MOZAMBIQUE
NMP Advogados – PLMJ Colab Mozambique

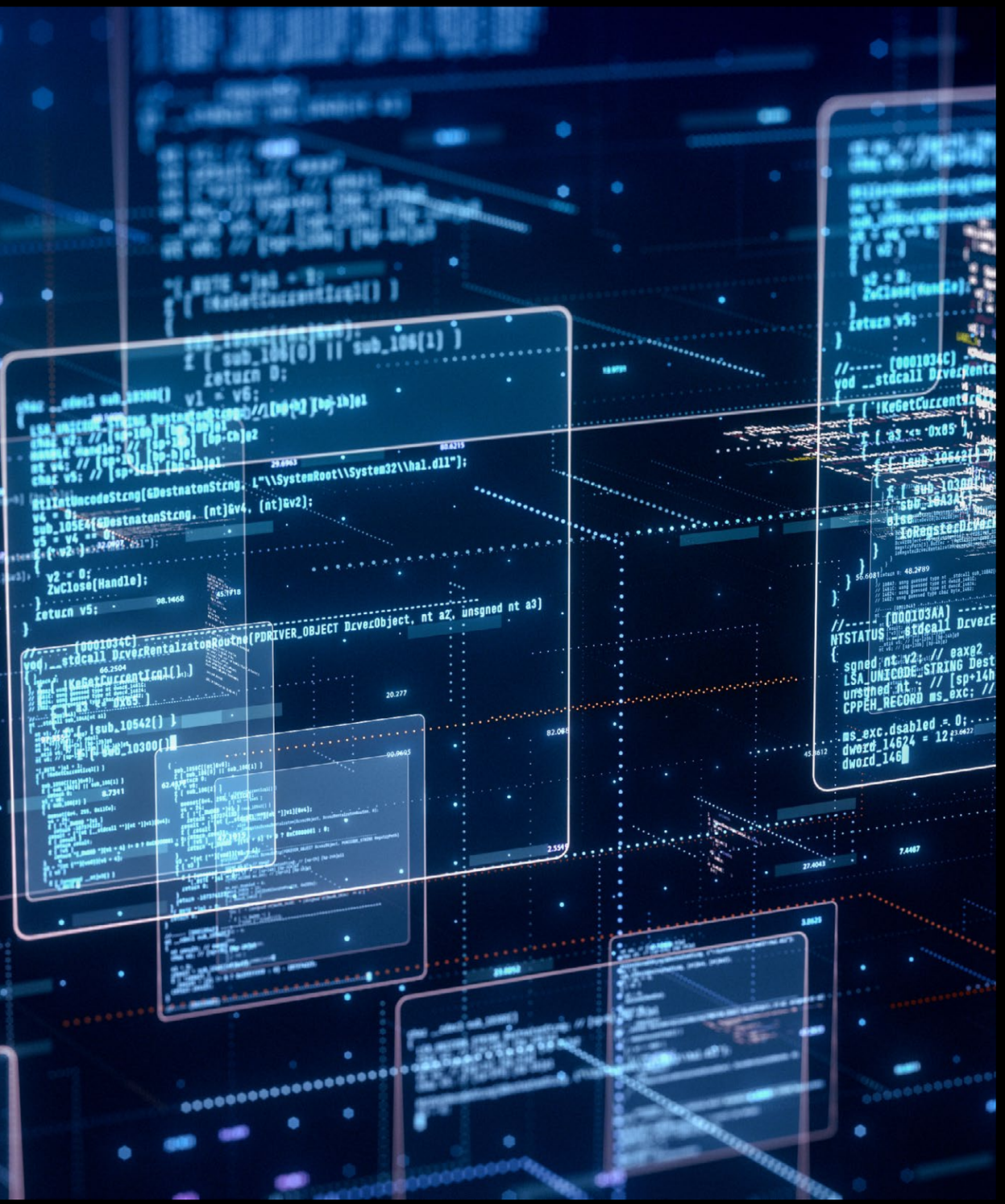
PORTUGAL
PLMJ Advogados

COLAB

New legal framework for cybersecurity and cybercrime

Transformative Legal Experts

PLMJ



Contents

Laws 13 and 14 of 1 July 2026, enacting the Cybersecurity Law and the Cybercrime Law respectively, were published in the Official Gazette, Series I, No. 123, on 1 July 2026. The latter repeals certain provisions of the Criminal Code and the Telecommunications Law.

