RCMOS – Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. Sao Paulo-SP.
Year V, v.1, n.1, Jan/July 2025. | submission: 2025-06-19 | accepted: 2025-06-21 | publication: 2025-06-23

Unlawful access as a form of data breach in Mozambique

Illegitimate access as a form of data breach in Mozambique

Illegitimate access as a form of data breach in Mozambique

Raul de Miguel Benjamin Jofrisse Nhamitambo1
Alvaro Rui Massingue2
Elvis Ernesto Job3
Emerson Sergio Guissiuana4
Juvencio Jonas Miambo5

SUMMARY

This research aims to analyze Unlawful Access as a form of Data Violation in Mozambique. In the Mozambican context, illegitimate access to data emerges as a critical challenge in the digital contemporary world, characterized by the obtaining, use, modification or disclosure of digital information without due authorization or legal support. The Electronic Transactions Law of Mozambique (approved by Law No. 3/2017, of January 9) and the Penal Code (approved by Law No. 24/2019, of December 24), describe unauthorized access to computer systems or databases, underlining the seriousness with which the legislator views this problem. The increasing digitalization of services, both in the public and private sectors, highlights the importance of data protection. The exposure or misuse of personal and sensitive information can trigger a series of harmful consequences. The advancement of information technologies in Mozambique has brought with it opportunities, but also serious risks to the privacy and digital security of citizens and institutions. One of the main risks is illegitimate access to personal data, which

[1] PhD in Legal Sciences, from the University for International Cooperation in Mexico (UCIMEXICO) - Mexico (2020); Master in Legal Consulting for Companies, from the University of Madrid (UDIMA) - Madrid (2016); Bachelor of 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 Higher Institute of Accounting and Auditing of Mozambique (ISCAM), teaching the subject Taxation Complements in the Master's Course in Auditing; Author, Reviewer, External Evaluator and Peer in the Multidisciplinary Scientific Journal O Saber (since II Semester of 2024); Author, Evaluator and Peer in the Multidisciplinary Journal RECIMA21 (since I Semester of 2025) and Evaluator and Peer in the International Journal Consinter of Law (International Council for Contemporary Studies in Postgraduate Studies - CONSINTER), since II Semester of 2025 and Organizer of the Digital Scientific Publisher (since I Semester of 2025). Matola – Maputo.

ORCID: 0009-0006-4118-1970. rnhamitambo@gmail.com,(+258) 872058783/847417800.
[2] Third-year student of the Bachelor's Degree in Information Technology and Systems Engineering at Joaquim Chissano University.

[3] Third-year student of the Bachelor's Degree in Information Technology and Systems Engineering at Joaquim Chissano University.

[4] Third-year student of the Bachelor's Degree in Information Technology and Systems Engineering at Joaquim Chissano University.

[5] Third-year student of the Bachelor's Degree in Information Technology and Systems Engineering at Joaquim Chissano University.

consists of obtaining, using or manipulating private information without due consent or legal authorization.

Keywords: Illegitimate Access; Data Breach; Privacy; Digital Security.

ABSTRACT

This research aims to analyze Illegitimate Access as a form of Data Breach in Mozambique. In the Mozambican context, illegitimate access to data emerges as a critical challenge in the digital contemporary world, characterized by the acquisition, use, modification or disclosure of digital information without due authorization or legal support. The Electronic Transactions Law of Mozambique (approved by Law No. 3/2017, of January 9) and the Penal Code (approved by Law No. The increasing digitalization of services, both in the public and private sectors, emphasizes the importance of data protection. The exposure or misuse of personal and confidential information can trigger a series of harmful consequences. The advancement of information technologies in Mozambique has brought with it opportunities, but also serious risks to the privacy and digital security of citizens and institutions. One of the main risks is illegitimate access to personal data, which consists of obtaining, using or manipulating private information without due consent or legal authorization.

Keywords: Illegitimate Access; Data Breach; Privacy; Digital Security.

ABSTRACT

This investigation aims to analyze illegitimate access as a form of data breach in Mozambique. In the Mozambican context, illegitimate access to data emerges as a critical challenge in the contemporary digital world, characterized by the acquisition, use, modification or dissemination of digital information without the need for authorization or legal support. The Law of Electronic Transactions of Mozambique (approved by Law No. 3/2017, of 9 January) and the Penal Code (approved by Law No. The increasing digitalization of services, both in the public and private sectors, emphasizes the importance of data protection. The exposure or misuse of information Personal and confidential can trigger a series of harmful consequences. The advancement of information technologies in Mozambique has brought with it opportunities, but also serious risks to the privacy and digital security of citizens and institutions, which consists of illegitimate access to personal data. to obtain, use or manipulate private information without the need consent or legal authorization.

