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

Year V, v.1, n.1, Jan/July 2025. | submission: 09/05/2025 | accepted: 11/05/2025 | publication: 13/05/2025

Criminal investigation into digital media

Criminal investigation on digital media

Criminal investigation in digital media

Raul de Miguel Benjamin Jofrisse Nhamitambo1

SUMMARY

This research aims to address Criminal Investigation on Digital Media. Criminal investigation is the activity that comprises the process of detection, collection of evidence and proof that, under the terms of criminal procedural law, aims to ascertain the existence of a crime, determine its agents and their responsibility, within the scope of a judicial process. It should be noted that criminal investigation only exists as such within the scope of a criminal process. In a State of law, the validity of new means of obtaining evidence provided by technological evolution does not occur automatically. On the contrary, these, due to their harmfulness, are covered by an insurmountable prohibition of evidence, requiring legislative intervention in order to provide for them in a clear, express and determined rule, with a dense and autonomous legal regime, so that their use becomes admissible and the evidence obtained through them appears legitimate.

Keywords: Criminal investigation; agents and their responsibilities; judicial process; Digital Media.

ABSTRACT

This research aims to address Criminal Investigation on Digital Media. Criminal investigation is the activity that comprises the process of detection, collection of evidence and proof that, according to the criminal procedural law, aims to ascertain the existence of a crime, determine its agents and their responsibility, within the scope of a judicial process. It should be mentioned that criminal investigation only exists as such within the scope of a criminal process. In a State of law, the validity of new means of obtaining evidence provided by technological evolution does not occur automatically. On the contrary, these, due to their harmfulness, are covered by an insurmountable prohibition of evidence, requiring legislative intervention in order to provide

[1] Doctor of 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 Technologies Law (ICT Law) - at the Joaquim Chissano University (UJC) - Maputo (since February 2020), in the Degree Course in Information Technologies and Systems Engineering; Assistant Professor of Administrative Law and Notions of Administrative Law - at the Pedagogical University of Maputo (UP - Maputo), in the Degree Courses in Human Resources Management and Public and Educational Management; Senior Legal Assistance Technician - Legal Office (UP - Maputo); University Professor of Introduction to Law, Administrative Law I and II and Labor Law, in the Bachelor's Degrees in Law, Accounting and Auditing and Public and Local 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 Complements of Taxation in the Master's Course in Auditing; Author, Reviewer, External Evaluator and Reviewer in the Multidisciplinary Scientific Journal O Saber (since Semester II of 2024); Author, Evaluator and Reviewer in the Multidisciplinary Journal RECIMA21 (since Semester I of 2025) and in the International Journal Consinter de Direito (International Council for Contemporary Studies in Postgraduate Studies - CONSINTER), since Semester II of 2025 and Organizer of the Digital Scientific Publisher (Since Semester I of 2025). Matola – Maputo. ORCID: 0009-0006-4118-1970. rnhamitambo@gmail.com.(+258) 872058783/847417800.

for them in a clear, express and determined norm, with a dense and autonomous legal regime, so that their use becomes admissible and the evidence obtained through them appears legitimate.

Keywords: criminal investigation; agents and their responsibility; judicial process; DigitalMedia.

ABSTRACT

This investigation aims to address Criminal Investigation in Digital Media.
Criminal investigation is the activity that comprises the process of detection, collection of evidence and testing that, according to the criminal procedural law, has the objective of determining the existence of a crime, its agents and their responsibility, within the scope of a judicial process. It is worth mentioning that solo criminal investigation exists as such within the scope of a criminal process. In a State of law, the validity of new means of obtaining knowledge provided by technological evolution does not occur automatically. On the contrary, these, due to their injury, are covered by an insalable evidentiary prohibition, requiring legislative intervention to foresee them in a clear, express and determined norm, with a dense and autonomous legal regime, so that their use is admissible and the test obtained through them seems legitimate.

Keywords: criminal investigation; agents and their responsibility; judicial process; Digital Measurements.

INTRODUCTION

In this work we will address Criminal Investigation on Digital Media. It constitutes a truism to affirm the extensive scope of the use of computer systems in everyday life every citizen in modern society, and it is equally evident that, with the use of these devices, each of us leaves a kind of digital trail or footprint, made up of countless computer data created at every moment and at every step in the use of information and communication technologies2 .

Due to its potential evidentiary relevance, obtaining this data, processed, stored and communicated by computer systems and networks, and the information contained therein, may be – and, taking into account the ubiquity of these technologies and the constant digitalization of society,

[2] This digital trail or footprint is made up of traces created as a result of the use of information and communication technologies, and can be active (or avoidable) – made up of data provided by the user – or passive (or unavoidable) – consisting of data obtained and recorded by the device without any action by the user – and, taking into account the multiplicity of information processed, stored and transmitted by computer systems and networks, may contain a wealth of relevant information about the user and their personal characteristics and their use of the system. Thus, UNODC, “Introduction to digital forensics”, in Electronic Resources Laws on Sharing and Crime, available at https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-4/index.html, accessed on 1 May 2025.

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

more often than not it will actually be3 – in the interest of the criminal investigation and the carrying out of the justice.

According to Nhamitambo (2025), the Government of Mozambique is also fully aware 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 co-communications (article 253), Automated database (article 254), Unlawful access (article 256), Illegal recordings (article 257), Theft of fluids (article 276), Computer fraud and communications (article 289), Fraud relating to electronic payment instruments and channels electronic (article 294), Abuse of electronic means of payment (article 295), False computer science (article 336), Interference in data (article 337), Interference in systems (article 338), Misuse of devices (article 339), Public incitement to commit a crime (article tigo 345), Public apology for crime (article 346), Publicity of the conviction decision (article 448);

ÿ Electronic Transactions Law, approved by Law No. 3/2017, of January 9, which aims to protect consumers and regulate the use of electronic systems in the Government, sector private and civil society;

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

ÿ Telecommunications Network Security Regulation, approved by Decree 66/2019, of 1 August;

ÿ SIM Card Registration Regulation, approved by Decree 18/2015, of 28 August;

[3] According to DAVID SILVA RAMALHO, Hidden Methods of Investigation in a Digital Environment, Almedina, 2017, p. 102, digital evidence is currently present in most criminal proceedings. PEDRO DIAS VENÂNCIO, «Digital evidence and the digitization of evidence», in Boletim da Ordem dos Advogados, n.º 57, 2009, p. 33, states that «the future of Justice is closely linked to digital evidence». In turn, JOÃO CONDE CORREIA, «Digital evidence: the laws we have and the law we should have», in Revista do Ministério Público, n.º 139, 2014, p. 55, notes that this currently constitutes «the core of evidence».

