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

Civil liability of providers and information security in Mozambique

Civil liability of providers and information security in mozambique

Civil responsibility of providers and information security in Mozambique

Raul de Miguel Benjamin Jofrisse Nhamitambo1

SUMMARY

Society faces major challenges in balancing the guarantee of the right to information, which goes beyond the right to freedom of expression, and the protection of privacy and private life in the face of new technological challenges. This leads the doctrine to revisit the assumptions of civil liability of providers and information security. According to the theory of subjective liability due to culpa in omittendo, providers have the duty to: remove the illicit content immediately after notifying the victim and adopt the necessary measures, respecting the limits of their technical capacity, for the purpose of identifying the user responsible for disseminating the offensive material. In the same judgment, it was found that providers are jointly liable with the direct author of the damage in the event that they do not make the content
infringing inaccessible immediately after the interested party becomes aware of its existence.
Keywords: Society, right to information, responsibility.

ABSTRACT

Society faces major challenges in balancing the guarantee of the right to information, which goes beyond the right to freedom of expression, and the protection of privacy and private life in the face of new technological challenges. This leads the doctrine to revisit the assumptions of civil liability of providers and information security. The theory of subjective liability due to culpa in omittendo, providers have the duty to: a) remove the illicit content immediately after notifying the victim; b) adopt the necessary measures, respecting the limits of its technical capacity, for the purpose of identifying the user responsible for disseminating the offensive material. In the same judgment, it was found that providers are jointly liable with the direct perpetrator of the damage if they do not make the infringing content inaccessible immediately after the interested party becomes aware of its existence.
Keywords: Access, visually impaired people, job market.

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

Senior Legal Assistance Technician – Legal Office (UP - Maputo); University Lecturer in Introduction to Law, Administrative Law I and II and, Labour Law, in the Bachelor's Degrees in Law, Accounting and Auditing and, Public and Local Administration – at the Instituto Superior Maria Mãe de África (ISMMA); Assistant Professor at the Instituto Superior de Contabilidade e Audiria de Moçambique (ISCAM), teaching the subject Taxation Complements in the Master's Degree in Auditing; Author, Reviewer, External Evaluator and Peer in the Multidisciplinary Scientific Journal O Saber (since II Semester 2024); Author, Evaluator and Reviewer in the Multidisciplinary Journal RECIMA21 (since Semester 1 of 2025) and in the International Journal Consinter de Direito **(International Council for Contemporary Studies in Postgraduate Studies – CONSINTER), since Semester 2 of 2025** and Organizer of the Digital Scientific Publisher (Since Semester 1 of 2025). Matola – Maputo. ORCID: 0009-0006-4118-1970. rnhamitambo@gmail.com.(+258) 872058783/847417800.

ABSTRACT

Society is facing important challenges to reconcile the guarantee of the right to information, which extends the right to the freedom of expression, with the protection of privacy and private life in the face of new technological challenges. This leads to the doctrine to review the civil responsibility assumptions of providers and information security. According to the theory of subjective responsibility for guilt in omitting, providers have the obligation to remove the illicit content immediately after notifying the victim and adopting the necessary measures, respecting the limits of their technical capacity, to identify the user responsible for disseminating the offensive material. In the same sentence, it was determined that the providers are jointly and severally responsible with the direct author of the damage if the infringing content is not inaccessible immediately after notifying the interested party of its existence.

Keywords: Society, right to information, responsibility.