Keywords: Illegitimate access; Data breach; Privacy; Digital security.

INTRODUCTION

In this paper we will discuss Illegitimate Access as a form of Data Violation.

in Mozambique. The increasing digitalization of contemporary societies has brought with it

a series of challenges, especially with regard to information security and protection of personal data.

In Mozambique, illegitimate access to data has become a growing concern, reflecting not only the vulnerability of technological infrastructures, but also the lack of robust legislation regulating privacy and data protection. This phenomenon is not not only a technical issue, but also a social one, since a data breach can have devastating consequences for individuals and organizations, undermining trust public and the integrity of institutions. The relevance of this topic is evident, considering the current context of Mozambique, where digitalization is advancing rapidly, but without due attention to security issues.

Lack of awareness about the importance of data protection and scarcity of resources for the implementation of effective security measures further aggravate the situation. In addition Furthermore, the growing interconnection between digital systems and platforms makes the country a target attractive to cybercriminals, who exploit existing weaknesses.

In the contemporary digital age, the protection of personal and corporate data has become a fundamental concern for individuals, organizations and governments around the world. In Mozambique, a country that is experiencing significant growth in the use of technologies information and communication, illegitimate access to data emerges as an increasingly serious threat concerning privacy, security and economic stability.

Unauthorized access can be defined as unauthorized entry into computer systems. or databases, with the purpose of viewing, copying, modifying or destroying information confidential. This practice constitutes a serious violation of the fundamental rights to privacy and protection of personal data, as well as representing a threat to security national and the integrity of institutions. The Constitution of the Republic of Mozambique, enacted in 2004, establishes in its article 71 the right to privacy, including inviolability of communications. However, specific legislation on data protection and information security still presents significant gaps that make it difficult to combat effective against illegitimate access and other forms of data breach.

The research is qualitative and uses a bibliographic and documentary method.

THEORETICAL BASIS

Unlawful Access and Data Breach

Illegitimate access to information systems constitutes one of the main threats to security digital today. According to Sêmola (2014), illegitimate access can be defined as "any attempt to enter or use computing resources without due authorization, aiming to compromise the confidentiality, integrity or availability of the information". This definition covers both external and internal attacks, carried out by unauthorized individuals or by persons exceeding the permissions granted to them granted. According to Pinheiro (2018), data breach refers to the "compromise of confidentiality, integrity or availability of personal data or sensitive, resulting in unauthorized access, destruction, loss, alteration or disclosure." In Mozambican perspective, this definition takes on specific contours due to the social, economic and technological particularities of the country.

Historical Evolution of Data Protection

The protection of personal data emerged as a global concern from the 1970s onwards, with the advent of the first specific legislation in Europe. According to Doneda (2019), the data protection has evolved from a privacy-centric approach to a more comprehensive informational self-determination, recognizing the right of individuals to control your personal information.

In the African context, data protection has gained relevance more recently. The European Union African Union adopted in 2014 the Convention on Cybersecurity and Personal Data Protection, also known as the Malabo Convention, establishing a regional framework for data protection on the continent (African Union, 2014). In Mozambique, the debate on data protection has gained momentum only in the last decade, driven by the growth the use of digital technologies and greater awareness of the risks associated with inappropriate handling of personal information.

International and Regional Legal Framework

The protection of personal data is internationally recognized as a fundamental right. Documents such as the Universal Declaration of Human Rights (1948) and the Covenant International Covenant on Civil and Political Rights (1966) establishes the right to privacy as a fundamental human right.

In the European context, the European Union's General Data Protection Regulation (GDPR), implemented in 2018, it has become a global reference in terms of data protection personal, influencing legislation around the world (Carvalho, 2020).

In the African context, in addition to the Malabo Convention, the African Charter on Human Rights and of the Peoples also offers privacy protection, although it does not explicitly mention the data protection (Makulilo, 2016).

Forms of Illegitimate Access to Data

According to Cert.br (2022), the main forms of illegitimate access to data include:

ÿ Phishing Attacks: Involves the fraudulent obtaining of sensitive information (passwords, credit card numbers) through impersonation, usually via email or fake websites.

ÿ Malware: Malicious software such as viruses, trojans, ransomware and spyware, which are designed to infiltrate systems, extract data, or cause damage.

