

AFRICTIVISTES

POLICY ANALYSIS

August 2020





Africtivistes

Ligne Africaine des Web activistes pour la démocratie

ENDCODE

Tech. Law. Policy. Africa.



Please note that our submission below does not constitute an in-depth analysis, nor a multi-jurisdictional comparison of Mauritania's laws against international standards. This article may be used as the basis of further in-depth analysis. EndCode did this analysis as part of its partnership with AfricTivistes.

Analysis of the Status of Cybercrime and Data Protection Law in Mauritania

Current Status

The **Law on Cybercrime (Law No. 2016-007)** (“the Cybercrime Law”) was promulgated 4 years ago and has not yet been brought into effect. While the enactment of the law is a positive and important development, the effect of the delay is that the nation does not enjoy a robust regulatory framework for cybercrime and cybersecurity.

There is a similar challenge in terms of the **Law on the Protection of Personal Data (Law No.2017-020)** (“the Data Protection Law”) framework as the legislation was promulgated in 2017 and has not commenced. The effect is that Mauritanian citizen’s personal data remains vulnerable and in the event of a data breach or any unethical processing of personal data, citizens do not have recourse. At this time, no indication has been given as to when the law will be implemented.

Under Mauritanian law, the government must proclaim enabling decrees in order to bring both laws into legal effect. It has been reported that the decrees have been drafted, however these have not been published. The consequence is that Mauritania does not have an entirely operational legal framework for cybercrime and personal data protection as the relevant legislation has not been brought into effect.

Perspectives on the Legal Frameworks

As recognised in international best practices, the objective of cybercrime legislation is to establish standards of acceptable behaviour for users of information and communications technology. Cybercrime legislation therefore is concerned with the following aims:¹

1

<https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html#:~:text=Cybercrime%20law%20identifies%20standards%20of,infrastructure%2C%20in%20particular%3B%20protects%20human>

- Creating offences and providing legal sanctions for cybercrime by enabling the investigation and prosecution of offences committed online.
- Protecting ICT users and mitigates and prevention of harm to people, data, systems, services and infrastructure.
- Upholding human rights.
- Facilitating cooperation between countries on cybercrime matters
- Cybercrime law imposes rules of conduct and standards of behaviour for the use of the Internet, electronic devices and related digital technologies. In addition, it provides rules of conduct and standards of behaviour which regulate the actions of the public, government, and private organisations;
- Enshrining rules of evidence and criminal procedure, and other criminal justice matters online. Further, it provides a regulatory framework to reduce risk and/or mitigate harm perpetrated against individuals, organisations, and infrastructure in the event of a cybercrime. In essence, cybercrime law provides substantive, procedural and preventive law.

Mauritania's cybercrime legislation provides as follows:

- Cybercrimes are criminalised under Chapter II of Law 2016/007, titled 'Offenses Against the Confidentiality, Integrity And Availability Of Data And Computer Systems'; and
- Articles 4 – 13 make provision for various cyber offenses including offences related to: breach of the confidentiality of a computer and/or the data stored thereon, breaches of the integrity and availability of a computer, the use/distribution of technologies/devices that may be used to commit cyber offences.

It is apparent that the Cybercrime Law aims to provide standards for acceptable conduct for users of information and communication technologies and this is aligned with international standards. In addition the Cybercrime Law creates offences and provides penalties for infringements, which are also vital aspects of international standards on cybercrime.

The international standards discussed above also demand that cybercrime legislation protects ICT users and critical infrastructure - in this regard, it is noted that Mauritania's Cybercrime Law fulfils these requirements.

In addition to the Cybercrime Law, the Mauritanian government is contemplating the development of a national cybersecurity strategy and has appointed the Computer Security Service, part of the Director General of Information Technology and Communications (DGITC),

which is specifically tasked with investigating cybercrimes (African Union & Symantec, 79). Mauritania, however, lacks an official and operational Computer Emergency Response Team (CERT).

The [Organisation for Economic Cooperation and Development \(OECD\) Guidelines on Personal Data Protection²](#) are recognised as an accepted model against which the Mauritanian data protection regime may be benchmarked. The Guidelines are formulated as follows:

- **Collection Limitation:** Data collection should occur only with the knowledge and consent of a concerned individual (data subject).
- **Data Quality:** One may only collect information which is relevant and accurate for a particular purpose.
- **Individual Participation:** The data subject must be made aware that their personal data has been collected and should be able to access it where personal data has been collected.
- **Purpose Specification:** The intended use of the personal data must be disclosed at the time of collection.
- **Use Limitation:** Collected data may not be used for purposes other than that disclosed at the time of collection.
- **Security Safeguards:** Reasonable measures must be implemented to protect personal data from unauthorised use, destruction, modification, or disclosure.
- **Openness:** Data subjects must be enabled to access their personal data as collected and be enabled to contact the entity collecting their data.
- **Accountability:** Data processors must be held accountable for any infringement of the principles above. A dedicated person responsible for compliance must be appointed.