ÿ Regulation for the Registration and Licensing of Intermediary Providers of Electronic Services Electronics and Digital Platform Operators, approved by Decree No. 59/2023 of 27 October;

ÿ Consumer Protection Regulation for Telecommunications Services, approved by Decree 44/2019, of 22 May;

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."

The research is qualitative and uses a bibliographic method.

THEORETICAL BASIS

Cybercrime: the modern relevance of digital evidence

Digital evidence is, and will increasingly be, a crucial means of evidence that may exist and be necessary to obtain in proceedings relating to any and all types of crime. However, it is undeniable that there is an umbilical and inextricable relationship between digital evidence and the phenomenon of cybercrime, since this type of evidence is essential in the investigation of this, both occurring in the same digital environment, and the means of obtaining digital evidence. Therefore, it is necessary to carry out a brief analysis of the phenomenon of cybercrime, its current importance and legislative developments at national and international level in combating this.

Digital forensics: principles and procedures for valid and effective data collection digital proof

Having established the sui generis nature of digital evidence, its technical complexity and its importance today, it is easy to understand the need for the emergence of an area specialized in dealing with this means of evidence: digital forensics, the branch of science forensics dedicated to the use of scientifically proven methods for identification,

acquisition, preservation, analysis and presentation of processed evidentiary data, stored or transmitted by computer systems – in general, for the procedure of obtaining digital evidence –, in accordance with the purposes of the criminal investigation and the administration of justice and in compliance with current legislation4 .

Currently, it is practically unanimous that obtaining this means of proof, to show valid in the eyes of digital forensics and therefore admissible in court with full evidentiary force, must be guided by four maxims: the legality of the action of all stakeholders; the existence of appropriate training and specialized support in order to to mitigate technical complexity; preserving the integrity of computer data in its original and unaltered form; and documentation of the entire procedure and maintenance of the chain custody that can guarantee the authenticity of the evidence in Court.

Regarding the legality of the procedure for obtaining digital evidence, the entity responsible for the criminal investigation department is responsible for ensuring full compliance with the law applicable throughout the procedure, as well as compliance with the requirements of the principle of proportionality and respect for the rights, freedoms and guarantees of those concerned.

As for specialization, whenever the person responsible for the criminal investigation is faced with, or is expected to come across digital evidence in the course of this, you should notify a a specialist (or a specialist team) in digital forensics in a timely manner and, if possible, ensure your presence in the procedure, in order to guarantee the follow-up of the best international practices in this area throughout the entire procedure; this support specialized must, of course, be constantly updated and aware of new developments in the area and be equipped with resources and equipment appropriate to the complexity technique of the procedure. Additionally, any participant in the handling of the evidence digital must have the necessary training for this, particularly in cases where it is not possible for an expert to be present on site in good time, and such training must also be extendable to any procedural participant, so that they have knowledge

4 Definition adapted from DIGITAL FORENSIC RESEARCH WORKSHOP, «A road map for digital forensics», in Proceedings of the Digital Forensic Research Conference, 2001, p. 16. COE, EEG, pp. 135-137 subdivides this branch into computer forensics – focused specifically on computers –, mobile forensics – focused on mobile computer systems, such as smartphones and wearables and embedded forensics – focused on integrated systems, such as those belonging to the Internet-of-Things, smart home devices, and automotive electronic systems, each with its –, network forensics – focused on computer networks –, and own specialized knowledge due to how different the procedure for obtaining evidence is in each of them. In a similar sense, MÁRIO ANTUNES / BALTAZAR RODRIGUES, Introdução à Cibersegurança, 2nd ed., FCA Editora, 2022, p. 149.

sufficient technical expertise to be able to detect any procedural irregularity that may compromise the probative value of the digital evidence presented in court and, thus, assess the validity of this.

As for preserving the integrity of the evidence, any action taken during the throughout the procedure it is possible to alter any computer data in the system that is the subject of the diligence, with priority being given to making a full copy (bit stream imaging)5 of the entire storage medium thereof, combined with the use of a write-blocker6 , this copy must then be subject to an integrity verification method (checksum, hashing or digital fingerprinting)7 and digital signature8 , and on the

which will affect the remaining measures to be taken in the seizure and analysis of specific data computer systems, in order to guarantee their authenticity and reduce the occurrence of evidence dynamics (the occurrence of any influence that alters, obscures or obliterates the evidence, regardless of the intention, in the period between its acquisition and its presentation in court).

As for documentation and maintenance of the chain of custody, it is crucial that all phases of the procedure are meticulously documented by the responsible investigator, carrying out namely the identification of relevant systems, the recording of computer data obtained, the description of the methods, techniques and tools used in the acquisition and analysis of these, and the way in which they were preserved throughout this process. The documentation prepared will be the main source of proof of compliance with the principles that guide the obtaining digital evidence, the validity of the steps taken and the admissibility and value of the evidence obtained, and must allow the procedure to be externally auditable98, being It is also based on this that the final report will be prepared.

[5] That is, the creation of an exact copy (or duplication), bit-for-bit, of the contents of the original storage medium and all data contained therein (including data of a temporary and volatile nature).
[6] A device or computer program that prevents any computer data from being altered during the duplication or copying process, a necessary step due to the volatile contents of the system memory, which can be modified with any operation performed.
[7] This corresponds to the assignment of a unique value to the clone obtained in the duplication process, calculated by the computer through a cryptographic function, and which ensures that no modification occurs, since the value resulting from the calculation of the altered data would be completely different, even if this modification were limited to one bit, thus allowing subsequent verification that no alteration occurred and that the forensic image is an exact copy of the original support.
[8] The researcher must, in this way, authenticate that all computer data were, under his/her responsibility, obtained in accordance with the technical and scientific requirements in force in the area at any given time.

As for the digital evidence itself, the general criteria for its technical admissibility mainly deal with its integrity, authenticity, reliability and credibility: this must be obtained in the least intrusive way possible and preserved throughout the procedure, not the way in which it was collected, handled, preserved and analyzed should raise any doubts about its veracity; the data generated by the user must be attributable to this and the data generated by the system must be considered as resulting from the operation adequate at the time they were produced, and it must be proven that both of these were collected using preservation methods that prevent any modification thereof; the information obtained must establish the facts in a way that is representative of its original state and, as such, indisputable, and must be persuasive as to to the facts it represents so that it can be considered true by the parties involved procedural to the point of substantiating a judicial decision.

