Internet Society Lesotho Chapter

CIPESA

Online Privacy at Stake in Lesotho

with the Adoption of the Compliance Monitoring and Revenue Assurance Regulations, 2021

August **2021**

Introduction

The Constitution of Lesotho, 1993 as amended protects every person from arbitrary search of the person or entry by others of his or her premises under section 4(1)(f) and 10. Similarly, section 11 protects individuals' privacy and family life. In 2011, Lesotho enacted the Data Protection Act[1] which stipulates principles for regulation of processing of personal information to protect the privacy of personal information. Despite the constitutional provision and the enactment of the data protection law, several legislative measures undertaken in the country undermine individual data protection and privacy contrary to established regional and international human rights standards. Moreover, Lesotho is yet to sign and ratify[2] the African Union Convention on Cyber Security and Personal Data Protection.[3]

The draft Compliance Monitoring and Revenue Assurance Regulations, 2021 have been made in accordance with section 55(1) and 55(2) of the Communications Act, 2012. The objective of the regulations is to provide conditions, requirements and procedures for monitoring of telecommunications traffic in Lesotho through the installation of tools or systems for transparency in monitoring the regulatory compliance of mobile network operators and mobile financial service providers.

While subsidiary legislation is relevant to put into effect the provisions of the Act, in their current form the regulations could interfere with individual rights and freedoms including data protection and privacy. This brief highlights the major concerns that could arise from the adoption and implementation of the regulations.

The Positive Elements

The objectives in regulation 4, specifically (a) on generating reliable statistics and (b) on monitoring quality of service for international and national interconnection traffic, could form the basis for improved service delivery. Further, regulation 4(c) on detecting, tracking and blocking fraud and 4(d) on providing the international mobile subscriber identity (IMSI) details and subscriber identification module (SIM) profile for fraudulent SIM, could help to counter phone fraud.

Similarly, monitoring mobile money gateways and transactions to capture transactional information from the unstructured supplementary service data (USSD) platform under regulation 4(h) and monitoring international money transfer gateways and transactions which use mobile phone-based platforms to remit international incoming transfers under regulation 4(i) could help counter money laundering which is a big threat to the financial sector and at the same time may be used to finance illicit activities like terrorism.

1 *Data Protection Act, 2011. Retrieved from http://www.nic.ls/lsnic/community/policies/Data_Protection_Act_2011_Lesotho.pdf*

2 *https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf*

3 *African Union Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf*

Procedure for installing C-MART

Under regulation 6 the procedure for installing the compliance monitoring and revenue assurance tool (C-MART) includes the provision of international incoming voice services (regulation 6(a)), termination and origination of international incoming and outgoing telecommunication traffic (regulation 6(b)), interchange of local telecommunication traffic using national gateways within Lesotho (regulation 6(c)), provision of mobile money services (regulation 6(d)), and mobile money transfer services using mobile phone based platforms (regulation 6(e)).

This regulation once adopted will potentially guarantee protection of the consumer against cybercrime such as theft, fraud and identity theft and other forms of abuse since it requires licensing from the Authority prior to carrying on business. Similarly, it could work to ensure that only authorised persons deal with consumers.

Confidentiality of Information.

Regulation 16 prohibits unlawful disclosure of any information received by the Lesotho Communication Authority during the exercise of its powers or duties except where the release of such information is required by law. Similarly, regulation 13(2) requires the Lesotho Communication Authority to ensure that there is no transmission of personal data to third parties, either public or private, except as permitted by law. This guarantees some level of protection of the data subject from personal data breaches and invasion of privacy.

Provisions of Concern

The Objectives

While the objectives of a law or proposed legislation are critical in establishing the justifications for the law, the objectives in regulation 4 provide an opportunity for the Lesotho Communication Authority (Lesotho Communication Authority) to wantonly interfere with individual privacy. The objectives include generation of reliable statistics (regulation 4 (a)), monitoring quality of service (regulation 4 (b)), detecting, tracking and blocking fraud (regulation 4 (c)), providing international mobile subscriber identification details and SIM profile for fraudulent SIM (regulation 4 (d)), monitoring mobile money gateways and transactions (regulation 4 (h)), and monitoring international money transfer gateways and transactions (regulation 4 (i)). Privacy of the individual could be affected through, among others, unauthorised access, storage, processing and usage of data without the consent of the data subjects. Such acts are parallel to the established regional and international data protection principles and potentially interfere with the intent of the Data Protection Act to protect personal information from unauthorised processing.

Similarly, regulation 13, in as far as it provides for monitoring and inspection by requiring licensees to allow Lesotho Communication Authority or its representative to install and maintain necessary equipment on the licensee's network and facilitation of the "installation of data transmission equipment between the Authority's monitoring system installed at their switch centers and the Authority's main operating center", perpetuates privacy infringement by enabling real time monitoring, interception and surveillance.

Moreover, there is no provision for judicial oversight over monitoring and inspection of communication traffic. This is ambiguous and potentially facilitates consistent data privacy breaches. Furthermore, the provision in regulation 13(2) to the effect that; "Authority shall ensure that the data collected, is for the exclusive purpose of monitoring compliance with these Regulations and that it is not transmitted or given to third parties, either public or private, except as permitted by law" does not in any way provide an assurance that personal data shall not be transmitted to third parties.

