another or to obtain an illegitimate benefit, for oneself or for a third party, using a document produced from computer data that were the subject of the acts referred to above or card or other device in which the data is recorded or incorporated object of the acts referred to in the previous number, shall be punished with the penalties provided for in one and in another number, respectively. and is punished with a prison sentence of 1 to 5 years and a fine up to 1 year. And finally, for importing, distributing, selling or holding for commercial purposes any device that allows access to a communications system or service conditional access, on which any of the actions has been carried out mentioned above, is punishable by a prison sentence of 2 to 8 years.

Interference with data (article 337), characterized by altering, deteriorating, rendering useless, erase, suppress, destroy or in any way alter computer data and; by means of the introduction or transmission of computer data or, in any other way, installing vulnerabilities, interfering with the functioning of computer systems, intentionally causing harm to someone, and is punishable by imprisonment of 1 to 2 years and corresponding fine.

Interference in systems (article 338), characterized by altering, deteriorating, rendering useless, erase, suppress, destroy or in any way alter computer data and; by means of the introduction or transmission of computer data or, in any other way, installing vulnerabilities, interfering with the functioning of computer systems, intentionally causing harm to someone. And, it is punished with a prison sentence of 1 to 2 years and corresponding fine.

Abusive use of devices (article 339), characterized by producing, selling, distribute, import or otherwise disseminate or introduce into one or more computer systems devices, programs or other computer data intended to produce unauthorized actions, without legitimacy and is punished with a prison sentence from 1 to 2 years.

Public instigation to commit a crime (Article 345), characterized by publishing in writing or any other means, provoke or incite the commission of a specific crime, in a meeting

public, through social media, and is punished with a prison sentence of 1 to 3 years or with a fine of up to 2 years, if a more severe penalty is not applicable due to other legal provision; for religious reasons, instigate others or participate in acts of violence and disturbance of public order, is punished with a prison sentence of 1 to 5 years.

The penalty cannot be higher than that provided for the typical unlawful act committed.

Public apology for crime (article 346), characterized by publishing in writing or any other means, reward or praise another person for having committed a crime, in a manner appropriate to create a danger of another crime of the same nature being committed, in public meeting, through social media, is punishable by imprisonment up to 6 months and corresponding fine, if a more severe penalty is not applicable due to other legal provision.

The penalty cannot be higher than that provided for the typical unlawful act committed.

Publicity of the conviction decision (article 448), characterized by the existence of conviction for crimes provided for in Chapter II of Law No. 24/2019, of 24 December (which approves the Penal Code), regarding Corruption and Crimes Related should be publicized in a media outlet to be determined by the court, as well as through the posting of a notice, stating the identification of the public servant, the elements of the offence, the sanctions applied and their duration. 2. The publicity of the conviction decision is carried out at the expense of the convicted person and at the place of carrying out the activity, for a period of no less than 30 days, in a manner clearly visible to the public.

Authorship of the Crime

For ZACARIAS (2016), cited by Nhamitambo (2025), the first problem to be faced in cybercrimes is the determination of authorship. It is very difficult for the person who intends commit a criminal offense uses your real personal identification. There are cases where the criminal, impersonates another person, through the improper use of their personal passwords. And

in computer networks, it is not possible to identify the user visually or through documents, but it is possible to identify the address of the machine that sends the information to the network. The breach of confidentiality of user connection data is only the provision by part of the companies, at first, of what IP would have been used and the time of certain criminal action carried out on an Internet service is postulated in the Law of Revision of the Penal Code approved by Parliament in July 2019.

Active subject

He is the one who commits computer crime.

Passive subject

The passive subject may be a public or private legal entity, or a natural person, to whom the acts carried out by the active subject are levied. This is the victim.

Materialization of cybercrime

According to Nhamitambo (2025), in general, it can be said that the evidence of crimes Cyber data is extremely volatile. It can be erased in seconds or lost easily. In addition, they have a complex shape and are usually mixed with a large amount of legitimate data, requiring a thorough analysis by technicians and experts who participate in the prosecution of the sentence.

According to COSTA (2016), cited by Nhamitambo (2025), the evidence of the crimes cybernetics, on a computer, can be classified as user evidence and system evidence". The author explains that user evidence is that produced by the active subject himself, in text files, images or any other type. As for the system evidence is produced by the operating system, based on the subject's action active.

For MORRAIS (2015), "the practice of cybercrimes is not synonymous with impunity, a since the two elements that make up the crime, authorship and materialization, are liable to

verification through criminal investigation". And, it also says that the central issue will be look at the capacity of the Mozambican criminal sphere, with the impacts of advances technological, can face these crimes, that is, the ability to investigate these crimes that are becoming more and more frequent, in order to reduce or even mitigate them.

Concept of crime

According to Nhamitambo (2025), Crime or offense is any event, carried out in a voluntary in which the criminal law itself says it is a crime. Under the terms of art. 1 of Law No. 24/2019, of December 24, which approves the Penal Code.

And, it should be noted that there are public crimes (for example: computer crimes), semi-public crimes public (for example: theft) and private crime (for example: crimes of injury, defamation).

Legislative Evolution in the Matter of Computer or Cyber Crimes

In this context, the use of the internet has increased and, as a consequence, the number of virtual scams. According to Cadoso (2020), cybercrime has existed for a long time, however, advancement and ease of use of the internet and technological resources create an environment attractive for criminal exploitation.

Characteristic of the criminal agent

The agent is intelligent, cultured, literate, has good computer knowledge, using sub-refuge as alien providers, fake identifiers (IPs), public places internet access known as LAN houses, IP changes when changing providers.

By breaking a digital protection barrier, that program becomes vulnerable and obsolete.