INTRODUCTION

Information technology has revolutionized the way we live and do business. convergence of technologies for smart environments and integrated ecosystems has left us vulnerable. This has been accompanied by a growing threat that knows no bounds, example title: Cyber threats. Currently, there are a multitude of threats and risks that may harm the proper functioning of cyberspace, including ICT systems and services in Mozambique that may have a negative impact on efforts to harness ICTs for socio-economic development. Given the cross-border feature of ICTs, no sovereign nation or multinational corporation can ensure cyber security alone, requiring a joint approach, both within the country and at the international level. It is in this context that Mozambique has been giving great strides to create an environment in which citizens have increasing access to Information and Communication Technologies (ICT) and associated services with a high sense of security. For this reason, several actions at different levels have been created and implemented by the Government, for example: Electronic Transactions Law, approved by Law No. 3/2017 of 9 January, Mozambique's National Cybersecurity Strategy, Mozambique e-Government and Communication Infrastructure Project (Mozambique Electronic Government and Communications Infrastructure -MEGCIP), Rede Government Electronics (GovNet), State Personnel Information System (SIP), e-SISTAF (State Financial Administration Information System), among others.

The present research aims to address Mozambican legislation in terms of respect for providers and their responsibilities and information security. The provider will be held civilly liable in the event of damage caused in the exercise of their daily activities.

The research is characterized as:

Regarding the purpose: Bibliographic, based on material already prepared and published, such as books, scientific articles and legislation. According to CRESWELL, bibliographic research is based on material already prepared and published, such as books, scientific articles and legislation. This approach allows for critical and in-depth analysis of existing theories and perspectives on the topic, providing a solid foundation for building knowledge.

Therefore, by adopting a bibliographical approach, this study is strengthened by integrating theoretical knowledge consolidated with practical reality, supporting its conclusions and recommendations on scientific and normative bases. In this way, the research proposes reflections and solutions based on specialized literature and official documents.

Regarding nature: Basic or pure, seeking to produce new knowledge on the subject in question. As for nature, this study is classified as basic or pure, seeking the production of new knowledge. As Lakatos and MARCONI (2017) point out, research basic is aimed at generating theories and concepts, contributing to the advancement of understanding of a given topic.

Regarding the approach: Qualitative, seeking to understand the meanings and interpretations of phenomena related to the theme. The qualitative approach adopted in this study.

Data Analysis Techniques and Instruments

To analyze the collected data, content analysis was used, which, according to BARDIN (2011), is a methodology that enables the categorization, interpretation and inference of information contained in textual materials, allowing the identification of patterns and underlying meanings in the speeches and documents analyzed.

RESPONSIBILITY OF PROVIDERS

Provider

According to the “Aurélio” dictionary, provider is a word belonging to both the class of noun as well as adjective, meaning “something or someone that provides or furnishes the necessary: the Government is the provider of your benefits”. Also, provider can be any “individual in charge of certain establishments, charitable institutions or welfare”. Therefore, any entity, company, individual or even a group of people who provide something of any kind (food, products, services, etc.) can understand yourself as a provider, which is why this term is used in several areas. However, it is important to note that in our context, when we speak of this term, we are referring to context of Information and Communication Technologies (ICTs).

Provider classification

According to the Electronic Transactions Act2 , in articles 10 and 13, providers may be classified in two ways: primary and intermediate, each having its own clearly defined responsibilities according to the same law.

Primary Service Provider

“Primary service providers are government or delegated public institutions by the Information and Communication Technologies Regulatory Authority that send, receive or store institutional, collective or individual data”. Ibdi (article 10, number 1) [O]s primary service providers may delegate their competences to third parties, grant concessions their attributions and competences to intermediary service providers provided that:

a) the activity of the delegated entity complies with the law and the rules established by the delegating entity;

b) the delegated entity provides its services in its own name and is liable under the terms of the Law.

2 Electronic Transactions Law, approved by Law No. 3/2017, of January 9.

Regulatory Entity

"The Regulatory Entity is a public institution with legal personality, autonomy administrative and performs its functions in accordance with this Law, its respective organic statute and other applicable legislation". Ibdi (article 11, number 1).

According to Ibdi (article 11, number 2 and 3), the National Institute of Information Technologies and Communication (INTIC) is the Regulatory Entity within the scope of this Law, having its organization and operation regulated by the Organic Statute approved by the Board of Ministers.