> These two laws introduce a specific framework of penalties for cybercrime into Mozambican law.

These two laws have a significant cross-cutting impact because they apply to a large proportion of economic operators that rely on networks and information systems. For the first time, they introduce a specific framework of penalties for cybercrime into Mozambican law.

This informative note analyses the main aspects of each piece of legislation, focusing particularly on the practical implications for organisations.

The Cybersecurity Law

Law 13/2026 of 1 July

The Cybersecurity Law provides the framework for the new legislation. Its central objective is to protect the state, its institutions and its citizens in cyberspace by safeguarding data communication networks, information systems and critical infrastructure.

Its scope extends beyond operators of traditionally sensitive infrastructure to include the following sectors:

i) The Public Administration

ii) the private sector

iii) operators of critical infrastructure networks

iv) intermediary service providers

v) digital service providers

vi) operators of essential service networks

vii) cybersecurity service providers

viii) digital platform providers

ix) electronic communications operators

x) any natural persons and entities using data communication networks and information systems (on a residual basis)

However, this scope does not include public administration bodies involved in activities relating to networks, information systems, or critical infrastructure for the purposes of national defence, internal security, or state security. It also does not include bodies that handle classified information in accordance with applicable legislation. Where an entity falls into more than one of the defined categories, the most stringent security rules for networks and information systems will apply.

The law is governed by a broad set of principles, including collaboration and cooperation, protection of human rights, transparency, disclosure of vulnerabilities, integrity, legality, proportionality, necessity and privacy.

ORGANISATION OF THE NATIONAL CYBERSECURITY SYSTEM

The law establishes an institutional framework for cybersecurity governance, comprising bodies responsible for political and technical coordination, as well as a wide range of operational entities.

The National Cybersecurity System comprises these bodies and entities, which are organised within a hierarchical structure.

In terms of these bodies, there are three key pillars:

i) The **National Cybersecurity Council (CNSC)**, chaired by the Prime Minister, is the multi-sector coordination and governance body with powers to undertake political and strategic coordination, monitor the National Cybersecurity Strategy, and issue opinions.

ii) The **National Cybersecurity Authority**, whose functions are carried out by the Regulatory Authority for Information and Communication Technologies, is responsible for regulation, supervision, inspection, licensing, accreditation of professionals, and setting standards and norms in the field of cybersecurity.

iii) The **National Cybersecurity Incident Response Team (nCSIRT.MZ)**, operating within the Information and Communications Technology Regulatory Authority, is the operational coordination body for incident prevention and response.

In the event of a state of siege or emergency, the National Cybersecurity Authority's functions will be carried out by the Cyber Coordination Centre of the Defence and Security Forces.

The system comprises the following entities: the National Network of CSIRTs, Critical Infrastructure Operators, Intermediary Electronic Service Providers, Essential Service Operators, Digital Service Providers, Digital Platform Operators, Data Centre Operators, Cloud Computing Platform Operators, Cybersecurity Service Providers and Digital Communications Operators.

OBLIGATIONS OF THE ORGANISATIONS

The law imposes specific obligations on each category of organisation. In general, all entities covered by the law must:

i) Register with the National Cybersecurity Authority.

ii) Implement measures to govern, identify and protect against cyber risk, and to detect, respond to and recover from attacks.

iii) Maintain the confidentiality of their users' communications.

iv) Cooperate with the competent authorities.

Public Administrations, Private Sector Organisations, Critical Infrastructure Operators, Essential Service Operators, Digital Service Providers, Digital Platform Operators, Data Centre Operators, Cloud Computing Platform Operators and Digital Communications Operators are required to establish an institutional CSIRT.