RESULTS AND DISCUSSION

Classification of Cybercrimes

According to Nhamitambo (2025), **Pure computer crimes,** according to Amabélia Chuquela, are those in which the use of the computer system is the means necessarily used for the 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.

In our understanding, **pure or specific computer crimes** are those in which legislated by the first in criminal law, at the time the crimes committed by the computer and without its use, it would not exist. And, **Impure or improper computer crimes** are those in which the crimes already existed before the classification of cybercrimes. For the existence of it, the active agent or the criminal just uses a new way of carrying out the crime, a new tactic.

[9] Depending on the model followed, the division may be different, with one act or another being situated in different locations. In a similar sense to that followed here, ANTUNES/RODRIGUES, Cibersegurança, cit., pp. 154-155 and RAMALHO, Métodos Ocultos, cit., pp. 111 et seq. RODRIGUES, Prova Penal IV, cit., pp. 497 et seq. presents its own “dynamic-reversive model”, but whose phases, in general terms, would also fit here.

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) cited by Nhamitambo (2025), conceptualize virtual crime itself
such as those in which the computerized device and/or its content is the target of criminals -
computerized systems, databases, files or terminals (computers, smartphones)
nes, tablets) are attacked by criminals, usually after identifying vulnerabilities
des, either through malicious programs or social engineering (scammer tricks the victim,
causing you to provide personal and/or strategic information).

For Albuquerque (2006, p.168) cited by Nhamitambo (2025), impure virtual crimes
"would concern crimes in which computer resources constitute the means of execution,
having as its object legal assets that are already protected by existing criminal types". In society,
information age, the incidence of criminal offences "have as their material object or means of execution
implementation of the computer technology object: hardware, software, networks, etc.

Criminal investigation into digital media

According to Delbono (2018), **"forensic computing, forensic computing, forensic computing,
Digital forensic analysis or examination** is the application of scientific and analytical techniques
specialized technological infrastructures that allow identifying, preserving, analyzing and
present data that is valid within a legal process. Such techniques include
reconstruct the computer asset, examine residual data, authenticate data and explain the
technical characteristics of the applied use of data and computer assets".p. 160

Means of obtaining digital evidence in the face of anti-forensic measures

The prevalence of cryptography10 in the functioning of information technologies is exposed and
communication, as well as the accessibility of anti-forensic measures, are easily inferred
the difficulties that this situation represents in relation to the normal means of obtaining evidence

[10] Encryption is used to protect data from theft, alteration or compromise and works
transforming the data into a secret code that can only be unlocked with a unique digital key.

digital11. In fact, “day by day, new techniques of concealment or concealment are developed that make it difficult for authorities to identify the agent of the activities", which has «enhanced a widespread inadequacy of criminal law and procedure to effectively combat cybercrime»12. Let us explore in greater detail how encryption and other anti-forensic measures make it difficult (or impossible) to acquire digital evidence, comparing the means of obtaining this with the protection granted by it.

Therefore, the use of anti-forensic measures can make it difficult or impossible to identification of the relevant computer systems and the user responsible for the acts in investigation, particularly when these measures hide the digital trail of this or anonymize your network traffic, cutting off the investigation before it even has a chance chance of running. However, even when these systems are already identified – or are, at the very least, identifiable – anti-forensic measures may, in the phase of obtaining stricto sensu test.

The progressive protection of network traffic by cryptographic protocols is associated with a loss of readable access13 to more and more data relating to computer communications by part of the traditional communications operators, which constitute the cooperative entities

[11] In the Council of the European Union resolution on encryption (13084/1/20), which aims to reconcile “security through encryption and security despite encryption”, it recognised that encryption is a necessary means of protecting fundamental rights and digital security, but that at the same time it is necessary to ensure the ability of competent authorities in the field of security and criminal justice to exercise their legal powers. It also recognised the trend for applications and IT devices to encrypt stored data by default, and communication channels to be increasingly protected by end-to-end encryption, but that the inclusion of these encryption solutions (designed for legitimate purposes) in the modus operandi of criminals, as opposed to the increasingly evident dependence of authorities on access to electronic evidence to effectively combat serious and organised crime, makes the prevention, investigation and prosecution of crimes more difficult or virtually impossible. Finally, it acknowledged that it is necessary to “strike the right balance” that, regardless of the technological environment, allows the powers of competent authorities to be preserved in the performance of their duties, through lawful access to computer data that safeguards procedural guarantees and the fundamental rights of those concerned and that respects the principles of necessity, proportionality and subsidiarity. To this end, the European Union aims, in close consultation with service providers and other relevant stakeholders, to combine efforts and coordinate the investigative capacities of its institutions and bodies and its Member States, defining and establishing innovative approaches taking into account new technologies and examining appropriate technical and operational solutions.

[12] RAMALHO, Hidden Methods, cit., p. 98. The Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Union Strategy for Combating Organised Crime (2021-2025), COM(2021)/170, also recognises the continued loss of effectiveness of means of obtaining evidence and the need to adequately empower authorities in the digital age.

[13] That is, the data continues to exist, but in its encrypted version and, as such, useless as evidence, as it is not be able to access the information contained therein.

in criminal investigation in a digital environment par excellence, and which, in this way, have been replaced by other entities that make cooperation difficult (such as web service providers or anonymizing services), obtaining such data becomes dependent on these in case of encryption in transport, or, in cases of onion routing and end-to-end encryption, tip, in which there is completely no third party of a centralized nature with access to them, from the direct obtaining of their records (or, as we will see, their interception at the source) on the devices of those involved in the communication, i.e., at the ends14.

Additionally, the remaining anti-forensic measures may also make research and fruitless data seizure, particularly when potentially relevant data is are concealed by steganography techniques15, when they are previously eliminated in such a way as to leave no trace of them or altered to mislead the investigation, or when digital trail obfuscation tools are used that prevent the creation of such data.

In short, if the authorities can – naturally complying with the respective assumptions – order those who have availability or control of the data in question to communicate to the process or allow access to them, directly carry out a research and seizure of computer data present in a given computer system, or intercept computer communications, these means of obtaining evidence have been increasingly fruitless in the face of the growing use of anti-forensic measures aimed at to your frustration.