Intermediary service provider

According to Ibdi (article 13), the intermediary service provider is the one whose responsibility is the materialization of the competences assigned by the primary provider, this through the granting of a license by the latter. "The licensing for the exercise of the activities of intermediary service provider is the responsibility of the regulatory entity". Ibdi (article 13, number 2)

Responsibilities of the bodies

Regulatory entity

The Regulatory Entity has the following responsibilities, Ibdi (article 12, number 1):

a) ensure respect for and compliance with the law and its regulations;

b) submit proposals for regulations and other legislation implementing this Law, within the limits of the law;

c) perform regulatory, supervisory and inspection functions;

d) ensure the implementation of the e-Government interoperability framework;

e) apply sanctions arising from non-compliance with this Law and other applicable legislation;

f) disseminate and promote the application of electronic transactions, electronic commerce and Electronic Government; g) license intermediary service providers;

h) issue, modify, renew, suspend or cancel the licenses and registrations established in the this Law;

i) ensure the management of the ".mz" domain;

j) ensure the implementation and operation of the electronic certification system of State;

k) protect consumers in the context of electronic transactions, electronic commerce and Electronic Government;

l) create mechanisms to protect the national technology industry and services; information and communication;

m) issue an opinion on the commercial licensing of commercial organizations in the area of information and communication technologies;

n) collect fees and fines;

o) propose to the Council of Ministers the updating of rates.

The regulatory entity may also “exercise other powers defined in the Organic Statute”. Ibdi (article 12, paragraph 2).

Intermediary service provider

According to this Law, the Intermediary Service Provider has its responsibilities divided into six areas: as a service issuer, service receiver, receiver and issuer of services, entity that ensures the storage of information, information monitor, entity that ensures the registration of users' identities.

Intermediary service provider as service issuer

1. The intermediary service provider is responsible for guaranteeing access and ensuring the communication of information transmitted by users linked to it, through a network or communication system.
2. Providing access to and transmitting information issued by users who, include automatic, intermediate and transient storage of transmitted information in a data communication network, until the end of the period defined for its transmission.
3. The intermediary provider must keep all communications from information transmitted by users linked to them, and may not disclose, provide or use to the detriment of users.

4. The intermediary provider may, by means of a court decision or administrative decision, duly substantiated, provide communications of information that have content criminal or that threaten the security of the State. Ibdi (article 14).

Intermediary service provider as service receiver

“The intermediary service provider is responsible for guaranteeing access and ensuring the communication of information received, intended for users linked to it, through a data communication network or system”. Ibdi (article 15).

Intermediary service provider as sender and receiver of services

The intermediary service provider must, Ibdi (article 16):

a) maintain the integrity of the information it receives and transmits in its capacity as provider intermediary;

b) refrain from using or passing on to third parties data or information sent or intended for users linked to it, except by court order;

c) prevent the removal or deactivation of access to stored information;

d) be liable for damages and losses caused to users, within the scope of the duty of confidentiality and protection of their data and information.

Intermediary service provider as an entity that ensures the storage of information

1. The intermediary service provider is responsible for storing information for users or from them to others linked to them, without prejudice to the duty of protection and confidentiality to which it is bound.

2. The provisions of the previous number do not apply to cases in which the service recipient acts under legal order of the competent authority of the provider.

3. The provisions of this article shall not affect the decisions of a court or administrative authority. competent. Ibdi (article 17):

Intermediary service provider as information monitor

1. The intermediary service provider is not subject to the general obligation to monitor the information that it transmits or stores, nor to seek facts or circumstances indicative of illegal activity.

2. Without prejudice to the provisions of paragraph 1, the intermediary service provider must collaborate, in the sense of:

a) inform the competent public authorities of any illegal activities detected;

b) submit to the competent authorities, at their request, information enabling the identification of service recipients who have storage contracts;

c) obtain and maintain data that allows the identification of service providers that contributed to the creation of content integrated into services provided by them to third parties;

d) identify users who transmit or store data with offensive content, using the communication service with an unidentified sender;

e) act immediately, without any other formalities, upon a complaint, claim or information of theft, robbery, loss or disappearance of electronic means made by the user with the aim of recovering or preventing its unlawful use.