NETWORK SECURITY, INFORMATION SYSTEMS AND SECURITY REQUIREMENTS

The law imposes a duty on entities covered by it to ensure the integrity, confidentiality and privacy of communications regarding network security. This duty is accompanied by an obligation to retain traffic data for a minimum period of one year, which may be extended by a court order.

In this context, intermediary and digital service providers that store traffic and location data must grant the competent authorities access to such data whenever requested to do so by them and in accordance with the law.

The National Cybersecurity Authority is responsible for establishing and updating cybersecurity requirements to enable the adoption of internationally recognised standards and rules.

The minimum security requirements include the following:

i) An information security policy.

ii) A cyber risk management methodology.

iii) Incident reporting procedures.

iv) Internal audit mechanisms.

v) The appointment of an information security officer.

vi) The establishment of a team specialising in incident detection and response.

In addition, public and private sector organisations must appoint a cybersecurity officer and an internal cybersecurity auditor. They must also draw up an Institutional Information Security Policy.

INCIDENT REPORTING AND RESPONSIBLE DISCLOSURE OF VULNERABILITIES

Organisations must report **incidents with significant impact** to the CSIRT for their sector and the National CSIRT within the timeframe set by the National Cybersecurity Authority. The law expressly stipulates that reporting does not incur additional liability for the reporting party. 'Significant impact' is determined by parameters such as the **number of users affected**, the **duration of the incident**, and the **geographical distribution of the affected area**.

Any individual or legal entity may report, publish or disclose vulnerabilities provided the disclosure is made in good faith.

The law also permits the voluntary reporting of incidents, which must not result in additional obligations being imposed on the organisation reporting the incident.

Regarding the disclosure of vulnerabilities, the law establishes a framework for their responsible disclosure. Under this framework, any individual or legal entity may report, publish or disclose vulnerabilities provided the disclosure is made in good faith. Disclosure is deemed to be in good faith if it has not been made under duress; if a reasonable period of at least 90 days has been allowed for the vulnerability to be rectified; and if precautions have been taken to prevent harm. Methods of identification involving denial-of-service attacks, physical evidence, malicious code, social engineering or the alteration, removal or destruction of data are excluded from the good faith regime.

CYBERSECURITY FUND

The law establishes the Cybersecurity Fund (CSF), which is managed by the National Cybersecurity Authority. The aim of the CSF is to secure financial resources to promote and strengthen cybersecurity. Entities that are registered and licensed to provide cybersecurity services must contribute 1% of their previous year's gross revenue to the CSF.

> The law establishes the Cybersecurity Fund, aiming to secure financial resources to promote and strengthen cybersecurity.

PENALTIES

The law sets out an extensive list of administrative offences, including:

i) Failure to report incidents.

ii) Obstruction of investigations or audits.

iii) Failure to comply with security requirements.

iv) Refusal to comply with the Authority's directives.

v) Carrying out activities without a licence.

Penalties are calculated as multiples of the minimum wage in the civil service, varying according to the seriousness of the offence. For example: (i) failure to comply with security requirements is punishable by a fine of between 90 and 160 times the minimum wage; (ii) failure to comply with the obligation to report incidents is punishable by a fine of between 80 and 100 times the minimum wage; and (iii) carrying out activities without a licence is punishable by a fine of 64 times the minimum wage.

REGULATIONS AND ENTRY INTO FORCE

Within 180 days of its publication, the Council of Ministers must draw up regulations for the law.

The law will come into force 90 days after publication, that is, on 29 September 2026.

RETURN HOME

The Cybercrime Law

Law 14/2026 of 1 July

PURPOSE AND SCOPE OF APPLICATION

The Cybercrime Law sets out substantive and procedural criminal provisions. It also sets out provisions relating to international cooperation in criminal matters in the field of cybercrime, as well as the collection of electronic evidence. The law applies to all individuals and legal entities, whether public or private, who use data communication networks and information systems.

Chapter II of the law sets out fourteen criminal offences. The penalties for these offences increase progressively according to their seriousness.