Digital or Information Technology (IT) Evidence

Digital evidence is a protected element in a digital medium. However, an assessment correct of what would be its reason for being in any information that, subject to intervention human, has not been extracted from a computer. IT evidence must be in a form

[14] It is therefore no surprise that there has already been a joint statement by Europol and European police chiefs against the progressive use of end-to-end encryption in instant messaging and Voice-over-IP communication services. EUROPOL, «European Police Chiefs call for industry and governments to take action against end-to-end encryption roll-out», available at https://www.europol.europa.eu/medi press/newsroom/news/european-police-chiefs-call-for-industry-and-governments-to-take-action-against-end to-end-encryption-roll-out., accessed on May 3, 2025. 15 It is the technique of hiding data within an ordinary, non-secret file or message to avoid detection; the hidden data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step to hide or protect data.

human readable or capable of being interpreted by people skilled in representing these information with the help of a computer program.

The main characteristics of all digital evidence are: that it can be volatile, anonymous, duplicable, alterable, modifiable and disposable. These elements are extremely importance at the time of a forensic analysis.

Sources of digital evidence

Digital evidence sources are containers of elements susceptible to investigation, because, in its content, the information generally associated with the owner of the medium is protected.

The following table shows the digital media and what sources of evidence they contain:

DIGITAL MEDIUM	APPEAL	EVIDENCE
Office and personal computers	Internal hard drives	Log files Cookies Hidden files Browsing history Printing spool Temporary, compressed, password protected and SWAP files
Pen drive access control device	Biometric proximity card	User identification data Access levels Permission Settings
Digital cameras	Memory card	Images Videos Sounds Recording date and time
Memory card		Images Document or spreadsheets Photographs
Printers - Scanners	Memory card in scanners	Documents
Access points on wireless routers		Configuration files
Diskettes - CD and DVD		
GPS - Cell Phones	Memory card Internal memory of the cellular device	SMS Whatssap Telegram Photographs Emails Videos Voice notes

Source: Author.

Identifying a hard drive, for example, is important for the validity of any medium.
of evidence, because once removed from the computer, it enters the chain of custody and is essential
to fulfill identification requirements when performing a skill.

Computer Expertise

The application of computer science in criminal expertise can be directly related to
forensic computing, a specific area of forensic science, and active in the military branch,
government and intelligence, which according to (ALTIMUS & KATEEB: 2014) computing
forensics can be defined as forms of analysis with the aim of involving preservation,
extraction and documentation of evidence obtained from digital media, arising from evidence
digital. The role of forensic computing has functions such as an investigative process, which
according to (SONNTAG: 2008), it can be considered the mixture between elements of the Science of
Computing and Law, focusing on the analysis and collection of information from computers,
networks, GPS data, wireless systems, storage devices (pendrives, hard drives,
cell phones and the like) how to solve and also understand the practices related to crimes
cybernetics and IT, in order to advance legal processes, being subject to fitting
in legal penalties according to the crime committed in question obtained through evidence during the
expertise.

In most cases, forensic computing will be directly linked to scientific police, its
practice will be carried out by an expert, who will use specific tools and resources to
the extraction of information that is necessary for the preparation of an expert report. In this
phase, the expert's prudence and knowledge will play extremely important roles in the
development of the criminal process, since the report must be precise and impartial, as well
therefore, in this report, the expert must describe in a formal, succinct and objective manner all
the procedures and technical examinations used in their expertise.

(FRANCE: 2005), states that an expert should be understood as a qualified person or
experienced in the subject being discussed, aiming, when requested, to clarify
facts that are in the interest of justice.

Examining the Evidence

In forensic computing according to (POLLIT et al., 2000), evidence can be represented by printers, chips and boards in general, central processing units, media storage and monitors, and can be easily described as a physical unit. In However, evidence, while stored on these physical media, will be latent and will only exist in a metaphysical electronic form. The examination process will make the evidence visible and at the same time explain its origin and significance.

Therefore, according to (NIJ, 2001), it implies that in the examination phase, several things must be carried out. First, the content and condition of the evidence in its entirety. This documentation will allow all parties to find out what will be contained in the evidence. In this process, the search for information that may be hidden is also included. Once all the information becomes visible, the process of reducing data can begin, as a practice of refinement or filtering. Given the huge amount of information that may be stored on a storage medium, this part is considered fundamental. However, (POLLIT et al., 2000), emphasizes that evidence is not will always exist in isolation, this evidence is a product of stored data created through the use of an application.

Extracting Evidence

According to (NIJ, 2004), the extraction of digital evidence should be cautious due to its fragility, that is, improper handling or examination, may result in damage, alteration or even destruction of evidence. An examination resulting from errors committed by the in charge of the expertise, may be liable to imprecise conclusions, and are therefore highly recommended to take into consideration the preservation of this type of evidence. However (POLLIT et al.,2000), argues that the biggest challenge for forensic computing is to develop methods and techniques that allow obtaining valid and reliable results at the same time that protect the evidence from possible damage. The extraction of digital evidence will be carried out through a broad use of resources, through software, hardware or tools for this purpose. In this way, the extraction of evidence can be carried out through the most varied methods.

Logical Extraction

Logical extraction consists of acquiring data in files and directories from the device's operating system. (MOOIJ, 2010), explains that logical extraction can be carried out in two ways: Software-Hardware Units or Software specific to the carrying out logical extraction. However (BEN-MOSHE, 2012), confirms that, no matter how much the logical extraction becomes a considerably fast process, of low complexity, however, it has the disadvantage of limiting data acquisition, since in this practice it will not be possible possible to obtain data deleted from the system. “Logical extraction involves extracting data using the device's operating system through a set of commands known (e.g. AT commands). This means that extraction tools data communicates with the device's operating system and requests information from the system. This allows most of the device data to be acquired in real time. real." (CELLEBRITE MOBILE SYNCHRONIZATION LTD, 2014).

Physical Extraction

Physical extraction consists of a scan followed by the acquisition of data contained in the flash memory of the device, and then a detailed copy (bit by bit) is made. According to (MURPHY, 2014), summarizes, stating that physical extraction can also be called physical acquisition, or otherwise physical memory dump, such that the data obtained comes as a raw hexadecimal dump, which can be analyzed later to obtain legible information that is deemed necessary. In this extraction method, because it is of high complexity, there is the advantage of being able to acquire deleted files from the system, and through logical extraction, this could go unnoticed. However, there is its disadvantage, this practice is time-consuming and requires decoding (MOSHE, 2012). It is worth mentioning that flash memory was developed from an EEPROM (Electrically Erasable Programmable Read-Only Memory and Electronically Erasable is non-volatile memory, meaning your information will still be stored even without the presence of a power source. In the case of a scan for data extraction on a mobile device, the tool will make an acquisition directly on the Flash memory of the same.