3. For the purposes of the provisions of paragraph e) of the previous number, the user is obliged to inform the intermediary service provider regarding theft, robbery, loss or disappearance of means electronic devices in their possession and use. Ibdi (article 18).

Intermediary service provider as an entity that ensures the registration of identity of users

In relation to this point, “intermediary providers must register and identify their users, under the terms to be regulated”. Ibdi (article 19) Service providers, if the wish, can still provide certification services, as long as they are duly accredited and fulfill their responsibilities as agents of certification.

Accreditation of certification service providers

For accreditation of certification service providers, the following must be complied with:

presuppositions, Ibdi (article 59):

1. Any certification service provider intending to issue qualified certificates is subject to accreditation issued by the competent services.

2. Accreditation may be conferred on a certification service provider, which, cumulatively, meet the following requirements:

a) demonstrate the security necessary to provide certification services;

b) ensure the operation of a fast, secure directory and immediate revocation services;

c) ensure that the date and time at which a certificate is issued or revoked can be determined accurately;

d) verify by appropriate means in accordance with relevant legislation, the identity, and, if applicable, any special attributes of the person in whose favor the document is issued qualified certificate;

e) hire personnel who have the knowledge, experience and qualifications necessary for the services provided;

f) use reliable systems and products that are protected against modifications and that guarantee technical security of process coding;

g) take measures against certificate forgery in cases where the service provider certification generates signature creation data, ensuring confidentiality during the process of generating said data;

h) has sufficient financial resources to operate in accordance with the requirements established in this Law, in particular with regard to the assumption of liability for damages;

(i) electronically record all relevant information relating to a qualified certificate for an appropriate period of time, with the aim of providing evidence of certification for effects of legal proceedings;

j) not to store or copy subscription creation data of the person to whom the provider certification services provides key management services;

k) before entering into a contractual relationship inform the person of the terms and conditions concerning the use of the certificate including limitations on its use;

l) use reliable systems to store certificates in a verifiable manner, so that

to which:

i) only authorized persons may access to make entries and changes;

ii) the information can be verified for authenticity;

iii) certificates are publicly available for access only in cases where the consent of the certificate holder has been obtained;

iv) any technical changes that compromise safety requirements are apparent to the operator.

INFORMATION SECURITY

Information

"Data that has been transformed, manipulated and organized and that has value to support the decision making", for example: The student is exempted because he achieved an average of 14 points. Fedeli, et.al. (2010), cited by SABBEN3 . In modern business management, information is treated as an important asset4 of the company. This information can be printed, handwritten, recorded on magnetic media, or simply being known to employees (spoken). Information can be classified according to the following criteria: confidentiality, integrity, availability, or it may have a standard classification.

Information characteristics

Quality information must basically have the following characteristics, known as: acronym (ACID): Timely: must be provided at the right time and in a timely manner; Confidential: must not be accessed by unauthorized persons; Integrity: must not be altered, deleted without authorization, etc.; And available: it must be accessible whenever it is needed. Therefore,

3SEBBEN, A., et al. Introduction to computing: an approach with libreoffice. Federal University of the Southern Border. Chapaco-UEFS, 2012.

4 An asset is any element that has value for a given organization, for example: its image, its facilities, its personnel, its capital, its data, etc.

for quality information, organizations and other entities must create the necessary conditions for the fulfillment of the characteristics described above, a fact that makes the information management process quite useful.

Information Security Information Security, or Information Systems Security "is the protection of information against various types of threats to ensure the continuity of business, minimize risks, maximize return on investment and opportunities business" [ISO 27002].

"It is the area of knowledge dedicated to the protection of information assets against unauthorized access. authorized, undue changes or their unavailability" Idem.

