Internet Society Lesotho Chapter

CIPESA

Lesotho: SIM and Device Registration Pose Major Threats to Data Protection and Privacy

August 2021

Introduction

The Kingdom of Lesotho has drafted the *Communications (Subscriber Identity Module and Mobile Device Registration) Regulations, 2021.* The regulations are to be made pursuant to section 55 of the Communications Act, 2012 and will apply to corporate, private and commercial subscribers of mobile telecommunications services utilising SIM and subscribers of foreign licensees who are roaming on the network of a licensee in the Kingdom.[1]

The objectives of the regulations under **Regulation 4** include the provision of a regulatory framework for the registration of subscribers of mobile telecommunications services utilising SIM and mobile devices in Lesotho; and the establishment, control, administration and management of a Central Database of subscribers. Despite the objectives reflecting a legitimate need, the provisions have a far-reaching impact on privacy and data protection of telecom services users in Lesotho.

Storage of Subscriber Information in a Central Database

Regulation 5 mandates the Lesotho Communications Authority (LCA) to establish and maintain a central database of all registered subscriber information. The central database is required to be mandatorily segregated across network services in a manner that ensures easy access to data by authorised persons in respect of subscribers' information of the different licensees. Moreover, under **Regulation 6**, the central database is a property of the government, while its management, care and control are vested in the LCA.

The centralisation of personal information presents a great threat to the privacy of all persons whose data is collected, processed and stored in such a system. While centralised systems are simpler and quicker to develop, there could be weaknesses making the database vulnerable to hacking or access by unauthorised third parties. This could happen despite the provision in Regulation 7(2) that the administration of the central database shall be in accordance with the latest standards issued by the International Organisation for Standardization (ISO) on security and management of electronics and personal data. It is currently not clear to what extent these standards shall be implemented in the design, operation and management of the database.

1 *Regulation 3 on the Application of the regulations*

Unrestricted Access to and Use of Subscriber Information

Under **Regulation 8** the licensee has an express right to retain and use its subscriber information on its network in accordance with applicable laws and the provisions of the license conditions. Furthermore, under **Regulation 9**, the subscriber information on the central database shall be provided only to security agencies and such release is by **Regulation 11** required to be in accordance with the law provisions. However, **Regulations 8** and **9** take away the data subjects' autonomy over their data while at the same time creating wide room for data breaches by licensees and security agencies. Further still, there is no guarantee that access under **Regulation 11** by security agencies will be in accordance with the law.

Past experiences have shown that while access to data by authorised persons may be for legitimate purposes such as preservation of security, state security agencies often have unrestricted access to subscriber information with limited oversight. This often perpetuates the abuse of individuals' privacy. In other instances, such access has been used to track, trace, intimidate, persecute and suppress individuals that are critical of the government. These regulations neither provide a check nor a balance through a judicial authority and a data protection authority to oversee access to and use of subscriber data collected and stored in the central database. Further, no remedy is provided for breaches committed by the Authority or by state security agencies.

Mandatory Registration and Transmission of Subscriber Information to the Central Database

Under **Regulation 12** licensees are required to register every subscriber's information and transmit it to the central database. The information to be registered includes "(a) biometrics and other personal information of a subscriber who requests for registration of mobile devices and the activation of a SIM; and (b) in the case of an institution, corporate or other juristic person, the biometrics and other personal information of the authorised representative of the institution, corporate or other juristic person and the name, address and where applicable, the registration number of the juristic person issued by the relevant authority."

Under **Regulation 2**, the biometric information collected will include fingerprints and facial image of subscribers, while the personal information collected will include their full names (including mother's maiden name), gender, date of birth, residential address, nationality, district of origin, occupation and such other personal information and contact details of subscribers specified in the Registration Specifications.

Similarly, under **Regulation 13**, activation of new subscribers requires that the licensee provides them with a SIM enabled for limited access to their network services, which shall last for the duration of activation subject to presentation of personal information. Furthermore, under **Regulation 15**, personal information of foreign subscribers shall be registered within 48 hours before roaming services are provided to them.

The mandatory and excessive requirement for the registration of personal information of subscribers for both nationals and foreigners interferes with constitutionally guaranteed rights. It could infringe on the privacy of the individual through data breaches contrary to the Data Protection Act of 2011 and **section 14** of the Constitution of Lesotho which provides for freedom of expression. It is not apparent how the extensive list of biometric and personal information collected is necessary and proportionate for the government's aim of regulating telecommunication services in the country.

Deactivation and Deregistration of a Mobile Device and SIM

Regulation 16 provides that, "the licensee may deactivate and deregister a mobile device or SIM upon request by a subscriber after verification and confirmation of the subscriber information on the mobile device and SIM." And further that "records of any deactivation or deregistration shall be transmitted to the central database by the licensee in accordance with specifications issued."

However, no justification is provided for the transmission and neither is there a specification of the duration for storage of the transmitted data. This potentially runs contrary to **section 19** of the Data Protection Act which limits data retention to the prescribed period and **section 18** which provides for purpose specification and regulates further processing. In its current state the regulation facilitates infringement of privacy and data breaches as it lacks requisite checks on personal data usage, processing and management within the acceptable standards.

Imposition of Liability on Subscribers

Regulation 17 prohibits proxy registration of any mobile device or SIM, while **Regulation 19** imposes liability on subscribers for any activity carried out using a mobile device or SIM registered with their personal information. The restriction of proxy registration together with liability for acts done using SIMs or devices, in the absence of exceptions to deal with circumstances of fraudulent registration, lost devices, errors and mistakes during registration, could potentially result in innocent civilians being convicted for offences committed without their knowledge.

Conclusion

These **regulations** have a chilling effect on the right to privacy and freedom of expression contrary to well established regional and international human rights instruments. These include article 19 of the *Universal Declaration of Human Rights* (UDHR) and the *International Covenant on Civil and Political Rights* (ICCPR), article 9 of the *African Charter on Human and Peoples Rights*, and the *African Union Convention on Cyber Security and Personal Data Protection*. They also contravene the *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019* especially Principle 40 on privacy and the protection of personal information, Principle 41 on privacy and communication surveillance and Principle 42 on the legal framework for the protection of personal information.

While the regulations could potentially contribute to curbing cybercrime and make some steps to protect data of subscribers from potential misuse by licensees, they have overreaching negative effects on the right to privacy as well as freedom of expression. They give wide opportunities to the government and its security agencies to wantonly use subscribers' personal data without their consent, an aspect that has a chilling effect on freedom of expression and limits the right to access information. There is an urgent need to drop the repressive and regressive provisions in the regulations while maintaining those that aim to curb cybercrimes.

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