CRIMINAL OFFENCES

Chapter II of the law sets out fourteen criminal offences. The penalties for these offences increase progressively according to the seriousness of the conduct and the affected legal interest. The most serious offences, such as cyber espionage, are punishable by up to 10 years' imprisonment. The most significant offences can be grouped into four broad categories:

i) Offences against the confidentiality, integrity and availability of data and systems;

ii) Offences relating to property and documents;

iii) Offences against state security and critical infrastructure; and

iv) Other offences of particular social gravity.

The first group comprises offences that are typical of cybercrime and are aimed at protecting systems and data.

Unauthorised access (Article 4) is punishable by a prison sentence of 1 to 2 years and a fine of up to 1 year for anyone who gains access to another person's device without legal permission or authorisation with the aim of obtaining non-public information, accessing private data or commercial or industrial secrets, or gaining unauthorised remote access. The same penalty applies to anyone who produces, sells, distributes or disseminates devices or programmes designed to carry out such acts. Criminal proceedings do not require a complaint to be made, except in cases involving data relating to private life.

Similarly, the **unlawful interception of computer data transmissions (Article 5)** is punishable by up to three years' imprisonment and a fine of up to two years.

Data interference (Article 6), which involves the unlawful alteration, damage, rendering unusable, deletion or destruction of computer data, is punishable by a prison sentence of between 1 and 2 years and a corresponding fine. This penalty is increased to 3 years' imprisonment if the conduct intentionally damages critical infrastructure or disrupts critical services.

Anyone who **obstructs, prevents, interrupts or seriously disrupts the operation of a computer system (Article 7)** is punishable by a prison sentence of up to 2 years and a fine of up to 1 year. The offences in Articles 6 and 7 share a common aggravating factor. Both provide for more severe penalties where the conduct affects critical infrastructure or services. Interference with systems is punishable by a prison sentence of between 2 and 8 years where it results in substantial damage, disruption to essential services, or significant harm to third parties.

Also, within the first group, **the misuse of devices constitutes a separate offence under Article 8**. This offence covers the production, sale, distribution, import or dissemination of devices, computer programmes or data intended for unlawful access or interception offences. The punishment is imprisonment for a term of between 1 and 2 years.

In the second group, relating to property and documents, **computer forgery** (Article 9) criminalises the unlawful entry, modification, deletion or suppression of computer data with the intention of creating false documents. This offence carries a prison sentence of between 1 and 5 years and a fine of up to 1 year. The penalty increases to 2 to 8 years' imprisonment for the import, distribution or possession of devices enabling unlawful access to communication systems for commercial purposes.

The same article also applies to the manipulation, forgery or misuse of another person's identity. Similarly, **computer and communications fraud** (Article 10) punishes the unlawful interference with data processing with the intention of unlawful enrichment that causes financial loss to another person with a prison sentence of up to 3 years and a corresponding fine.

The third group comprises offences that pose the greatest threat to national security and critical infrastructure, as reflected in the significantly harsher penalties imposed.

Cyber espionage (Article 11) carries a prison sentence of 3 to 10 years for unlawfully accessing government computer systems with the intention of obtaining classified or strategic information for foreign intelligence purposes. The same penalty applies to those who hack into corporate networks to steal trade secrets.

Similarly, **cyber-terrorism and violent cyber-extremism** (Article 12) carry prison sentences of between 2 and 8 years for attacks on, intrusions into, destruction of, or tampering with data or critical infrastructure systems. This offence also applies to the mobilisation, recruitment or dissemination of content via computer systems for political, economic or religious motives with the intention of causing panic, fear or terror.

Finally, two offences of particular social gravity are worth highlighting.

Cyber-extortion (Article 13) carries a prison sentence of up to 2 years and a corresponding fine for threatening to disclose compromising information, attacking computer systems, or exfiltrating personal data in exchange for payment. The sentence increases to up to 3 years if the victim is the head of a sovereign body, a government official, or head of a public body.