Basic principles of information security

Confidentiality: Certainty that what was said, written or spoken will be accessed only by authorized persons;

Integrity: Guarantee that the information has not been altered (improperly or otherwise) authorized); Availability: Guarantee that the information will be accessed when necessary; organizations, so that they are guaranteed the provision of quality services, their maintenance, etc., must define solid information security policies. This practice will minimize the number of vulnerabilities5 that their assets are subject to, and above all, minimize the impact in the event of certain threats6 that properly exploit these vulnerabilities.

Cybersecurity

Cybersecurity (also called Cyber Security), refers to the practices employed to ensure the integrity, confidentiality and availability of information. It is composed by a set of tools, risk management approaches, technologies, training and methods to protect networks, devices, programs and data against attacks or unauthorized access authorized. Cybersecurity is the set of technologies, processes and practices designed to protect networks, computers and other electronic devices, programs and data, from potential attacks or threats. In practice, ensuring cyber security in a

5 It is a weakness within the organization's assets that can be exploited by a threat.
6 It is an event, or an external force that can exploit a vulnerability and potentially break the basic principles of Information Security, a fact that can put the health of the organization at risk.

company/organization, for example, requires the coordination of efforts across the entire system information, which includes: Application security; Information security; Network security; Disaster recovery/business continuity planning; Operational security; End user education.

Most common threats in cyberspace

The most common threats in cyberspace are: viruses, phishing, keylogger, spyware, ransomware, botnet, clickjacking, denial of service, SQL Injection, etc.

How to prevent cybersecurity attacks

With so many threats out there, it's essential to learn how to protect yourself from security breaches. cybersecurity. To protect yourself from such risks, it is important to have a solid security foundation cybersecurity that mitigates the risk of an attack. In addition, there are some tips that should be useful for everyone who uses the network and all types of Internet devices: Install and update regularly antivirus software for all computers used in business, at home or in other locations. Do a little research and find the best protection provider in internet and don't buy the cheapest software: Secure your internet connection using a firewall; Make backup copies of important data and keep it safe; Train employees or family members in cybersecurity and its principles; Regularly change passwords and use strong passwords. A strong password contains lowercase letters, uppercase letters, special characters, and numbers. It is recommended not to make it a word, just a random combination. Regularly update software and operating systems and; Protect the network.

Therefore, in addition to these responsibilities on the part of companies to guarantee a secure cyberspace, countries around the world have also been implementing several strategies to make this precious and ideal asset a reality, as is the case in Mozambique. It is for these reasons that our country ended up moving forward with a proposal known as “Mozambique National Cyber Security Strategy”, which advocates several strategies to provide our country, organizations and the general public with a cyberspace healthy and safe.

Mozambique's National Cybersecurity Strategy

Guiding principles According to this proposal, the principles that support this strategy are, (ENSC:12): i. Legality: The ENSC of Mozambique takes into account the various laws in force in Mozambique and will promote the protection of the rights, freedoms and fundamental guarantees of Mozambicans. ii. Risk-based approach: ENSC adopts a risk-based approach risk in assessing responses to cyber threats and risks, ensuring Security Cybernetics in Mozambique. iii. Cooperation and Coordination: This Strategy promotes the coordination and cooperation between the various stakeholders, both at national and international. iv. Shared responsibility and cybercrime: ENSC recognizes the individual and shared responsibility of all ICT users (individuals, sector private and Government). v. Universal access to cyberspace: ENSC will seek to ensure that all Mozambican citizens should have access to and be able to use cyberspace safely, regardless of location, gender, race, economic status, among others. others.

Strategic Objectives

According to the proposal referenced above, in order to achieve the vision7 and mission8 of ENSC, defined 5 (five) strategic objectives: I. Improve the protection of critical infrastructure information (ICI). II. Strengthen the legal, technical and operational framework for cybersecurity. III. Establish a national framework to promote information sharing, cooperation and Coordination in cybersecurity matters. IV. Develop technical capacity to research and innovation in cybersecurity. V. Create a national culture of cybersecurity. To achieve these objectives, a series of actions must be carried out. It is important to highlight that these actions are categorized according to each one of the strategic objectives presented above.