Manual Extraction

This method is considered a last resort and not highly recommended, as which depends on the manual work of the expert in charge, and as mentioned previously, may result in loss or possible damage to the evidence, which will in fact result in imprecise and poor character conclusions in obtaining evidence. At this stage of extraction, the user in question will extract the information through access to the operating system and then selectively, evidence that is considered relevant to the fact to be judged will be acquired. It is a very slow process that requires patience and time, therefore, it is used only as a last available resort.

Tools Used

In forensic computing, there are countless devices, techniques, resources and tools used for evidence extraction, whether in Software or Hardware solutions. Examples such as XRY, Cellebrite UFED, Solo4 and the Tableau writeblocker line are among the most famous devices used in computer forensics.

Micro Systemation XRY

Developed since 2003 by the Swedish company Micro Systemation, XRY is a software designed for the forensic extraction of data from mobile devices such as Cell Phones, Smartphones, Tablets and also GPS navigation systems.

“The XRY system is the first choice among law enforcement agencies worldwide, and represents a complete mobile forensic system supplied with all necessary equipment what is needed to perform a forensic examination of a mobile device” (MICRO SYSTEMATION, 2014)

It has several versions, such as the following:

Logical

As the simplest version, XRY logical is the software-based solution for any PC with Windows platform. In this version, it has the necessary hardware for carrying out expertise on mobile devices, making it suitable for carrying out a logical data extraction.

Physical

XRY Physical is the solution based on forensic recovery of deleted or protected data, therefore, obtained by physically extracting data from the device.

Complete

It consists of the kit containing the logical and physical functions included. Widely used and recommended in obtaining evidence from mobile devices, in this version the user will count also with devices for cloning SIM cards, a unit of communication and its corresponding tools necessary for physical or logical extraction, so that the user obtains data extraction with the maximum efficiency possible.

Field Version

In this version of the device, it is suitable for portable use immediately, being then for use in the field (from the English Field). According to (MICRO SYSTEMATION, 2014), this version satisfies some organizations, which frequently requested kits forensic instruments that were portable, ergonomic and flexible, so that they could be carried out on-site inspections and could then easily connect to the network or in remote computers. This version comes with the Panasonic CF-18, or otherwise called Toughbook, a very robust, portable computer with high battery life, which was developed from the military standard MIL-STD-810F to withstand extreme conditions, considering that its case is made of a resistant magnesium alloy.

Cellebrite UFED

Developed since 1999 by the Israeli company Cellebrite Mobile Synchronization LTD, the UFED series or Universal Forensic Extraction Device, is acting as a competitor directly from the Micro Systemation XRY. Widely used by military forces and also by intelligence agencies, is an important tool for extraction, decoding and analysis of mobile device data. The UFED series also has a wide range of versions, being the field options (TK - Turn Key), Touch Logical, Touch Ultimate, 4PC Logical, 4PC Ultimate.

Touch Versions

According to (CELLEBRITE, 2014), the Touch version was developed as a standalone, a independent device created exclusively for carrying out forensic extraction of mobile devices. UFED Touch has an intuitive, touch-sensitive interface (touchscreen), also enabling physical extraction (in the Ultimate version), logic (in the Logical version), file systems and all types of data and passwords, including also deleted files from a wide variety of mobile devices. In addition to being a portable version, the UFED Touch also has the operating kit (cables, connectors, etc.).

4PC versions

The 4PC version was developed as a forensic solution that runs on a hardware existing, that is, on a computer or a notebook. This version is versatile and has a variety of applications, accessories and peripherals. In the Ultimate version, it has the possibility of carrying out physical extraction.

TK Version – Turn Key

Considered the most complete version of the UFED series, the TK or Turn version Key, was developed for recommended use in the field, providing the user with all the applications along with all the necessary apparatus to carry out forensic analysis in adverse conditions. Just like the XRY Field Version from Micro Systemation, the TK version in addition to also having Panasonic's line of resistant and robust laptops, the TK version features the Toughbook CF-18 and CF-53, or the Toughpad G1.

Solo4

Developed by the American company Intelligent Computer Solutions – ICS, the Image MASSter Solo4 is made up of hardware specialized in high-speed acquisition and duplication of data from Hard Drives, widely used in forensics. The transfer rate and copying data through this device, corresponding to 13GB/min and reaching incredible 18GB/min, with support for SATA-2, IDE, SAS and USB interfaces. Using this equipment, is related to the duplication of large quantity devices storage, that is, HDs, which can be used to duplicate the Hard Drive without the

aid of a computer, so the SOLO-4 works as a device characterized as
standalone, that is, it can be used in the field. However, the SOLO-4 is also capable of
perform the sanitization of a hard drive, which according to (ARANHA, 2013), can be summarized as
effectively delete all data from a disk.

Tableau

In the forensic computing environment, the American company Guidance Software developed the
device called “Tableau” functioning as a Duplicator and Write Blocker, but it continues
the question: What is a Write Blocker? “Forensics bridges (write blockers) are
fundamental in any computer forensics kit. Examiners have in their hands a
high-speed technology capable of generating images of today's large hard drives and
fast, both in the laboratory environment and in the field.” (DIGITAL FORENSICS, 2014)
Forensic bridges, known as Write Blockers, consist of tools that perform
the forensic image of the evidence having only access to the Read-Only function, that is, it has
read-only access to a storage device without compromising its integrity
of evidence, protecting your data. This tool is directly linked to the foundation
mainstay of forensic computing, based on maximum preservation of chain data
custody.

Investigating the Cloud

In every forensic investigation, we not only look for relevant information on devices
digital, but we also ascend to the virtual space, currently called **cloud** or **cloude,**
where social networks and the deep web are located.
It should be clarified that since the cloud is a virtual space, there is a timely approach to
technological research, but there is also a legal aspect in which forensic investigators have
a limitation. Much of the information contained on social networks or websites is private and, to
To obtain them, you must ask for authorization from the judge of the jurisdiction and, if the suspicious sites are
foreigners, the request will be made at an international level.
Without a doubt, in technical work it only reaffirms evidence or those that are conducive to the procedure.
so that the judicial operator, when faced with a complaint, can begin his investigation work.

An important element for any cloud event is the preservation of evidence, which is observed using specific tools or software to give them a true existence.
The participation of a notary may be useful, who will contribute to the expert's report. computer science for your notarial act.

