TECHNOLOGY, MEDIA & TELECOMMUNICATIONS SECTOR

CDH
CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

REGULATING THE FOURTH INDUSTRIAL REVOLUTION – South Africa's Cybercrimes Bill is signed into law

Compiled by Preeta Bhagattjee, Aphindile Govuza and Reece Westcott

9 JUNE 2021

On 26 May 2021, President Ramaphosa signed the Cybercrimes Bill into an Act of Parliament and a law of the Republic of South Africa as the Cybercrimes Act 19 of 2020 (Cybercrimes Act). The Cybercrimes Act is South Africa's attempt at regulating the proliferation of digitised criminal activities that have resulted as a consequence of the Fourth Industrial Revolution. This is, however, not South Africa's first foray into regulating aspects of our increasingly digitised future - other examples include the Protection of Personal Information Act 4 of 2013 (POPIA) and the recently published Draft National Data and Cloud Policy. This article will delve into the notable aspects of the Cybercrimes Act, while also highlighting certain provisions and their interaction with other existing laws such as POPIA.

The Aim of the Cybercrimes Act

The Cybercrimes Act aims to both create new offences that, for example, criminalise the theft and interference of data, while also modernising existing criminal offences to cater for the particular nature with which many cybercrimes are committed. The objectives of the Act are therefore to:

- create offences and impose sanctions that relate to cybercrime;
- criminalise the dissemination of harmful data messages; and
- further regulate law enforcement's jurisdiction over cybercrime by granting extensive powers to investigate, search, access and seize articles used in committing an offence, such as computers, databases or networks, etc.

Specific offences created under the Cybercrimes Act include a person's unlawful access – being the unlawful and intentional access to a computer system or a computer data storage medium (commonly referred to as "hacking"); and the unlawful interception, interference or acquisition of data, a computer program, a computer data storage medium or a computer system.

The 'modernised' criminal offences include cyber fraud – being fraud committed by means of data or a computer program or through any interference with data or a computer program; cyber forgery – being the passing-off of false data or a false computer program with the intention to defraud; cyber extortion – being, *inter alia*, the unlawful and intentional interception of data for the purpose of obtaining any advantage from another person or compelling another person to perform or to abstain from performing any act; and the theft of incorporeal property. Of note, however, is the criminalisation of malicious or harmful communications. These are communications, or rather 'data messages', which:

- incite or threaten damage to property or violence;
- threaten persons with damage to property or violence; and
- disclose an intimate image.

By defining 'person' as both a natural or a juristic person, the Cybercrimes Act casts a wide ambit as to who it applies to. Consequently, both ordinary citizens and organisations may be subject to both the offences and protections afforded by the Act. A person who is convicted of an offence under the Cybercrimes Act is liable to a fine or to imprisonment for a period of up to 15 (fifteen) years or to both a fine and such imprisonment as may be ordered in terms of the offence.

The Interaction with POPIA

Amongst other laws and regulations, the Cybercrimes Act has a number of provisions that interact with certain aspects of POPIA. POPIA specifically regulates the manner in which the lawful processing and protection of personal information of both natural and juristic persons should be carried out. The definition of 'processing' in section 1 of POPIA includes a wide range of activities such as the collection, receipt, modification, retrieval, alteration, transmission, degradation, erasure or destruction of personal information. Where any personal information is subject to unauthorised access or possession, POPIA addresses the obligations of the lawful holder of such personal information (i.e. the responsible party and/or operator, as defined under POPIA) to have taken

REGULATING THE FOURTH INDUSTRIAL REVOLUTION – South Africa's Cybercrimes Bill is signed into law

appropriate measures to secure and safeguard the personal information in the first place and when such data breach occurs or is suspected to have occurred, to take reasonable steps to address same including to report the occurrence to the Information Regulator (being the regulatory body established in terms of POPIA to ensure compliance with POPIA). The perpetrators of such unauthorised access or possession of personal information would now also be charged with an offence under the Cybercrimes Act.

In terms of section 22 of POPIA, a responsible party is obliged to report to the Information Regulator any actual or suspected instance where the personal information of a data subject is accessed or acquired by an unauthorised person. Section 54 the Cybercrimes Act imposes similar reporting obligations on electronic communications service providers and financial institutions who become aware that their electronic communications service or electronic communications network have been involved in the commission of any category or class of offence/s as outlined above.

Consequently, electronic communications service providers and financial institutions will be obliged to report the unauthorised access of the data/personal information within their possession to both the Information Regulator and the South African Police Service (SAPS), respectively. Of note, however, are the particular timeframes afforded to these persons when reporting such incidents. POPIA mandates that such a data breach must be reported to the Information Regulator and data subject *'as soon as reasonably possible'*, while the Cybercrimes Act specifically mandates that such an offence must be reported to the SAPS *'not later than 72 hours'* after having become aware of the offence. Companies who function as electronic communications service providers and financial institutions must be cognisant of their respective obligations under these two Acts, along with any other instance where the Cybercrimes Act may coincide with other laws or regulations that may be relevant in this regard.

Conclusion

With the invariable influx of people who have access to the internet or any other electronic communications medium, the rapid increase in cybercrimes is all but guaranteed due to the anonymised and global nature of cyberspace. South Africa has now taken a significant step to cater for this eventuality by enacting the Cybercrimes Act. The date that the Cybercrimes Act will come into force is still to be announced.

Preeta Bhagattjee, Aphindile Govuza and Reece Westcott