Implementation mechanisms

According to this proposal, there is no organizational structure in Mozambique suitable for the coordination of cybersecurity policies and interventions at the national level

7A nation with a secure, resilient cyberspace and an aware society.
8 Develop the necessary capacity and cybersecurity environment that ensures a safe cyberspace.

operational and strategic. Considering that ensuring cyber security is material transversal and covering different sectors of society, there is therefore a need for development of an integrated and coordinated approach to security-related matters cybernetics. In response to this need, this strategy requires the establishment of a National Cybersecurity Council (CNSC) at a strategic level.

National Cyber Security Council (CNSC)

Its members

This advice, given the sensitivity of the area in which it operates, ends up justifying the fact that it is composed of very complex elements, which we will now present, (ENSC: 21): Minister who oversees the Defense area; Minister who oversees the area of order, security and public tranquility; Minister who oversees the area of Justice; Minister who oversees the area of communications; Minister who oversees the area of information technologies and communication.

Your role

Analyze and guide the State on issues and/or other pertinent matters that contribute for cybersecurity; Develop strategies for creating frameworks and policies appropriate national and regional cybercrime organizational structures. Ensure the creation of institutional capacity with a view to guaranteeing National Defense against attacks and cyber crimes; Idem.

In addition to CNSC, to ensure better implementation of ENSC, other elements are necessary, such as the following: a coordination and implementation unit of ENSC, funding and resources, and monitoring and evaluation. Therefore, all these elements, when well associated, can bring good results in the implementation of ENSC.

Civil liability of providers and information security

All service providers, when carrying out their activities, must always seek ensure its own safety, as well as the safety of its users, since the type of services they provide are very sensitive as they are subject to various attacks,

fact that can compromise information security, negatively influencing life and health of the organization as well as its users. Therefore, under the Transactions Act electronics, approved by Law No. 3/2017, of January 9.

Service providers have the following responsibilities: ensuring the confidentiality, integrity and availability of information; which constitute the pillars basics of information security.

There are several types of internet providers, and there are also distinctions in what concerns the civil liability of the various internet providers: backbone provider, access provider, hosting provider, content provider, search engine provider or search and email provider.

The civil liability of providers in the processing of sensitive data emerges as a vital research area. This research is justified by the imperative need to protect personal information of users, ensuring that providers operate within a framework legal that promotes data security and individual privacy.

The Mozambican legislator deals, in the Civil Code, with the two types of liability civil in different places: while contractual liability appears in arts. 798 and seq., that is, it is found in the chapter that regulates, alongside compliance, the forms and effects non-compliance with obligations; extra-contractual liability is regulated in arts. 483 et seq., in the chapter on sources of obligations, section “civil liability”. Note that as regards the regime of the obligation to compensate, the legislator dealt with the aforementioned modalities jointly – arts. 562 et seq. –, establishing a regime specific to the aforementioned obligation, which is likely to emerge from both modalities. This is a place of confluence of the consequences arising from the two types of liability, as if unifying your regime10. In this sense, we have different regimes with the same consequence – the obligation to compensate. Therefore, contractual civil liability and civil liability non-contractual liability are not watertight compartments, sometimes even functioning as true communicating vessels9 . And, in this regard, there will be cases in which the same legal fact will trigger both types of civil liability10.

9 See VARELA, João Antunes, Obligations in General, Volume I, pp. 521 and 522.

10 Imagine, for example, that a pharmacist, distracted, delivers the wrong medicine to a customer: we have a case of extra-contractual liability, for violation of the right to physical integrity; and, simultaneously, a case of contractual liability, for violation of the purchase and sale contract. Other cases in which this may occur are medical liability in private hospitals.

CONCLUSION

Conclude that, with the growth of ICTs and the Internet, the Mozambican Government had the need to analyze and approve the creation of several bodies to provide Mozambican citizens with more services based on ICTs and the Internet. This is the case of communication service providers, and data storage on computer networks.