Six degrees of separation theory

The emergence of social networks has generated a type of social phenomenon in man that is rarely seen before. corresponded. Facebook, Twitter, LinkedIn and others that allow you to establish relationships personal between users, being able to share material (files or images), thoughts or reflections of their intimate life. It is not strange to discover in these networks that their users feel pain or joy, as well as the story of a journey or the acquisition of something good.
The six degrees of separation theory attempts to prove that any person on Earth can be connected to another through a chain of acquaintances that is no more than five or six intermediaries.
This applies to today's social networks, where a user has a significant number of of contacts that actually come from a generator contact and generally do not know or shares tastes or affinities.
But not all that glitters is gold and not everything that is shown on social media is information. pleasant. These networks have often been used for complex purposes, such as pornography or pedophilia. For these cases and in the case of an illicit complaint, essential aspects such as: validation of the attacking users (they have an identifying ID), capturing evidence of the content observed on the screen must be taken into account, identifying, validating and recording electronic evidence through established protocols or good practices.
Furthermore, the possibility of preserving digital evidence must be managed with the performance of a notary that provides a first-level legal framework for the work of the computer expert.
If any of the premises discussed are not fulfilled correctly, the evidence presented may be challenged and the evidence supporting the case will be lost.

Deep alert

In the deep web or the invisible web you can not only browse the internet through conventional browsers, such as Firefox, Chrome or Internet Explorer and with which you can obtain a variety of information, usually indexed and often repetitive, which is called the surface web or superficial web.

The so-called deep web, dark web or invisible web is part of the Internet content that is not can be accessed by conventional search engines such as Google, Yahoo! Bing or Duck Duck Go, or through classic browsers, mentioned above.

When browsing in conventional browsers, our visits are tracked through our IP address, provided by our Internet service provider. On the other hand, browsing the The deep web is virtually anonymous and our visits are not tracked.

Browsing the deep web allows us to enter a world that is often dangerous and without security, especially for inexperienced Internet users. The material is generally varied, from child pornography to drug trafficking, hackers and people who wipe records criminals.

Web pages in surface navigation are www.unapagina.com; instead, in deep web, the format looks like onion asd67asdt124byasdfyieerbhi34y8 (dot) and they are encrypted.

The first-tier application for browsing the deep web is called tor or tor network.

This browser uses Mozilla Firefox's privacy-optimized and open-source software16, which allows the user to browse anonymously by hiding their IP address. You can access potentially blocked websites and most importantly, it does not track the user.

Investigating criminal elements at this stage, there are numerous contents with material potentially likely to commit a crime, its verification is not easy, especially when the human being must be found behind the keyboard. The performance of a task of intelligence in this network implies the appearance of the secret agent, a figure not always accepted in the judicial field.

[16] Copyright gives the right to study, modify, and distribute the software freely to anyone and everyone. any purpose.

In principle, there would be another alternative to detect criminals. Furthermore, one should know deeply how to navigate and assess, if potential criminals make a mistake, so that they reveal their identity.

Cloud research using open sources. “Information is power”

The term open sources or osint refers to all information published on the Internet and open to the public. This information is characterized by being chaotic, disorderly and disqualified, as well as allowing decisions to be made for the person who ordered the investigation.

The word "int" is not only associated with osint, but with other ways of performing the intelligence, which are:

- Humint: These are sources of information generated by human beings.
- Sigint: Sources of information obtained from digital elements.
- Geoint: This is information that comes from satellites.

To conduct open source research, it is useful to know what sources are used, as well as be able to find them. Almost as a spin-off from the previous point where deep browsing and its dangers have been explained, potentially useful research sources are found in deep web and also on the surface.

Another element that the researcher must take into account is that many tools are free, but other paid ones, not all tools get information locally and can only be used outside.

The information obtained is chaotic and unclassified, and it is the researcher who must give the he, with his experience, a practical and precise approach to future decisions.

Evidential problems in cybercrimes

As a fundamental instrument for determining and conditioning a research model digital forensics, the digital evidence will be identified in order to recognize the various phases procedural, and what content corresponds to each one. However, despite the impact that had in determining the necessary standards that should characterize the digital proof, the The reality is that, as it is a technically complex test that lacks interpretation specialized, this scenario will be difficult to assert. In the vast cyber world, the proof

digital must be collected quickly, complying with all necessary precautions, under penalty to lose integrity. Therefore, the investigator must consider the evidence by its nature ephemeral, which makes it difficult to preserve it in an electronic-digital device that allows increase its period of investigative usefulness, beyond what is naturally considered. To In addition to being temporary, digital evidence is also fragile and changeable, falling on the investigator forensic the need to redouble the care to be taken. Before collecting the evidence, you should identify, in an even more rigorous manner, what type of digital evidence is in question. Only with this identification, the investigator will be able to guarantee the probative force of the digital evidence, without danger of this, be changed or disappear. If there is this possibility of change or disappearance, the investigator must also consider digital evidence due to its nature volatile and unstable. The instability demonstrated by this test, arising from the constant mutability that characterizes it, makes it more difficult to grasp. This difficulty is seen in situations where the investigator is initially faced with evidence with certain characteristics, and later, this is modified, totally or partially. Digital proof consists still in immaterial evidence. In this way, the immateriality of digital evidence will impose on the forensic investigator must be knowledgeable in specific techniques, otherwise he will lose the strength of evidence, in the event that the investigator significantly alters it, due to ignorance of its presence. This need for the researcher to have technical and scientific knowledge must particularly to the complexity and codification that characterize digital evidence. In this way, to access computer systems or networks, the researcher must equip himself with all the techniques and scientific knowledge, to use keywords or use search techniques decryption. In certain situations, forensic investigation should take into account the dispersion of digital evidence, that is, it may be distributed across several “terminals, computers and networks that extend over a vast spatial or geographic area.”

Emerging in a digital environment, the approach to forensic investigation should be based on with the diffuse and dispersed nature of computer crime, there being no concentration of its constituent elements of the computer complex. As mentioned, digital evidence covers momentary electromagnetic impulses relevant to the computer network or system electronic communications. Therefore, digital evidence is characterized as dynamic and changeable. The The researcher's skills require that he/she carry out a structured investigation

temporally, comparing several time periods, allowing access to digital evidence of greater usefulness for research.

An approach generates, in the field of work appears on the scene with its own vicissitudes evidentiary. First of all, it should be remembered that in law, particularly in procedural law, criminal, the principle of freedom is governed by which, as is known, the facts investigated can be proven by resorting to all types of elements of conviction, as long as the constitutional guarantees of those involved are not violated.

As **Sueiro** explains in his book on computer crime cases: “although until the there has been no reform in the area of computer crime…, the truth is that increasingly imperative, indispensable and necessary, due to the gradual change in criminal proceedings, from physical, bodily or tangible evidence to digital evidence, electronic or intangible.”