ÿ Social Engineering Attacks: Psychological manipulation of people to induce them to carry out actions or disclose confidential information.

ÿ Vulnerability Exploitation: Taking advantage of flaws in operating systems, applications or hardware to gain unauthorized access.

ÿ Brute Force Attacks: Repeated attempts to discover passwords or encryption keys through multiple combinations.

Impacts of Illegitimate Access

The impacts of illegitimate data access are multidimensional. According to a study by IBM Security (2023), data breaches have significant financial costs for companies

organizations, including expenses for investigation, notification, technical response, loss of customers and reputational damage.

For individuals, the consequences include identity theft, financial fraud, damage to reputation and violation of privacy. At the national level, illegitimate access to data government or critical infrastructure may pose threats to national security and to social stability (Ponemon Institute, 2022).

Particularities of the Mozambican Context

The Mozambican context presents particularities that influence both the occurrence and combating illegitimate access to data. According to Machava (2021), the rapid growth in the use of digital technologies, combined with low levels of digital literacy and infrastructure poor security creates an environment conducive to data breaches. Mussá (2020), identifies some challenges specific to the Mozambican context:

ÿ Digital Inequality: Unequal access to the internet and digital technologies creates disparities in understanding and being able to protect against digital threats.

ÿ Institutional Limitations: The lack of resources and technical capacity of institutions responsible for enforcing the law and regulating the digital environment.

ÿ Limited Awareness: Low levels of awareness about digital security among the population general population and even among IT professionals.

ÿ Incomplete Legal Framework: Gaps in specific legislation on data protection and cybersecurity.

RESULTS AND DISCUSSION

Illegitimate Access

Illegitimate access is one of the main forms of data breach, characterized by for obtaining, manipulating or using information without due authorization from the holders or legal guardians. This phenomenon assumes particular relevance in the context of digital infrastructures, where the growing digitalization of processes and the massification of

data storage in computerized systems increases the possibilities of occurrence from unauthorized access.

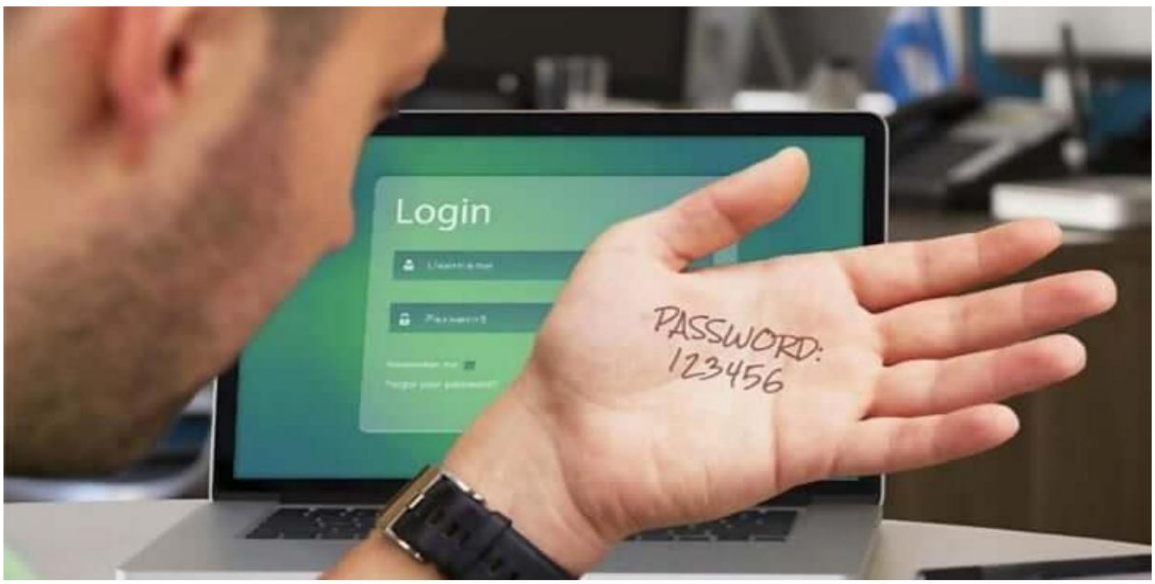
According to article 256 of Law 24/2019, of December 24, which approves the Criminal Code of Mozambique, Illegitimate Access says that whoever, without legal permission or without being able to do so authorized by the owner, by another holder of the rights to the system or part of it, to invade a another device, fixed or mobile, connected or not to the computer network, in order to obtain non-public information from private mail or electronic communications, access to data private, commercial or industrial secrets, confidential information or remote access is not authorized use of the device, is punishable by imprisonment of 1 to 2 years and a fine of up to 1 year.