Mauritania's Data Protection Law enshrines similar fundamental principles of data processing which are an important feature and aligned with OECD Guidelines. The fundamental principles provide that:

- The collection, storage, processing, storage of personal data must be lawful, fair and not fraudulent.

2

<https://www.oecd.org/internet/ieconomy/oecdguidelinesonthe protectionofprivacyandt ransborderflowsofpersonaldata.htm>


- Personal data must be collected only for specified, explicit and legitimate purposes and may not be subsequently processed in a manner incompatible with the purposes for which it was originally collected.
- Personal data must be adequate, relevant and not excessive in relation to the purposes for which it was collected and processed.
- Personal data may not be retained for a period exceeding the time necessary for the purposes for which it was collected or processed.
- Personal data must be accurate and updated where necessary. Reasonable measures must be taken to ensure that inaccurate or incomplete data is erased or rectified.
- The processing of data may only be undertaken in compliance with the principle of transparency on the part of the controller.
- Personal data must be kept confidential and are protected in accordance with the Law, especially where data is transmitted across a network.
- Personal data may only be processed subject to written legal agreement between the parties.

The internationally accepted principles of collection limitation, purpose specification, data quality, individual participation, security safeguards are provided in the legislation. As assessed against the OECD Guidelines, the Mauritanian Data Protection Law seemingly satisfies international standards. In addition, the requirement of a written contract between parties goes beyond the Guidelines and offers a greater degree of protection to data subjects. It is however, concerning that the Data Protection Law does not provide for individual participation and openness.

Note that the Data Protection Law does, however, omit provisions on the portability of data, breach notifications, privacy by design and the requirement for in-house Data Protection Officers (in certain instances). It is emphasised that at the least, the Data Protection Law should provide for breach notifications which are an essential part of enforcement for Mauritania's authorities, and are also a vital mechanism to enable Mauritanian citizens to protect their privacy and identity.

It is noteworthy that the Article 10 of the Mauritanian Constitution enshrines the fundamental rights to freedom of expression and the right to freedom of opinion and thought, however, the right to privacy is not enshrined.

Human Rights Watch (in January 2019) [criticised](#) the Mauritanian government and opined that the government has used overbroad and needlessly stringent laws (legislation related to cybercrime, criminal defamation and others) as a means of suppressing dissent and criticism.



The penalties and offences in the legislation were argued to have the potential to be used to suppress civil liberties, in particular the right to freedom of expression. UNODC warns that international law recognises it is sometimes necessary to impose limitations on human rights, however this is only justifiable in the pursuit of a legitimate purpose, in accordance with existing legislation and necessary and proportionate in relation to the purpose of the limitation.

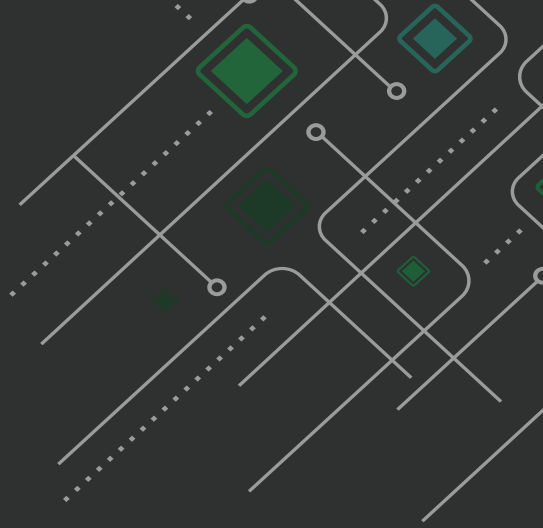
The cybercrime law, when measured against the criteria discussed above, may produce dangers to the exercise of civil liberties in Mauritania.

The primary criticism of the data protection law is that it is not operational. Increasingly, African nations are under threat from cybercriminals and at the same time, private and public sector institutions are also at risk of data breaches, Mauritians' personal data is vulnerable. The lack of implementation of the legislation means that there is no recourse in the event of a breach of personal data.


In Conclusion

While experts predict that the African continent will have a billion internet users by 2022, many nations are increasingly affected by cybercrime. There is therefore an urgent need for effective cybercrime and personal data protection legislation in Mauritania and other African countries.

The interminable delay in bringing the laws into force undermines cybersecurity concerns. Mauritians therefore do not enjoy the benefits of the legislation and are at a disadvantage in securing recourse against any violations of their personal data.



Silky Oak House | Bally Oaks Office Park | 35 Ballyclare Drive | Bryanston
Johannesburg, South Africa

 +27 (0) 11 463 4594

 endcode.org

 base@endcode.org

 [@endcode_org](https://twitter.com/endcode_org)

Company Reg No. 2014/118528/07