The law punishes the offence of **child sexual content in the digital environment** (Article 15) with a prison sentence of between 6 months and 1 year, as well as a fine of up to 1 year. This offence covers the production, offering, exchange, making available, transmission or publication of sexual or pornographic content involving minors via a computer system.

An **attempt to commit these offences is also punishable** under the general provisions of the Criminal Code. Legal entities and equivalent bodies are criminally liable for the offences set out in the law, in accordance with the liability rules set out in the Criminal Code.

An attempt to commit these offences is also punishable. Legal entities and equivalent bodies are criminally liable for the offences set out in the law.

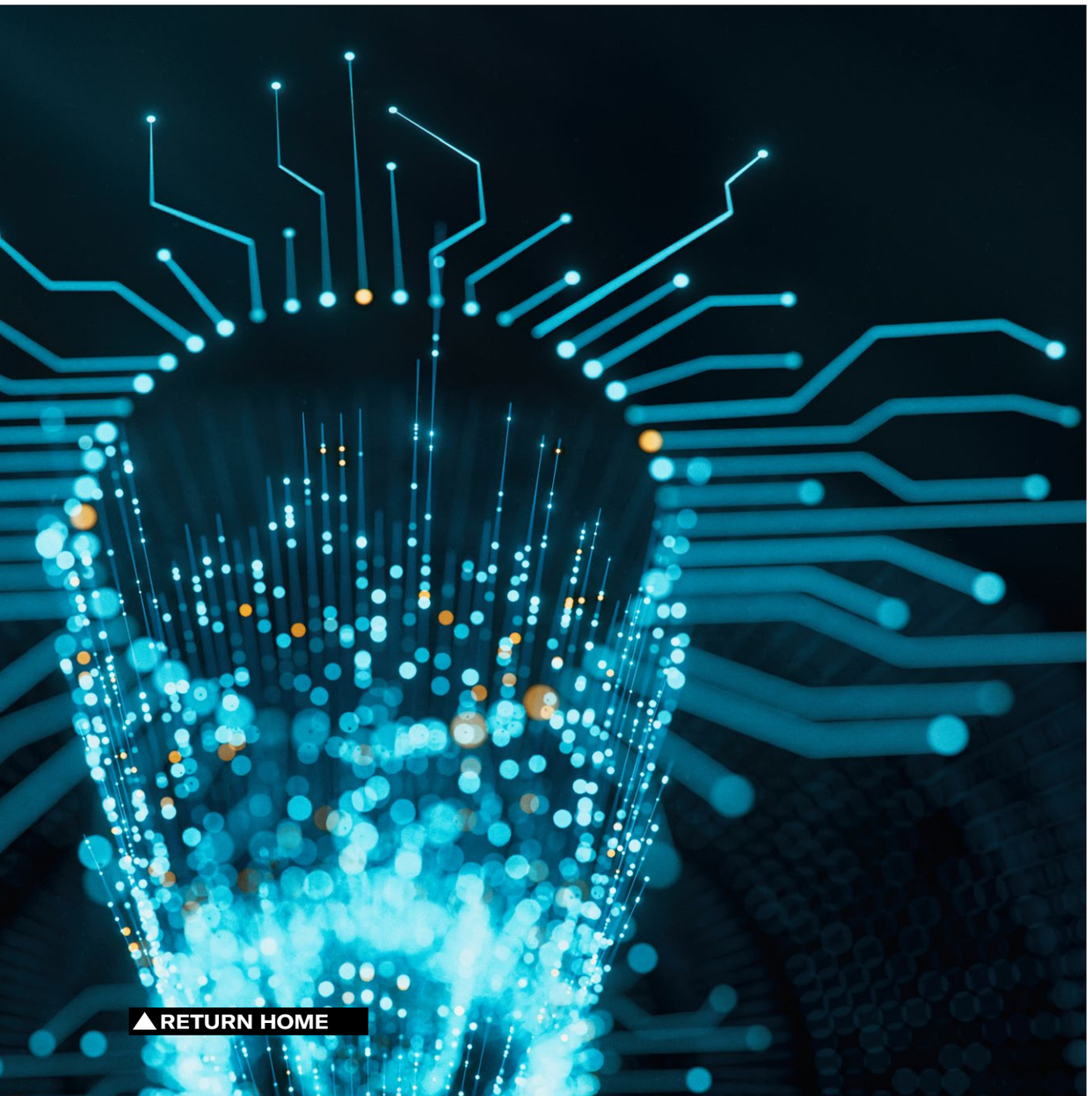
PROCEDURAL PROVISIONS

These provisions apply to the investigation of offences set out in the law, offences committed via a computer system and offences involving the collection of digital evidence.

The first set of mechanisms aims to prevent the loss of digital evidence before it is formally secured by the authorities.

Through the **expedited preservation of data** (Article 18), the competent judicial authority can order any person with access to or control over computer data, particularly the service provider, to preserve and protect the data in question for up to 3 months, extendable to a maximum of 1 year. This order may also be issued by the criminal investigation body, provided that it has prior authorisation from the judicial authority. In urgent cases, the judicial authority must be notified subsequently.

Additionally, the **data production order** (Article 20) empowers the judicial authority to demand the production of specific computer data, including that relating to the customers and subscribers of service providers. This order can also be directed at foreign providers under international treaties. Non-compliance is punishable by law. However, this order cannot be used against suspects or defendants, nor in relation to computer systems used for legal, medical or banking activities.



▲RETURN HOME

A second set of instruments relates to the physical seizure of evidence that has already been located.

Searching computer data (Article 21) generally requires an order from the competent judicial authority, which is valid for up to 30 days. However, the criminal investigation body may act without prior authorisation if there is voluntary consent, or in cases of terrorism or violent or highly organised crime. There must also be reasonable grounds to believe that a crime is about to be committed which poses a serious risk to the life or physical integrity of individuals.