The criminal agent, upon overcoming the blocks against prohibited conduct, will have a reduction in time of exploitation for such conduct until new mechanisms prevent its practice.

Your identity

According to the new modus operandi, cybercrime is always committed using a computer.
or device connected to the network. This makes it even more difficult to identify the offender. We are
before a virtual subject commanded by a real subject.

CONCLUSION

It can be concluded that with the classification of cybercrimes in 2014, Mozambique is now at
walk at chameleon pace. There is currently a need for the legislator to improve
approve the cyber law and that it reflects the reality of everyday life. The crime
computer or cybernetic is committed through ICTs, taking into account the evolution in the scenario of
information and technology.

Identifying those active in cybercrimes is difficult, a situation that is due to the
to the fact that, as a rule, criminals use the internet network made available in spaces
public. The transfer of data would not be protected, a situation that facilitates interception
of criminal practice, however, makes it difficult to identify the agents.

The fight against digital crime in Mozambique involves not only the need to criminalize
identification of harmful behaviors practiced in the virtual environment, as well as requiring a
public policy aimed at educating network users. Furthermore, it is imperative to constantly
evolution of investigative techniques concerning these practices, as well as the removal of
legislative barriers concerning obtaining data from agents.

REFERENCES

ALBUQUERQUE, Roberto Chacon de. Intangible objects in the age of crime
informatics. Legal Space, Journal of Law, v.7, n.2, p.165-178, 2006. Available at: . Access
on: 02 Mar 2021.

ARAÚJO, Fábio Lucena de. LEGAL ASPECTS IN THE FIGHT AND PREVENTION OF
RANSOMWARE. In: DOMINGOS, Fernanda Teixeira Souza et al. Cybercrimes:

collection of articles. Brasília: MPF (Federal Public Ministry), 2018. Chap. 5. p. 90-115. Available at: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-cybernetics collection-of-articles. Accessed on: July 22, 2021.

ASSUNÇÃO, Marcos Flávio Araújo. Secrets of the Ethical Hacker. 5th Ed. Florianópolis: Visual Books, 2014.

CAIADO, Felipe B.; CAIADO, Marcelo. Combating child pornography with improvements in identifying suspects and detecting files of interest. In: DOMINGOS, Fernanda Teixeira Souza et al. Cybercrimes: collection of articles. Brasília: MPF (Federal Public Ministry), 2018. Chap. 1. p. 8 25. Available at: https://memorial.mpf.mp.br/nacional/vitrine virtual/publications/cyber-crimes-collection-of-articles. Accessed on: July 22, 2021.

CRESPO, Marcelo. Digital crimes: what are we talking about? 2015. Available at: https://canalcienciascriminais.jusbrasil.com.br/noticias/199340959/crimes-digitais-do-que-we are talking. Accessed on: August 2, 2021.

GIMENES, Emanuel Alberto Sperandio Garcia. Virtual crimes. Journal of Doctrine: TRF4, [s. l], on line, 2013. Available in: https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Accessed on: July 20, 2021.

PIMENTEL, Alexandre Pinto; CARDOSO, Mateus Queiroz. The regulation of the right to oblivion in the law of the civil framework of the internet and the problem of civil liability of providers. AJURIS Journal, v. 42, n. 137, Mar., 2015.

NHAMITAMBO, Raul de Miguel Benjamim Jofrisse. ANALYSIS OF NATIONAL JURISPRUDENCE AND GAPS IN MOZAMBICAN LAW IN RELATION TO INFORMATION AND COMMUNICATION TECHNOLOGIES: Analysis of national jurisprudence and gaps in Mozambican law in relation to information and communications technologies. **RCMOS - Multidisciplinary Scientific Journal of Knowledge,** Brazil, v. 1, n. 1, 2025. DOI: 10.51473/rcmos.v1i1.2025.972. Available in: https://submissoesrevistacientificaosaber.com/index.php/rcmos/article/view/972.. Accessed at: May 3, 2025.

SANTOS, Paulo Ernani Bergamo dos. International law and the fight against cybercrime against children. In: DOMINGOS, Fernanda Teixeira Souza et al. Cybercrimes: collection of articles. Brasília: MPF (Federal Public Ministry), 2018. Chap. 8. p. 156-183. Available at: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-cybernetics collection-of-articles. Accessed on: July 22, 2021.

SORJ, Bernardo et al (org.). Surviving in the networks: a citizen's guide. São Paulo: Moderna, 2018. 82 p. Available in: https://crianca.mppr.mp.br/arquivos/File/publi/santillana/sobrevivendo_nas_redes_guia_2018.pdf. Accessed on: July 5, 2021.

SPINIELI, André Luiz Pereira. Computer crimes: comments on bill no. 5,555/2013. In: DOMINGOS, Fernanda Teixeira Souza et al. Cybercrimes: collection of articles. Brasília: MPF (Federal Public Ministry), 2018. Chap. 10 p. 198-217. Available at: https://memorial.mpf.mp.br/nacional/vitrine virtual/publications/cyber-crimes-collection-of-articles. Accessed on: July 22, 2021.

LEGISLATION

MOZAMBIQUE, Law No. 24/2019, of December 24. Approves the Law on the Revision of the Code Criminal. National Press, Mozambique, MPT, 24 December.

MOZAMBIQUE, Law No. 3/2017, of January 9. Establishes the principles, general rules and the legal framework for Electronic Transactions and e-government. National Press, Mozambique, MPT, January 9.

MOZAMBIQUE, Law No. 8/2004 of July 21. Approves the Telecommunications Law. Press National, Mozambique, MPT, 21 July.

MOZAMBIQUE, Decree No. 75/2014 of 12 December. Approves the Control Regulation Telecommunications Traffic. National Press, Mozambique, MPT, December 12.