Unlimited Power of the Lesotho Communication Authority

Under Regulation 5, powers of regulation and monitoring of telecommunications traffic are given to the Lesotho Communication Authority which already has broad powers under the Communications Act especially section 4 on general duties of the Lesotho Communication Authority and section 5 on the general powers of the Lesotho Communication Authority. The powers of the authority are generally exercised within licensing, regulation, suspension and revocation of licences. For example, under regulation 18(2), the Lesotho Communication Authority reserves the right to issue a civil penalty in terms of Schedule 2, or revoke an operator's licence for contravening the provisions of the Regulations. In this regard the regulations are wide and ambiguous as they detrimentally affect the independent functioning of the communications sector.

Biased licensee requirements

Regulation 7 provides for unquestionable installation of connections linking the C-MART network operations center (C-MART NOC) to the licensee's network. The regulation reads:

> *7 (1) A licensee shall not resist, deny access, obstruct or delay installation-*
> *(a) of a connection linking the C-MART NOC to the licensee's network; and*
> *(b) by the Authority on the licensee's premises, on interconnect border control system (IBCS) and transmission links between the same to the Authority's NOC.*

Under the provision, licensees have no level of autonomy over their infrastructure which may compromise balance between business and human rights observance. Hence, the question whether human rights such as privacy and data protection can be observed amidst doing business as encapsulated in the United Nations Guiding Principles on Business and Human Rights[4] comes into play, with the answer being most likely in the negative. Moreover, the penalty prescribed under Regulation 7(1) by Schedule 2 to regulation 18 (1) and (2) is punitively high to a tune of M500,000 (USD 33,823) for each day that the non-compliance persists. Such a fee could automatically kick licensees out of business.

Furthermore, under regulation 9 the licensee is primarily charged with ensuring the safety of C-MART devices installed on their network and premises with liability for damages and replacement of the damaged or destroyed device. A licensee is further required to make payments to the Authority based on the previous highest invoice plus 10% of the invoiced amount during the period the device remains tampered with, destroyed or damaged, save where the damage or destruction is by natural calamity. The provision is not only punitive and delimiting but also represents injustice and unfairness on the licensee, rendering their operations rather difficult. It could also increase the cost of accessing the internet in the country as service providers may incur additional operational costs, thus increasing internet costs to break even. This may worsen the country's internet access considering internet penetration which as of January 2021 stood at 47.9%.[5]

4 *United Nations Guiding Principles on Business and Human Rights, https://www.ohchregulation org/documents/publications/guidingprinciplesbusinesshr_en.pdf*

5 *https://datareportal.com/reports/digital-2021-lesotho*

Potential for real-time surveillance

Under regulation 10(1), "a licensee shall submit, to the Authority, call detail records (CDR) or information related to telecommunication traffic within six days after the end of each month." This is a mandatory requirement that Licensees must comply with. Further, under regulation 10(2), where the information is requested by the authority, it shall be submitted to it within 14 days. Further, under regulation 8, a licensee shall keep signaling data required to monitor telecommunication traffic, in accordance with the Regulations. Under regulation 8(2), the signaling data "shall include origin, destination, service information, time and path of communication and shall be processed and stored exclusively for the purpose of monitoring compliance with these Regulations." Regulation 8(3) provides that "The signaling data shall be stored in modified versions with the appropriate security measures, both physical and logical data and shall only be stored for the duration necessary for the purpose of monitoring compliance under these Regulations." It adds: "A licensee shall notify the Authority, in advance, of any upgrades or changes of their signaling system with detailed timelines to ensure the proper functioning of the C-MART"

The above-mentioned provisions potentially promote real time surveillance through monitoring and tracking information and data of individuals. It also promotes potential unlawful processing of personal data contrary to part IV (sections 30 to 38) of the Data Protection Act, 2011, which exempts processing of personal information that interferes with the privacy of the data subject.[6] Similarly, it is an addition to the arbitrary circumstances under section 25(4) of the where the data controller may not comply with consent provisions in respect of personal data.[7] section 25(4) among others provides in (c) that non-compliance is necessary – (i) to avoid prejudice to the maintenance or enforcement of law and order; (ii). to enforce a law imposing a pecuniary penalty; (iii) to enforce legislation concerning the collection of revenue by the state; (iv) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or (v) in the interests of national security.

Conclusion

The Compliance Monitoring and Revenue Assurance Regulations, 2021 largely interfere with individuals' privacy especially through real time surveillance and monitoring of communications and transactions. While they present opportunities for countering some cybercrime like phone fraud, they should be revised and the regressive provisions as highlighted above removed or amended to protect individuals' data and privacy rights which are guaranteed in the Constitution, the Data Protection Act, and regional and international human rights instruments.

6 *Data Protection Act, 2011*

7 *CIPESA, "Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa" CIPESA ICT Policy Briefing Series, 2018, https://cipesa.org/?wpfb_dl=272*

CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

+256 414 289 502

programmes@cipesa.org

@cipesaug

facebook.com/cipesaug

www.cipesa.org