Once the data has been located, the judicial authority may authorise its **seizure** (Article 22), which can take various forms. These range from seizing the physical medium to simply copying or technologically preserving the data, or even deleting it or blocking access to it. Seizures carried out by the criminal investigation body must be validated by a judicial authority within 72 hours at the most.

Finally, the law refers to two exceptional investigative measures that are already used in ordinary criminal proceedings and adapts them for use in cybercrime investigations.

The **interception of communications** (Article 23) is permitted in proceedings relating to offences set out in the law. It may be used either to record content or to collect traffic data.

Conversely, **covert operations** (Article 24) are only permissible in the investigation of offences punishable by a prison sentence of two years or more.

INTERNATIONAL COOPERATION

The law establishes a framework for international cooperation. This includes: (i) spontaneous exchange of information between national and foreign authorities; (ii) a permanent point of contact for cooperation, provided by the Public Prosecutor's Office and available 24 hours a day; and (iii) prompt preservation and disclosure of computer data in the context of international cooperation.

Cooperation may be refused where the data relates to a political offence, undermines the sovereignty or constitutional interests of Mozambique, or where the requesting state does not offer adequate safeguards for the protection of personal data.

Without the need for a prior request, foreign authorities may access computer data stored in Mozambique that is publicly available or receive data subject to the voluntary consent of a legally authorised person.

REPEALED PROVISIONS

Law 14/2026 repeals Articles 256, 289, 336, 337, 338 and 339 of the Criminal Code, as adopted by Law 24/2019 of 24 December and amended by Law 17/2020 of 23 December.

Articles 57 and 66(2) of Law 4/2016 of 3 July (the Telecommunications Law) are also repealed.

ENTRY INTO FORCE AND SUBSIDIARY PROVISIONS

The provisions of the Criminal Code, the Code of Criminal Procedure and Law 21/2019 of 11 November (the Law on International Legal and Judicial Co-operation in Criminal Matters) will apply, respectively, to offences, procedural measures and international co-operation, in all matters not contrary to the provisions of this law.

The Council of Ministers is responsible for issuing regulations to implement the law within 180 days. The law will come into force 90 days after publication, that is, on 29 September 2026.