Causes of Illegitimate Access

Illegitimate access to systems and data can occur for a variety of reasons, and in the context Mozambican, these challenges are particularly relevant. Let's explore each of these causes with specific examples. Lack of adequate security measures. Many institutions in Mozambique have not yet implemented robust data protection protocols. data.

For example, some government entities and private companies do not use encryption. to protect sensitive information, making it vulnerable to attack. In 2022, there were reports of data leaks in some financial institutions due to the lack of security measures effective security.

Use of weak credentials



Easy-to-guess passwords remain a significant problem. In Mozambique, many users (individuals and public legal entities) still use simple passwords such as "123456" or 5 "password", facilitating brute force attacks. In 2023, a study indicated that several utility accounts were compromised due to the reuse of weak passwords.

Social engineering attacks

Hackers exploit human vulnerabilities to gain access to sensitive information. A A common example in Mozambique is scams via WhatsApp, where criminals pretend to be employees of banks or telecommunications companies to deceive users and obtain access credentials. Phishing cases are also frequent, where fake emails request banking information.

Lack of specific legislation and challenges in application

Although Mozambique has laws related to data protection, such as the Penal Code approved in 2019, oversight still faces challenges. The lack of clear regulation on cybercrimes make it harder to punish attackers. In 2024, there were debates about the need for a specific data protection law to strengthen digital security in country.

Consequences of illegitimate access to data breach in Mozambique

The consequences of illegitimate access to personal data include: Violation of Privacy, unauthorized access to personal data compromises the privacy of individuals, exposing sensitive information such as political, religious, philosophical beliefs, ethnic origin or party affiliation. The Penal Code, in article 316, classifies as a crime the creation, maintenance or unlawful use of automated files containing such data, imposing prison sentences over two to eight years and a fine of up to one year.

Financial Losses

Illegitimate access to data can result in financial fraud, such as the misuse of banking or personal information to obtain illicit benefits. Article 319 of the Code Criminal law deals with fraud using computer means, punishing anyone who, with the intention of enriching themselves unlawful, cause financial harm to others by interfering in data processing or unauthorized use of computer programs.

Reputational Damage

Unauthorized disclosure of personal data may harm the public image of individuals or organizations, affecting their credibility and trust in society. Although the Code Criminal law does not specifically address reputational damage, data breach may be considered a form of defamation or slander, subjecting the offender to the penalties provided for such crimes.

Security Practices as a Pillar of Data Protection

In addition to legislation, implementing effective security practices is crucial to protecting personal data. The National Institute of Information and Communication Technologies (INTIC), highlights the importance of measures such as multi-factor authentication, data encryption and conducting regular audits to ensure the integrity and confidentiality of information. The creation of a Digital Certification System based on cryptography public key, as provided for in Article 11 of the Electronic Transactions Act (LTE), is one of the initiatives to ensure the authenticity and legal validity of documents electronics. The continuous training of information technology professionals and the Citizen awareness of the importance of data protection is also essential. INTIC promotes actions for the development of a data governance framework, aiming to guarantee access, protect individual rights and promote development socioeconomic of the country.

Importance of Data Protection in the Digital Age

In the digital age we live in, data protection has transcended mere convenience, becoming a fundamental pillar to ensure privacy, security and trust in electronic interactions that permeate our daily lives. The rapid advancement and omnipresence of

information technologies, social networks, digital financial services and systems government online services have boosted the collection, storage and daily processing of massive amounts of data, both personal and sensitive. This scenario, although it brings I get numerous advantages in terms of efficiency, connectivity and access to information, also carries significant risks. Exposure or inappropriate use of this data can trigger a series of serious damages, with impacts that extend from the sphere individual to the social and institutional fabric.

Types of Data Breaches in Mozambique

In Mozambique, illegitimate access to data is a growing challenge in the digital age, characterized by obtaining, using, modifying or disclosing digital information without the due authorization or legal support, which constitutes a violation of privacy and information security.

This illicit practice encompasses various conducts, such as the invasion of computer systems, the use of other people's credentials and the exploitation of technical flaws to access confidential data. The The Electronic Transactions Law of Mozambique (Law No. 3/2017, of January 9) establishes that unauthorized access to computer systems or databases constitutes an offence, as well as such as the interception, modification or use of digital information without consent (Arts. 46 and 47). In this context, types of data breach include:

Unauthorized access

Unauthorized access consists of the illicit obtaining of data by individuals or entities that do not have permission to do so. According to Tipton and Krause (2014), this type of breach represents one of the most frequent forms of attacks on information security, as allows the attacker to view, copy or manipulate sensitive information without leaving any trace evident.