The use of services like Google Maps, emails, screenshots, are old - recordings of audio and/or video on CD, DVD or USB or their respective frames - serve many purposes times, as crucial evidence for the discovery of cybercrimes.

It is clear that the challenges that cybercrime poses to judicial operators are not minors, forcing us every day to make great efforts to keep up with the times, if our function is to create an imputation or, on the contrary, to counter an accusation by means of of counter-tests and automatic by Internet sites or stenographies - hidden drawings in the which, when clicked, are activated and allow you to discover what is hidden below the original.

Example in Comparative Law:

A case involving a university systems engineering student who, through an IP located abroad, made an improper transfer of money between bank accounts in the country, Cassation confirmed his conviction for the crime of fraud through manipulation techniques of the computer as a phishing author. In addition to the technical incapacity invoked by the defense, a since this does not correspond to the tasks he performed on behalf of his employer or of his character as a university student of systems engineering, is present necessary logical relationship between the different pieces of evidence, through which it was possible to discover who, through computer manipulations, had improperly extracted funds from the account banking.

Internet Protocol

Internet Protocol - is a set of numbers (four decimal numbers, separated by a dot between them) that identify the interface of a device (a computer, smartphone etc.) on a network that uses the Internet Protocol (IP). The existence of IP is due to the the fact that information circulating on the network needs to know where to go and where to go should go. There can be two types of IP: a static one (it is unique and always the same) or a dynamic one (it is changed upon reconnection). An Internet service provider that has a contract with a Internet subscriber typically maintains a historical file with the assigned IP address (fixed or dynamic), the subscriber identification number, the date, time and duration of the address assignment in the same way if the Internet user is using a network public telecommunications company, such as a mobile or landline phone, the telephone company also will record the number dialed, along with the date, time and duration of the billing subsequent.

To provide the tests with the necessary safety guidelines (no pollution, no loss of security chains, inalterability), official experts are used, compared to other evidence. At the trial stage, they must be presented at the request of the party and with their control, like any other evidence.

There is practically no daily activity that does not incorporate into its development any digital or computational resource. It is said that every digital medium associated with human beings is a extension of your life, where personal and professional events take refuge and, why not, criminals, depending on the idiosyncrasy of the individual.

Computer tests can be planted on virtually any digital resource, where the investigator's ability and knowledge of his computer tools will provide a successful outcome to what is investigated, providing the judge or requesting a investigation sufficient elements to decide on a case or legal proceeding.

The biggest problem with the propatorial regime in cybercrimes is the need to ask for a judicial authorization for the collection of evidence. Since it may be the case that the expert have the proper authorization while the traces do not exist.

Another problem that prevails regarding the collection of evidence is that there is no practice of crime that manifests itself in flagrante delicto.

Breaking telematic confidentiality to obtain evidence in civil actions

The inviolability of the secrecy of correspondence and telegraphic, data and electronic communications telephone communications, which is a true corollary principle of inviolability provided for in the CRM, in line with the guarantees of privacy, honor and dignity of the person human. The area in question is the right to privacy, considered by a large part of the doctrine as an integral part of personality rights and, intended to protect the dignity of the human person, since "the rights to privacy and one's own image form the constitutional protection of private life, safeguarding an intimate space that cannot be crossed by external illicit interference" (MORAES, Ibidem, p. 47).

The original Constituent Assembly understood that it was best to specifically protect the image, private life and the privacy of citizens, thus providing on the matter:

Which provides for the right to privacy, giving each individual the possibility to oppose resistance to non-consensual interference in their private and family life, preventing disclosure of private content information.

However, given that this is a fundamental right, intended to protect one's own moral integrity of the individual, the enjoyment of the right to privacy is not absolute. As with all individual freedom, the exercise of this right is conditioned on the realization of coexistence ideal social, and cannot serve as a protective shell against illicit practices.

Like every individual right provided for and guaranteed in the CRM, the right to privacy is turned in favor of a greater interest, which is the social interest.

Given the impossibility of legally predicting, on a case-by-case basis, the limit to be established between the public and private interest, the Courts are responsible for determining the flexibility of individual rights, in the name of the community. It is in this context that telephone interception appears, as an exceptional measure, considered legitimate, only and solely, when the formalities, demands and requirements are observed legally imposed, since interference in people's private lives is, in principle, offensive to fundamental rights.

Telephone interception is the result of the need, perceived by the legislator, to equip itself with society with instruments that enable the containment of growing organized crime in the face of of the great evolution in communication systems, mainly telephony, now used by large-scale organized crime, even due to the ease of its acquisition.

Telephone interceptions, once legally regulated and carried out with obedience to the requirements imposed by our legal system, are accepted as lawful evidence, being admissible its result as a source of evidence in the proceedings.

It is essential that the court order be accompanied by a true and proper motivation, specifically linked to the specific situation. The lack of justification is grounds for nullity of the diligence, causing the uselessness of the evidence and leading to the invalidation of the material.

The judge must verify, when ordering the investigation, whether, in relation to the particular type of act imputed to the subject, the usefulness of the resource for evidentiary purposes is evident or convenient for the criminal investigation. The judicial authority must, in the motivation of the authorization for telephone interception, the following observations: compliance of the investigation for the purposes of criminal instruction; occurrence of a well-founded reason for which it is believed that the interception can provide useful elements for the development of instructional activities; assessment of the opportunity that allowed such serious interference in the interference in the lives of others, with regard to the likely obtaining of such evidence.

Access to data stored on electronic devices through search warrants and seizure

The restrictive constitutional interpretation given to the secrecy of communications, namely that it would only protect (content of) communications while they are in flow, it creates a situation of normative mismatch: modern cell phones, tablets and computers store a huge amount of information, photos and communications that offer faithful portraits and details of their owners, but which would not enjoy the same protection as communications in flow by the mere fact that they are now archived. It is under the terms of art. 68 of the Telecommunications Law, guaranteeing the confidentiality of communications transmitted through public telecommunications networks. Unless it is a matter of criminal.

The breach of telematic confidentiality to obtain evidence in civil proceedings is only permitted with judicial authorization. As well, liability for damages may also occur for the practice of a computer crime, under the terms of article 483 of the Civil Code, which, "He who, with intent or mere negligence, unlawfully violates the right of another or any provision

legally intended to protect the interests of others is obliged to compensate the injured party for the damages resulting from the violation".