Comments

These two pieces of legislation mark a significant milestone in Mozambique's legal framework concerning cybersecurity and cybercrime. From a practical perspective, the cross-cutting impact of the Cybersecurity Law is particularly noteworthy. It imposes extensive obligations on a wide range of public and private entities, including the obligation to register with the National Cybersecurity Authority. The law also establishes institutional CSIRTs and requires compliance with minimum security requirements, mandatory incident reporting, and financial contributions to the Cybersecurity Fund.

These two pieces of legislation mark a significant milestone in Mozambique's legal framework concerning cybersecurity and cybercrime.

Meanwhile, the Cybercrime Law completes the regulatory framework by introducing a distinct classification of cybercrimes, some of which carry substantial criminal penalties, such as cyber espionage, which is punishable by up to 10 years' imprisonment. It also regulates the methods for obtaining digital evidence. As such, it brings Mozambique's legal framework into line with international standards on cybercrime.

Both pieces of legislation require the Council of Ministers to adopt implementing regulations within 180 days. Therefore, it will be important to monitor the publication of these supplementary regulations, as they will largely determine how the new regimes are implemented in practice.

Next steps

In view of the framework established by the two pieces of legislation, it is recommended that organisations covered by them begin the compliance process immediately, paying particular attention to the following aspects:

- **Mapping the legal framework:** Organisations must identify which category or categories they fall into for the purposes of the Cybersecurity Law, as obligations vary depending on the applicable classification. If they fall into more than one category, the most stringent regime applies.

- **Registration with the National Cybersecurity Authority:** Most covered entities must register with the National Cybersecurity Authority in order to carry out their activities.

- **Establishment of an institutional CSIRT:** Entities subject to this obligation must prepare for the creation and governance of their incident response team.

- **Appointment of internal officers:** Public administration bodies, private sector organisations, and critical infrastructure operators must appoint a cybersecurity officer and an internal cybersecurity auditor to ensure the management of cyber risks.

- **Implementation of minimum security requirements:** Organisations covered by the requirements must review and implement an information security policy, a cyber risk management methodology, internal audit mechanisms and an employee training programme, in line with the minimum legal requirements.

- **Preparation of incident notification procedures:** Organisations must establish internal procedures to enable the timely identification, classification and notification of significant cybersecurity incidents to the CSIRT for the sector and the National CSIRT within the timeframes set by the National Cybersecurity Authority.

- **Review of data retention and access policies:** Organisations that store traffic or location data must ensure that such data is retained for a minimum period of one year. They must also review their procedures for responding to judicial requests for access to, preservation of, or seizure of data under the Cybersecurity Law and the Cybercrime Law.

- **Review of cooperation protocols with criminal investigation authorities:** Considering the new procedural provisions of the Cybercrime Law, organisations, particularly service providers, must review their internal procedures for responding to orders for the expedited preservation of data, data production orders, and requests for the interception of communications.

- **Monitoring of the regulations:** Close monitoring of the regulations to be approved by the Council of Ministers is required. These regulations will flesh out essential aspects of the current legislation, including technical security requirements and incident notification deadlines.

About PLMJ

→ Who we are

About NMP Advogados – PLMJ Colab Mozambique

→ Who we are

"The firm puts together a multi-tiered team, from juniors to partners, and we receive great advice from every level. We always feel supported from a Mozambican law perspective."

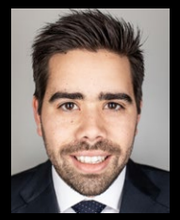
CLIENT REFERENCE FROM
The Legal 500

KEY CONTACTS

Pedro Lomba

Partner and head of the Technology, Media and Telecommunications practice

(+351) 213 197 412
pedro.lomba@plmj.pt



Nuno Morgado Pereira

Founding partner
NMP Advogados – PLMJ Colab Mozambique

(+258) 846 242 670
nuno.morgadopereira@nmpmozambique.com

Maio 2026

PLMJ COLAB ANGOLA — Mozambique — PORTUGAL

www.plmj.com