This body has its origin in light of the approval of the Electronic Transactions Law, approved by Law No. 3/2017, of January 9, which in addition to presenting the providers and their responsibilities, describes several other aspects related to various types of transactions electronics.

With a view to guaranteeing security in this type of transaction, as well as information security and the domain of ICTs in general, a proposal for a national cybersecurity strategy of Mozambique has been put forward. This proposal presents the strategies needed for the implementation thereof, as well as the implementation mechanisms, all with the purpose to ensure information security and a safe cyberspace.

Therefore, Information Security is a process that involves all business areas. an organization and should be understood as another discipline aimed at achieving the mission established. Information Security is achieved through the implementation of a set of of controls appropriate to the needs of the organization. Controls need to be established, implemented, monitored, analyzed and improved to ensure that the objectives of the business and security needs are met.

In the Provider's Civil Liability, the provider is held civilly liable for damages caused by third parties and is a subsidiary. Which must take steps to make it unavailable the infringing content, after a court order. The same is not responsible for the content generated by users, unless you neglect to remove illegal or offensive content.

REFERENCES

GAGLIANO, Pablo Stolze. Manual of civil law. single volume. São Paulo: Saraiva, 2017.

JORGE, Fernando Pessoa. Essay on the assumptions of civil liability. Lisbon: ALMEDINA, 1968.

LEONARDI, Marcel. Civil liability of internet service providers. São Paulo: Juarez de Oliveira, 2005.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Constitutional Law Course. 6th ed.

PADRÃO, Vinicius Jóras. The Constitutionality of Article 19 of the Civil Rights Framework for the Internet: a summary of the debate and a look to the future.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (org). Patrimonial Relations: Contracts, Ownership and Civil Liability. Forum: Rio de Janeiro, 2021. THINKING ABOUT THE LAW. Freedom Business Models. http://pensando.mj.gov.br/marcocivil/pauta/liberdade-de-modelos-de-negocios/. Accessed on: 01/16/2022. 63 Available in:

PINHEIRO, Patricia Peck. Digital Law. 5th ed. rev., updated and expanded in accordance with Laws No. 12,735 and 12,737, of 2012. São Paulo: Saraiva, 2013.

ROBERTO, Don Karl. Recent Developments in Canada's "Notice and Notice" Regime. Available at: https://ojs.lib.uwo.ca/index.php/uwojls/announcement/view/123. Accessed on: 02/04/2022.

RODOTÁ, Stefano. Life in the surveillance society. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. Constitutional Law Course. 6th ed. São Paulo: Saraiva, 2017.

SOPRANA, Paula. Supreme Court postpones judgment on removal of content from the internet until 2020. Available https://www1.folha.uol.com.br/tec/2019/12/supremo-adia-para-2020-judgment-on-removal-of-content-from-the-internet.shtml?fbclid=IwAR3m6R9VC4LLMX9Rix9GX-3Vlun4uP_-PYIINCW6gwgywPamt7mJy7I1xaA. Accessed on: 02/09/2022.

SOUZA, Carlos Affonso Pereira de. The five phases of protection of freedom of expression in the Civil Rights Framework for the Internet. Available at: http://site.fdv.br/wp-content/uploads/2019/08/Artigo-Cinco-Faces-da-Liberdade-de-Express%C3%A3o-no-Marco-Civil-da-Internet-Carlos-Affonso.pdf. Accessed on: 02/05/2022.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. Civil Rights Framework for the Internet: construction and application. Juiz de Fora: Edit Associated Publisher, 2016.

TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Civil liability of network providers: analysis of the application of the Internet Civil Rights Framework by the Superior Court of Justice.
IBERC Journal, Minas Gerais, v. 1, n. 1, p. 01-28, Nov./Feb. 2019.

National Legislation

BULLETIN OF THE REPUBLIC, Electronic Transactions Law, approved by Law No. 3/2017, of January 9. Official Publication of the Republic of Mozambique: Maputo.

Proposal for Mozambique's National Cyber Security Strategy.