Computer Science, the Internet and the Philosophy of Evidence

The advent of the internet has led to new problems arising in the courts in several areas that jurisprudence has gradually tried to resolve.

There are numerous legal issues that can arise and be related to the internet: digital evidence and assessment of this evidence, digital process, civil and criminal liability, disciplinary, copyright, privacy and fundamental rights of citizens, the responsibility for content posted on the internet, the protection of computer data, among others others.

Digital evidence is valid and necessary when it becomes imperative to substantiate or to determine the veracity of a party's allegation in a hearing, if there is no other means, serves then this, to verify statements, actions and perhaps decipher intentions that are denoted fundamental to the judge's conviction regarding intent.

In fair measure, digital evidence will not be a means of proof that answers all doubts. placed in court, however, it will be demonstrated countless times that for a certain type of criminality, be the only means of proof capable of creating conviction of truth in the judge.

Likewise, in the context of investigation, as a means of obtaining evidence, it does not replace in any way, no means of obtaining evidence already existing in the Code of Criminal Procedure. However, in certain types of research (not only those directly related to the cybercrime), can become a fundamental tool, having as its characteristic its special speed, immediate, as opposed to the investigation of a so-called 'traditional' crime. The competent entity, in its investigation, will be able to inspect the electronic traces left by the crime in the preparation phase, at the time of execution, and even if already consummated.

It is also easier and more convenient to obtain evidence through data content, than by resorting to the usual means of obtaining evidence.

This reality is also likely to generate growth in the scope of the valuation of Circumstantial evidence17 and especially a simplification of the evidence of the facts alleged in the judgment.

Telecommunications operators are reserved about the preservation and presentation of this evidence, in the sense that the simplification of international cooperation in this registration, have demonstrated a high rate of effectiveness, leading to convictions without actually the need to demonstrate the facts attributed to the defendants, resorting to seizure of data content. It is understood here that the basis is that the research carried out according to the procedures for international cooperation are sufficient to discover the relevant facts.

In this way, the use of evidence considered to be safer is called for, and which in turn is reflects a criminal investigation with minimal risks for the respective agents competent in the investigation.

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.

17 The distinction between direct evidence and circumstantial evidence is classic. Direct evidence refers to the facts that are proven, the subject of the evidence, while indirect or circumstantial evidence refers to facts that are different from the subject of the evidence, but which allow, with the help of rules of experience, an inference as to the subject of the evidence. Circumstantial evidence, more than any other, involves the intelligence and logic of the judge. Circumstantial evidence presupposes a fact, demonstrated by means of direct evidence, to which a rule of science, a maxim of experience or a rule of common sense is associated. This circumstantial fact allows the elaboration of a fact that reveals a consequence by virtue of a rational and logical connection. Furthermore, it is important to note that circumstantial evidence, or the operation of logic and presumptions, as well as the maxims of experience, is transversal to the entire theory of evidence, starting with the investigation of the subjective element of crime, which can only be achieved in this way, up to the actual accreditation of direct evidence contained in the testimony. (Speech at the Macau Legal and Judicial Training Centre on 30 November 2011)

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.

The classification of cybercrimes in Mozambique has evolved considerably, having been Law No. 35/2014 of December 31 was approved. It contained only 9 (nine) crimes computer science. And, in 2019, with the approval of Law No. 24/2019, of December 24, it went from 9 (nine) to 19 (nineteen) computer crimes classified and punished by criminal law.

Regarding evidence in cybercrimes, joint work is required between the Justice Administration Bodies for this purpose.

REFERENCES

Andrade, Manuel da Costa. 1994, “On valuation as a means of evidence in criminal proceedings of recordings produced by individuals”, Studies in Honor of Professor Eduardo Correia, Volume I, Coimbra.

ANTUNES, Mário / RODRIGUES, Baltazar, Introduction to Cybersecurity, 2nd ed., FCA Editora, 2022.

ÅRNES, André, Digital Forensics, Wiley, 2018 EUROPEAN DATA PROTECTION AUTHORITY, «Quantum computing and cryptography», in TechDispatch, No. 2, 2020.

AYCOCK, John, Computer Viruses and Malware, Springer, 2006.

BELEZA, Teresa Pizarro / PINTO, Frederico de Lacerda da Costa, «Criminal evidence and the defense guarantees: reading lines and tension points», in Criminal Evidence and Law of Defense, Almedina, 2010 BERCOVITZ, Rachel, «Law Enforcement Hacking», at Columbia Law Review, vol. 121, no. 4, 2021.

ABEL, Wiebke / SCHAFER, Burkhard, «The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822», in SCRIPTed, vol. 6, no. 1, 2009 ALBERGARIA, Pedro Soares de, «Article 125th – Legality of evidence», in Judicial Commentary on the Code of Criminal Procedure – Volume II, 3rd ed., Almedina, 2021.

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.

NHAMITAMBO, Raul de Miguel Benjamim Jofrisse. Computer crimes in the Mozambican legal system system. **RCMOS - Multidisciplinary Scientific Journal of Knowledge,** Brazil, v. 1, n. 1, 2025. DOI: 10.51473/rcmos.v1i1.2025.976. Available in: https://submissoesrevistacientificaosaber.com/index.php/rcmos/article/view/976. Accessed on: May 9, 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, «Guide to integrating forensic techniques into incident response», SP 800-86.

NEVES, António Castanheira, «The unity of the legal system: its problem and its meaning» had», in Digest, vol. 2, Coimbra Editora, 1995 — Summaries of Criminal Proceedings, 1968.

NEVES, Rita Castanheira, Interference in Electronic Communications in Criminal Proceedings, Coimbra Publishing, 2011.

NIELSEN, Jakob, «Nielsen's law of internet bandwidth», in Nielsen Norman Group, 1998.

NUNES, Duarte Rodrigues, «The admissibility of obtaining, directly by the authorities, location data through a GPS system in light of Portuguese criminal procedural law», in Judging, No. 32, 2017.

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. **11/2023:** Amends number 3 of article 311 of the Constitution of the Republic of **2004,** amended by Law No. **1/2018,** of June 12. National Press, Mozambique, MPT, 12 June.

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 December 12. Approves the Control Regulation Telecommunications Traffic. National Press, Mozambique, MPT, December 12.

MOZAMBIQUE, Law No. 25/2019, of December 26. Approves the Law revising the Code of Criminal Proceedings. National Press, Mozambique, MPT, 26 December.

MOZAMBIQUE, Decree-Law No. 1/2005, of December 27. Introduces amendments to the Code of Civil Procedure. National Press, Mozambique, MPT, December 27.