In Mozambique, the Electronic Transactions Law (which approves Law No. 3/2017, of 9 January), explicitly criminalizes improper access to electronic systems and data, in its Articles 46 and 47. Such acts are common in bank fraud, account hacking, digital platforms and government systems. Example: Hacking bank accounts via apps mobile, access to health or educational records without permission.

Relevance of Data Protection

With the growth in the use of digital services in the public sector (such as e-SISTAFE, e-SNIS, e-SNGRHE, online teaching platforms, among others), data breach has become a risk real for the privacy of citizens and the integrity of institutions. However, the country still faces technical and legal challenges, such as:

• Weak enforcement of existing legislation: Existing laws may not be enforced effectively. consistent or effective, whether due to lack of resources, institutional capacity or awareness on the importance of data protection.

• Low level of digital literacy: The lack of digital knowledge and skills on the part of citizens and even some institutions can make them more vulnerable to attacks cyber threats and data breaches, as well as making it difficult to adopt secure data protection practices of information.

• Absence of a specific national authority for the protection of personal data: Mozambique does not yet have an independent regulatory body specializing in protection of data, which limits the capacity for monitoring, supervision and enforcement of laws, as well as responding to data breach incidents.

CONCLUSION

It should be concluded that illegitimate access to personal data is a worrying reality in Mozambique. bique. Although the country has relevant constitutional and legal frameworks, there are still gaps in the application practical application and monitoring. Effective data protection depends on the creation of a framework more complete regulatory framework, the capacity building of institutions and the collective awareness of society. ity. Investing in data protection is, above all, investing in dignity, freedom and security of Mozambican citizens.

In Mozambique, there is an urgent need to strengthen digital security in the country. Despite the existence of legal instruments, such as the Penal Code and the Electronic Transactions Law, electronics, there are still regulatory and structural gaps that compromise the effectiveness of the prevention prevention and repression of cybercrimes. The increasing digitalization of public institutions

and private, combined with the lack of effective monitoring mechanisms, exposes citizens to risks increasing loss of privacy, financial and reputational damage.

To face this scenario, it is essential to approve specific legislation to protect protection of personal data, aligned with national and international standards, as well as the creation of an independent authority to monitor compliance. Likewise, the strengthening cybersecurity infrastructure, training qualified professionals and promoting digital education among the population are essential measures.

Data protection must be understood not only as a technical issue, but as a fundamental right, directly linked to the dignity, freedom and security of citizens. Mo-Zambia therefore needs to invest in an integrated, preventive and collaborative approach, which unite legal, technological and social efforts to ensure the integrity of information and the con-bail in the digital environment.

REFERENCES

DIÁRIO ECONÓMICO. INTIC points out lack of regulation for data protection 6 Jun. 2024. Available at: https://www.diarioeconomico.co.mz/2024/06/06/econo-mia/bank/intic-points-absence de-regulation-for-protection-of-financial-data, accessed on May 7, 2025.

NATIONAL INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (INTIC). Current legal and regulatory framework guarantees the protection of personal data in Mo-zambique. Available at: https://intic.gov.mz/actual-quadro legal-e-regulamentar-garante-a-personal-data-protection-in-mozambique. , accessed on May 4, 2025.

INTIC. INTIC disseminates personal data protection mechanisms. Available at: https://in-tic.gov.mz/intic-dissemina-mecanismos-de-protecao-de-dados-pessoais, accessed on 06 May 2025.

Sommerville, I. (2011). Software engineering. Pearson Education. Fernanda farinelli, concepts Basics of Object-Oriented Programming, (2007).

Solove, D. J. (2006). The digital person: Technology and privacy in the information age. NYU Press.

Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.

Tavares, José. Digital Law and Data Protection in Africa. Maputo: Academic Press Mozambican, 2022.

Tipton, H. F., & Krause, M. (Eds.). (2014). Information security management handbook (6th ed.). Auerbach Publications.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Withputers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

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.

INTERNATIONAL CHARTER. Mozambique and the African Union Convention on Cybersecurity Security Protection of Personal Data. https://www.cartainternacional.abri.org.br/Carta/article/view/1130, accessed on May 8, 2025.